Advances in Intelligent Platform Management: Introducing the New IPMI v2.0 Specifications

Tom Slaight
Principal Server Management Architect
Intel Corporation

February 18, 2004
Special Guests!

Phil Chidester
Manageability Architect
Server Management Firmware Group
Dell Computer

Steve Lyle
Manageability Architect
Hardware Systems Technology Division
Hewlett-Packard Company
Agenda

- IPMI Architecture and Initiative Update
- What’s New in IPMI v2.0?
- IPMI v2.0 Technology: How it meets platform management needs
- IPMI in Action
- IPMI Futures
IPMI Architecture and Initiative Update

IPMI

Intelligent Platform Management Interface

- Defines a standardized, abstracted, message-based interface to intelligent platform management hardware

- Defines standardized records for describing platform management devices and their characteristics

Promoters:

Adopters: 162 and growing

IPMI Enables Cross-Platform Management Software
IPMI v2.0 Specifications
Updated v1.5 Errata, 32- and 64-bit Drivers, & IPMI Conformance Test Suite

IPMI Architecture and Initiative Update

Initiative News

developer.intel.com/design/servers/ipmi
New Adopter’s Agreement

- IPMI v2.0 Second Generation Specification is under RAND (Reasonable And Non-Discriminatory) licensing model
  - Aligns with Industry standards licensing models (e.g. DMTF*, PICMG*, Infiniband*, etc.)

- All companies (including existing IPMI 1.5 adopters) will need to sign new IPMI v2.0 adopters agreement to implement IPMI v2.0 spec
  - Existing IPMI 1.5 adopters can continue to implement IPMI v1.5 under old licensing terms, but to new IPMI v2.0 agreement required to implement new IPMI v2.0 features

- New IPMI v2.0 Adopters license available on IPMI web site for your review

Sign Up as IPMI 2.0 Adopter Today!
IPMI v2.0 Architecture

IPMI Architecture and Initiative Update

IPMI Messages
IPMI in modular architecture

Typical Modular Application

- **LAN**
  - Remote Mgmt Console System

- **compute node A**
  - BMC
  - BP I/F
  - Sys I/F

- **compute node B**
  - BMC
  - BP I/F
  - Sys I/F

- **i/o node**
  - Satellite Controller

- **mgmt module**
  - Mgmt. Module Processor
  - BP I/F

- **chassis**
  - FAN
  - FAN
  - Satellite Controller
  - temp
  - PS
  - PS

- **Backplane Mgmt Interconnect**

- **IPMI Messages**

- **CIM to IPMI**
Where it fits…

IPMI helps reduce TTM and development cost for cross-platform management
Agenda

- IPMI Architecture and Initiative Update
- What’s New in IPMI v2.0?
- IPMI v2.0 Technology: How it meets platform management needs
- IPMI in Action
- IPMI Futures
Platform Directions for IPMI

- Integrated ‘Serial over LAN’ management
- Low Cost Systems
  - “Baseline” BMCs
- Group Managed Systems
  - ICMB and LAN-managed systems
- Modular Systems
  - General purpose and Service Availability Forum “AdvancedTCA” blade systems

IPMI enables competitive features across server classes
IPMI v2.0 Technology

IPMI v2.0 Additions

- **Serial Over LAN (SOL)**
  - Redirects local serial interface over an IPMI Session
  - Works with serial-based OS ‘command line’ interfaces
- **LAN Session Enhancements**
  - New user login and security configuration options enable tailoring security and performance to match the needs of the site
  - “Payloads” capability enables multiple types of management traffic (e.g. IPMI and SOL) over a single LAN session
- **Enhanced Authentication**
  - Stronger key exchange uses two-way challenge/response
  - Aligns with DMTF ASF 2.0* session establishment
- **Packet Data Encryption**
  - Enables remote operations such as user password configuration
- **VLAN Support**
  - Facilitates setting up ‘management-only’ networks

* Other names and brands may be claimed as the property of others
IPMI v2.0 Technology

IPMI v2.0 Additions

- **Low-cost BMC Support**
  - SMBus System Interface (SSIF) provides low-pin count system interface for low-cost (low pin-count) BMCs

- **Modular Extensions**
  - Node replacement, Redundant Management Bus monitoring, “Firmware Firewall” tailor IPMI to better support blade implementations

