July 22-26, 2013

MDC MANAGEMENT DEVELOPERS CONFERENCE

City Center Marriott
Portland, OR

SMASH & DASH: Technology Update

Hemal Shah (Broadcom), VP of Tech, DMTF

Jeff Hilland (HP), President, DMTF

Perry Vincent (Intel), SDMPWG Co-chair, DMTF

Disclaimer

- The information in this presentation represents a snapshot of work in progress within the Distributed Management Task Force (DMTF).
- This information is subject to change. The standard specifications remain the normative reference for all information.
- For additional information, see the DMTF website.