- **Enhanced OEM value-added feature support**
  - Support for OEM Security Algorithms and Payload options (e.g. KVM) on IPMI infrastructure
Agenda

- IPMI Architecture and Initiative Update
- What’s New in IPMI v2.0?
- IPMI v2.0 Technology: How IPMI v2.0 meets platform management needs
- IPMI in Action
- IPMI Futures
IPMI Technology

Remote Access
- Serial: Basic, Terminal, PPP
- ICMB: IPMI over Serial, Serial Port Sharing

Session Infrastructure
- SSIF

IPMI Core
- Firmware Firewall
- Sensor Access
- Control (on/off/reset/intr)
- Watchdog
- PEF
- LAN & Serial Alerting
- Logging
- FRU, SEL, SDRs
- Users & Privileges

Local Access
- System Interfaces: KCS, BT, SMIC, SSIF
- Mgmt Busses: IPMB, PCI-SMBus
SMBus System Interface (SSIF)

- Encapsulates IPMI messages in an SMBus compatible format
  - Compatible with common SMBus Host controllers
  - IPMI Requests delivered using ‘Block Write’ protocol
  - IPMI Responses retrieved using ‘Block Read’ protocol
    - SMBAlert signal status change/message available

- SMBAlert line notifies host that incoming message / status data is available
  - ‘Get Status’ command allows interface status to be polled
SMBus System Interface (SSIF)

Local (System Interface) Discovery

- BIOS tables describe location and type of system interface
  - New ACPI “SPMI” (service processor mgmt. interface) Table
  - SMBIOS Type 38 Record

- SPMI and Type 38 Tables Applicable to all IPMI System Interfaces
  - SMIC, KCS, BT, SSIF
SSIF and Multi-level BMC Options

Low Cost Options enable IPMI for all Server classes

IPMI v2.0 Technology

Acts as ‘Satellite Controller’ to ‘Full’ BMC

LAN

South Bridge

Baseline BMC

System Monitor

FRU

Full BMC

chassis sensors

RS-232

LPC

LAN

82551

PCI

SMBus

SMBAlert

power, reset

System Bus

sensor connections

chassis sensors

ipmi
techology
IPMI v2.0 Technology

SMBus System Interface (SSIF)

Single Part Messages
- Used for IPMI Message Content up to 32 bytes
  (SMBus protocols limited to 32-bytes of data)

BMC Write / Request
(via SMBus Block Write)
- BMC Slave Addr. | Wr
- SMBus CMD = 0x02
- Length
  - IPMI NetFn (even) | LUN
  - IPMI Command
  - <IPMI Command Data>

BMC Read / Response
(via SMBus Block Read)
- BMC Slave Addr. | Wr.
- SMBus CMD = 0x03
- BMC Slave Address | Rd.
- Length
  - IPMI NetFn (odd) | LUN
  - IPMI Command
  - IPMI Completion Code
  - <IPMI Command Data>
SMBus System Interface (SSIF)

Multi-part Messages
- Used for IPMI Message Content >32 bytes
- Block numbers enable retrieving lost or corrupted middle or ‘end’ read data

BMC Multi-part Write / Request
(follows single part format for Start, but uses special SMBus CMDs for start and transferring remaining data)
- Start: SMBus CMD = \textcolor{red}{0x06}, remainder matches single part format
- Middle: SMBus CMD = \textcolor{red}{0x07}, followed by add’l request data
- End: SMBus CMD = \textcolor{red}{0x08}, followed by last part of data

BMC Multi-part Read / Response
(Starts off with reserved pattern [0x01, 0x00] then uses special SMBus commands to retrieve remaining data)
- Start: SMBus CMD = \textcolor{red}{0x03}, followed by [0x01, 0x00] then regular response data (NetFn | LUN, CMD, etc.)
- Middle: SMBus CMD = \textcolor{red}{0x09}, First byte = 00b followed by add’l response data
- End: SMBus CMD = \textcolor{red}{0x09}, First byte = 01b, followed by last part of data
IPMI Functional Blocks

- **Remote Access**
  - Serial: Basic, Terminal, PPP
  - ICMB: RMCP
  - LAN: “RMCP+” Session, SOL (Serial Over LAN)

- **Firmware Firewall**
  - Control Access, Logging, Users & Privileges
  - Watchdog, LAN & Serial Alerting, FRU, SEL, SDRs
  - System Interfaces: KCS, BT, SMIC, SSIF
  - Management Busses: IPMB, PCI-SMBus

- **Session Infrastructure**
  - IPMI over Serial, IPMI over LAN v1.5, IPMI over LAN v2.0

- **Local Access**
  - New: IPMI v1.5
  - Extended: VLAN, Firewall, Firmware

- **Intel**
IPMI v2.0 Technology
Firmware Firewall
Partitioning for protection

• Problem: Bus topology enables local mgmt s/w to access other nodes

• Solution: “firmware firewall”

![Diagram of firmware firewall concept]
Firmware Firewall

- F/W blocks messaging to other nodes on shared bus
- Allows messages between local software and management module
- Local software may also be blocked from SDR or FRU updates that might be used to generate false events
- Firmware updates can only occur from management bus side
- Access rights can only be configured from management bus side
IPMI v2.0 Technology

Firmware Firewall

• **Configurable Command Discovery** commands
  – Support discovering which commands and sub-functions can be enabled/disabled
  – Two commands: *Get Configurable Commands*,
    *Get Configurable Command Sub-functions*

• **Command Configuration** commands
  – Provide mechanism for enabling/disabling those commands
  – Four commands: *Set/Get Command Enables*,
    *Set/Get Command Sub-function Enables*
Command Discovery commands

– Enable software to discover what commands and subfunctions are available on given mgmt. controller

– Discovery commands can be implemented separate from Firmware Firewall enable/disable commands

– Centralize command and sub-function discovery
  – Augments IPMI distributed parameter, and ‘try command’ discovery
  – Command and sub-function support can vary on a PER CHANNEL basis

– Three commands: Get NetFn Support, Get Command Support, Get Command Sub-function Support
IPMI v2.0 Technology

Users & Privileges

- Per Channel Multi-level, Multi-User Security
  - User, Operator, Admin and OEM Privilege levels for IPMI commands
  - Per-user configurable enables for payload access (e.g. SOL)

- IPMI v2.0 Login Options
  - ‘Anonymous’ login: no username or password required
    - Can be enabled for a given privilege level. E.g. “User Level”
  - Role-based login: password only, no username, for a given privilege level
    - E.g. “Admin” login
  - Username login: user name and user password required
  - ‘Two key’ login: user/role password plus ‘BMC Key’
    - Can prevent multiple system access by ‘human engineering’ a single username/password pair.

Flexible configuration enables security to be tailored to site needs
Payloads enable multiple types of traffic to be carried over a single IPMI session
– payloads can also be launched to a separate session

Standard and OEM Payload Types supported
– OEM payload types: Enable value-added features on IPMI session infrastructure (e.g. KVM)
  – Leverages IPMI User configuration and authentication

Payload support is discoverable
Payload access enabled on a per-user basis

Session Payloads Enable “1-port” Management
Payloads can be activated under common or separate ports.

- LAN
  - Network Controller
    - Port 26Fh
    - IPMI & Payload Msgs
    - IPMI v2.0 Technology
  - BMC
    - Payload Processing

- LAN
  - Network Controller
    - Port 26Fh
    - IPMI Msgs
    - Payload Processor
    - Payload Msgs

IPMI v2.0 Technology

Serial Over LAN

- Defines common format and protocol for serial redirection under an IPMI Session
  - Redirects baseboard “16550” serial controller interface over LAN
  - Launched as a standard payload type under IPMI v2.0 Session

- Specification supports multiple serial connections

- Can be combined with IPMI Serial Port Sharing
  - Enables single ‘back of the box’ serial connection to be shared for local serial/modem, BMC access, and LAN redirected management
IPMI Functional Blocks

Remote Access
- Serial: Basic, Terminal, PPP
- ICMB
- LAN: RMCP

Session Infrastructure
- Session Over LAN: "RMCP+", SOL (Serial Over LAN)
- Payloads

IPMI Core
- Users & Privileges
- Authentication
- Integrity
- Confidentiality
- Users & Privileges

Local Access
- System Interfaces
- Management Busses
- Serial Port

Payloads: KCS, BT, SMIC, SSIF, IPMI, PCI-SMBus
IPMI v2.0 Technology

Authentication, Integrity, and Confidentiality

- **Authentication Algorithm**: Defines what steps are used for authenticating a User and establishing a session
  - E.g. IPMI v2.0 uses for RAKP (remote access key exchange protocol)
- **Integrity Algorithm**: Defines algorithm for signing packets after session has been established.
  - E.g. HMAC-SHA1-96
- **Confidentiality (encryption) Algorithm**: Defines algorithm for encrypted payload data in a session.
  - E.g. AES-128 (Advanced Encryption Standard)
- Combination of Authentication, Integrity, and Encryption algorithms defines a **CipherSuite**
- **Standard CipherSuites** provide algorithm to trade-off between strength and performance
- **OEM CipherSuites** also supported
IPMI v2.0 Technology

Encrypted and Authenticated Packets

• Authenticated / Unauthenticated and Encrypted / Unencrypted packets can be mixed in single session
  – Improves performance on small micros. Bits in payload type field indicate whether the payload data is authenticated and/or encrypted

• Remote console can be given option to control when payload data is encrypted
  – Allows console to decide when an operation, e.g. remote password configuration, requires encryption
  – For IPMI messages, an encrypted request gets an encrypted response
  – For other payloads, a Suspend/Resume Encryption command is used

• Can configure BMC to require that payload is encrypted.
  – Prevents mis-behaved console from exposing sensitive data.

IPMI v2.0 technology reduces overhead for secure remote management
IPMI v2.0 Technology

VLAN

- IPMI v2.0 LAN Packet format extended for “Virtual LAN” routing per IEEE 802.1q
- Works with side-band filtering in enhanced management network controllers
- VLAN support configurable on a per-channel basis
IPMI Functional Blocks

Remote Access
- Serial: Basic, Terminal, PPP
- IPMI over Serial
- Serial Port Sharing

Session Infrastructure
- ICMB
- RMCP
- "RMCP+" Session
- IPMI over LAN v1.5
- IPMI over LAN v2.0
- SOL (Serial Over LAN)

IPMI Core
- Firmware Firewall
- Watchdog
- PEF
- LAN & Serial Alerting
- FRU, SEL, SDRs
- Users & Privileges

Local Access
- System Interfaces: KCS, BT, SMIC, SSIF
- Mgmt Busses: IPMB, PCI-SMBus

IPMI v2.0 Sessions
- Sensor Access
- Control Access (on/off/reset/)
- Logging
- Users & Privileges
- IPMI over LAN v2.0
- SOL (Serial Over LAN)
- RMCP+
- EVE
- Session Moads
- IPMI v2.0 Sessions

IPMI v1.5
- New
**IPMI v2.0 Technology**

**Sessions**
Discovery and Connection

- **Enhanced User Login Options**
  - New option for ‘Role-only’ logins
  - Simplifies use in small installations
    - no username to remember, can simply login in as User, Operator, or Admin

- **New commands for managed system discovery**
  - Facilitates automated discovery and access by remote applications
    - IPMI version (v1.5 or v2.0) discovery
    - Cipher-Suite discovery
    - Available Payloads
    - Existence of Anonymous and One- or Two-key login
      - enables remote console to present appropriate username and password entry options
v2.0 Session Activation

- Discover IPMI support using **Get Channel Authentication Capabilities** command
  - Enables discovering IPMI version
  - Tells console whether ‘anonymous’ and/or ‘1-key’ logins are enabled
  - Same command for v1.5 and v2.0

- Issue **Get Cipher Suites** command
  - Pick cipher suite for the maximum privilege level you want to establish the session at

- Activate session for given user...
  - IPMI v2.0 Uses dual Challenge/Response vs. IPMI v1.5 single challenge / response
IPMI v2.0 Technology

v2.0 Session Activation

– Send *Open Session Request*
  Get *Open Session Response*
  – Sets session IDs and negotiates a ciphersuite

– Send *RAKP 1 Message*
  Get *RAKP 2 Message* as Response
  – Submits username and target privilege level to BMC
  – Exchanges random numbers between console and BMC
  – Roughly equivalent to the console submitting a challenge to the BMC and the BMC submitting a challenge to the console.

– Issue *RAKP 3 Message*, Get *RAKP 4 Message* as Response
  – BMC and Console exchanged ‘signed’ RAKP 3 and RAKP 4 packets
  – Signature based on the random numbers and key data associated with the user
  – Session is activated when both parties verify the signed packets.
IPMI Functional Blocks

Remote Access
- Serial: Basic, Terminal, PPP
- IPMI over Serial
- ICMB: IPMI over LAN v1.5
- LAN: RMCP, "RMCP+" Session
- VLAN: SOL (Serial Over LAN)
- New: IPMI v1.5
- Extended: Backward Compatibility

Session Infrastructure
- IPMI Core: Firmware, Firewall
- LAN: IPMI over LAN v1.5, SOL (Serial Over LAN)
- Mgmt Busses: IPMB, PCI-SMBus
- System Interfaces: KCS, BT, SMIC, SSIF
- Alerting: LAN & Serial Alerting
- FRU, SEL, SDRs: Payloads
- Watchdog: PEF
- Users & Privileges: Logging

Local Access
- Serial Port Sharing
- Authentication: Integrity, Confidentiality
- LAN & Serial: Logging
- System Interfaces: KCS, BT, SMIC, SSIF

Backward Compatibility
Backward Compatibility

- Compatible command superset
  - Extends but does not replace IPMI v1.5 commands
- Managed systems can be discovered and used as an IPMI v1.5 system
  - Implementation can support both IPMI v2.0 and IPMI v1.5 connections simultaneously
  - Supports connecting using IPMI v1.5 protocols
    - IPMI v1.5 LAN packet support retained
- V2.0 packets/protocols required for new LAN features
  - e.g. enhanced auth., encryption, Serial Over LAN
IPMI v2.0 Technology

IPMI Session Activation

CONSOLE
- Discovery
  - Get Channel Authentication Capabilities, Rq
- Activation
  - Get Session Challenge, Rq
  - Open Session, Rq
  - Activate Session, Rq
  - RAKP Message 1
  - RAKP Message 3
- Active
  - Set Privilege Level, Rq
  - Activate Payload, Rq
  - Close Session, Rq

BMC
- Discovery
  - Get Channel Authentication Capabilities, Rs
- Activation
  - Get Session Challenge, Rs
  - Open Session, Rs
  - Activate Session, Rs
  - RAKP Message 2
  - RAKP Message 4
- Active
  - Set Privilege Level, Rs
  - Activate Payload, Rs

Rq=request, Rs=response

IPMI v1.5
IPMI v2.0
Common v1.5/2.0

CONSOLE BMC

Intel®

IPMI v2.0 Technology

Get Channel Authentication Capabilities, Rq
Get Session Challenge, Rq
Open Session, Rq
Activate Session, Rq
RAKP Message 1
RAKP Message 3
Set Privilege Level, Rq
Activate Payload, Rq
Close Session, Rq

Get Channel Cipher Suites, Rq
Get Session Challenge, Rs
Open Session, Rs
Activate Session, Rs
RAKP Message 2
RAKP Message 4
Set Privilege Level, Rs
Activate Payload, Rs

INTEL CORPORATION CONFIDENTIAL

42
Putting It All Together

IPMI v2.0 Technology

Remote Access
- Basic, Telnet, PPP
- Serial Port Sharing

Session Infrastructure
- Authentication
- Integrity
- Confidentiality

Firmware/Files
- Sensor Access
- Control (on/off/reset/intr)
- LAN & Serial Alerting
- Logging
- Users & Privileges

System Interfaces
- KCS, BT, SMIC, SSIF
- IPMB, PCI-SMBus

IPMI v1.5

Extended

New
Agenda

- IPMI Architecture and Initiative Update
- What’s New in IPMI v2.0?
- IPMI v2.0 Technology: How IPMI v2.0 meets platform management needs
- IPMI in Action
- IPMI Futures
As one of IPMI’s founding companies - HP has a long history of building industry standards around manageability.

HP’s entire line of Integrity IPF servers use IPMI, from the smallest 2-way server to the largest Superdome.

HP uses IPMI, along with other manageability standards like WBEM, to build interfaces that promote interoperability between OS’s and platforms.
HP: Enabling customer features

- IPMI fits well into the ecosystem of HP's value-added embedded management, covering some of the most basic functionality in a standard way
  - OS absent server health and server power control
  - Storage and retrieval of system event logs
  - A standard messaging mechanism for use with HP agents on Windows, HPUX, and Linux
- Upon this foundation, HP builds more features, to further enhance the manageability solution
  - Independent management LAN with secure (https) web interface or convenient Telnet UI to the management processor
  - Embedded web console
  - Enhanced event logging and diagnosis
  - Unique collaboration and repair features
  - Partition management, and more…
IPMI In Action

Dell Computer

“Standards simplify the computing environment and establish a common hardware and software platform, make it easier for systems to work together and to exchange information. Standards also simplify product development and service, thereby reducing our costs.”

Michael Dell

• Dell and IPMI
  – Dell a founding IPMI Promoter
  – IPMI a core management technology for today’s Dell PowerEdge servers

• IPMI benefits for Dell Customers
  – Helps lower server acquisition, training and operations costs
  – Enhances server availability
  – Enables server management with common tools and processes

• IPMI 2.0 extends these benefits
  – Enhances IPMI management security
  – Extends administrators reach with serial-over-LAN operations
  – Demonstrates industry focus on driving management standards

IPMI Delivers Common Management Interfaces
IPMI In Action

Dell PowerEdge™ 3250: An IPMI Manageable Standards-Based Server

A cost effective, scalable solution for compute intensive applications utilizing Itanium Processor Family and standards-based manageability

- Standards-based manageability for high performance computing
  - IPMI 1.5 server management
  - SMART drive monitoring
  - DMTF SMBIOS and ASF alerting

- Pro-active management for the scalable enterprise
  - Centralized operations enabled with IPMI monitoring and alerting
  - Remote control and recovery functions through IPMI server control, remote consoling
  - Large-scale remote operations via IPMI command-line interface

IPMI Supports “Real Server” Management
**IPMI In Action**

**Intel Corporation**

- One of the Founding Companies for IPMI
- Over 5 years of IPMI-based Management for Server Building Blocks
  - In pedestal, rack, and modular (blade) chassis
  - In Entry through Enterprise
  - With Itanium®, Xeon™, and IA-32 processors
  - In General Purpose and Telco systems
  - Small business to Data Center

**IPMI Works Across System Classes**
IPMI In Action

Intel Corporation

• Over 7 product generations
• Over 5 different processors used for BMCs
  – some large systems have had as many as four management controllers
• Use IPMI SDRs to tailor server building blocks to customer
• Implementations take advantage of Intel processor and chipset management features
  – E.g. Memory and Bus Correctable and Uncorrectable error status, power state information, temperature and throttling status, etc.

IPMI Is Proven Technology
IPMI Technology is Widely Supported

- Abit Computer Corp.
- Acer Inc.
- Adtron
- Amplus Inc.
- Advanced Micro Devices, Inc.
- Agilent Technologies GmbH
- Alberta Microelectronics Inc.
- Alliance Corp.
- American Megatrends Inc.
- Arima Computer Corp.
- Artesyn Technologies, Inc.
- ASIS LTD.
- ASUSTeK Computer Inc.
- Aventail Corporation
- Avian Communications Inc.
- Avocent, Inc.
- Axil Computer, Inc.
- Blue Wave Systems
- Bull S.A.
- C&D Technologies, Inc.
- California Digital Corp.
- Celestica
- C-MAC Engineering
- ColoWATCH, Inc.
- Communication Corporation
- Compellent Technologies, Inc.
- Concurrent Technologies, PLC
- CyberGuard Corporation
- Cyrcle Systems
- Data General Corporation
- Data Computer Corporation
- Data Associates
- Digi International
- Egenera, Inc.
- ElnVital Corporation
- Ericsson UAB
- ESO Technologies
- Evans & Sutherland
- Eversys Corporation

- Exabyte Corporation
- Extreme Engineering Solutions, Inc.
- Fabric7 Systems, Inc.
- Firstech Communications, Inc.
- FORCER Technology GmbH
- Flextronics Corp.
- Flextronics Technologies Corp.
- Folsom Computer Products
- Glucorex, Inc.
- HACO Corporation
- HCL (HCL Infosystems Ltd)
- Hewlett-Packard Company
- Hewlett Packard GmbH
- Hitachi America Corporation
- IBM
- Ibus America Corporation
- ImmoMediaLogic, Inc.
- Infineon Technologies
- Intel
- InterWorks Computer Products
- Invensys Information Products
- IPWare, Inc.
- JMC Products
- KeeLin, Inc.
- Kentron
- Kaputar, LLC
- L-3 Communication Corp.
- LANtronix
- LANT Technology
- Legrand France, Ltd.
- Leo, MEGWARE Computer GmbH
- Linux NetworX, Inc.
- Lycus, Inc.
- Magway, Inc.
- Marconi, Inc.
- MEGWARE Computer GmbH
- Merco Computer Systems, Inc.
- Micro-Star International
- Miranpoint, Inc.
- Mocoro Computer Systems, Inc.
- Mitsubishi Electric Corp.
- National Semiconductor Corp.
- NEC Corporation
- Network Storage Solutions, Inc.
- NDS Software, Inc.
- NEWSYS, Inc.
- NDC Software, Inc.
- ODL-Tech, Inc.
- Odyssey Computers Worldwide
- OSA Technologies, Inc.
- Open Source Development Lab
- PEP Modular Computers
- PERMITECH
- Petabyte Technologies, Inc.
- PDU Limited
- Phoenix Technologies Ltd.
- Philips Power Systems
- Planar Systems
- Plantronics, Inc.
- Quanta Computer Inc.
- Raiton Technology Corporation
- RAMbld Computer Inc.
- Reliant Computer Corporation
- Reliant Computer Corporation
- SBC (Seminole Group)
- SDI Group
- SDS Microsystems
- SGS-Thomson, Inc.
- SGS-Thomson Microelectronics Ltd
- Sharp Laboratories
- SCS Technology Corporation
- SFA Computer Corp.
- Synergy Microsystems
- Synergy Microsystems Inc.
- Synergy Microsystems
- Tyan Computer Corporation
- Trimm Technologies
- Tyan Microelectronics
- U.S. Digital Systems Corporation
- U.S. Digital Systems Corporation
- U.S. Digital Systems Corporation
- VIVID Technology, Inc.
- Vatica, Inc.
- VDI Corporation
- VDI Corporation
- VIA Technologies, Inc.
- Vico Technologies
- Vuki
- WIPRO Infotech, Inc.
Agenda

- IPMI Architecture and Initiative Update
- What’s New in IPMI v2.0?
- IPMI v2.0 Technology: How IPMI v2.0 meets platform management needs
- IPMI in Action
- IPMI Futures
IPMI Futures

Advancing Platform Management

IPMI v1.5
- Monitoring (temp, volt, fan, etc.)
- Control (power on/off/cycle, reset, diag. interrupt)
- System Event Logging
- FRU & SDR Information
- Watchdog Timer
- Serial and LAN access
- Serial and LAN alerts
- Platform Event Filtering
- Serial Port sharing
- Management busses

v2.0 Additions
- Session and Security Enhancements
- Serial Over LAN
- SSIF
- Alignment with ASF Authentication
- Encryption support
- Firmware Firewall
- Command Discovery
- Modular (blade) support

v2.0+ ...
- New Payload Types
- Enhanced Configuration Interfaces
- Links to Directory-based Authentication
- Improved Group Control
- Auxiliary Log Access
- Integration with Web Interfaces
- Web services-based access

Proven Foundation for New Platform Management Features
New Capabilities Under Consideration

- Additional redirection payloads:
  - e.g. KVM, USB-media

- Improved configuration interfaces
  - Simplified save/restore of configuration settings
  - Secure migration of user configuration
  - Integration with configuration of ‘Alternative Access’ features, e.g. Web Server, Telnet

- Interfaces to Directory-based authentication

- More efficient options for ‘group control’
  - E.g. option for ‘persistent’ connections
IPMI Futures

New Capabilities Under Consideration

- Auxiliary Log access
- OOB configuration integration with web-based interfaces
  - enabling/disabling web server, CLI, Telnet
  - Configuring user privileges associated with secured interfaces
  - Integration with directory-based authentication
- Web-services –based interfaces
  - Alignment with “CIM+” / DMTF SMWG
  - “IPMI over XML/SOAP”

IPMI will continue to evolve with valuable new capabilities
Where to get More Info

IPMI Web Site
- Latest IPMI Specifications & Errata
- Presentations
- IPMI Conformance Test Suite
- Example Drivers
- Tools
- FAQ and Integration Guides
- Mailing List
- List of IPMI Adopter Companies
- Adopter Agreements

developer.intel.com/design/servers/ipmi
Summary

- IPMI reduces TTM and development cost for platform management
- IPMI v2.0 enables cross-platform manageability across server classes
- IPMI v2.0 technology enables secure remote management
- IPMI v2.0 technology is widely supported
- IPMI will continue to evolve with valuable new capabilities
Advances in Intelligent Platform Management

Tom Slaight, Intel Corporation
Steve Lyle, HP
Phil Chidester, Dell

Questions?

More on IPMI and IPMI v2.0 at IDF:

- “Birds Of A Feather” - Get Together at lunchtime today
  Join us for an informal dialog and Q&A on IPMI and related technologies

- Session: OSA S010 - Design Considerations for the Open Standards
  Manageability Stack - IPMI, HPI and CIM
  1st session after lunch

- Technology Showcase - See demos of IPMI-based systems and SOL capabilities
  in the Intel Pavilion

Please remember to turn in your session survey form
Birds-of-a-Feather Lunch Discussions

**Where:** Level 3 Foyer *(Not in the main lunch area)*

**Arrive early – seating is limited**

**When:**

<table>
<thead>
<tr>
<th>Wednesday 12PM – 1:30PM</th>
<th>Thursday 12PM – 1:30PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11*</td>
<td>Enthusiast PC</td>
</tr>
<tr>
<td>Extensible Firmware Interface (EFI)</td>
<td>Ethernet in the Datacenter</td>
</tr>
<tr>
<td>802.16*/ WiMax*</td>
<td>Trusted Computing Group for More Secure Computing</td>
</tr>
<tr>
<td>Latin America Mobile/Data Environment</td>
<td>Advanced Switching based on PCI Express* Architecture</td>
</tr>
<tr>
<td>Server Manageability</td>
<td>Mobile Wireless Manageability</td>
</tr>
<tr>
<td>Advanced TCA*</td>
<td>Convergence in the digital home</td>
</tr>
<tr>
<td>Client Manageability</td>
<td>IPMI (Intelligent Platform Management Interface)</td>
</tr>
<tr>
<td>Advanced Switching based on PCI Express* Architecture</td>
<td></td>
</tr>
<tr>
<td>Mobile Wireless Manageability</td>
<td></td>
</tr>
<tr>
<td>IPMI (Intelligent Platform Management Interface)</td>
<td></td>
</tr>
</tbody>
</table>

*Seating is limited.*
Please fill out the Session Evaluation Form.

Thank You!
### SSIF - SMBus System Interface

<table>
<thead>
<tr>
<th>Operation</th>
<th>SMBus CMD</th>
<th>SMBus Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BMC Single Part Write</strong></td>
<td>0x02</td>
<td>Write Block</td>
</tr>
<tr>
<td><strong>BMC Multi-Part Write</strong></td>
<td>0x06</td>
<td>Write Block</td>
</tr>
<tr>
<td>- Start – first part</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Middle part(s) if any</td>
<td>0x07</td>
<td>Write Block</td>
</tr>
<tr>
<td>- End – last part</td>
<td>0x08</td>
<td>Write Block</td>
</tr>
<tr>
<td><strong>BMC Single Part Read</strong></td>
<td>0x03</td>
<td>Read Block</td>
</tr>
<tr>
<td><strong>BMC Multi-Part Read</strong></td>
<td>0x03</td>
<td>Read Block, first two data bytes after length = [0x01,0x00]</td>
</tr>
<tr>
<td>- Start – first part</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Middle part(s) if any</td>
<td>0x09</td>
<td>Read Block, first data byte after length = 0x00</td>
</tr>
<tr>
<td>- End – last part</td>
<td>0x09</td>
<td>Read Block, first data byte after length = 0x01</td>
</tr>
</tbody>
</table>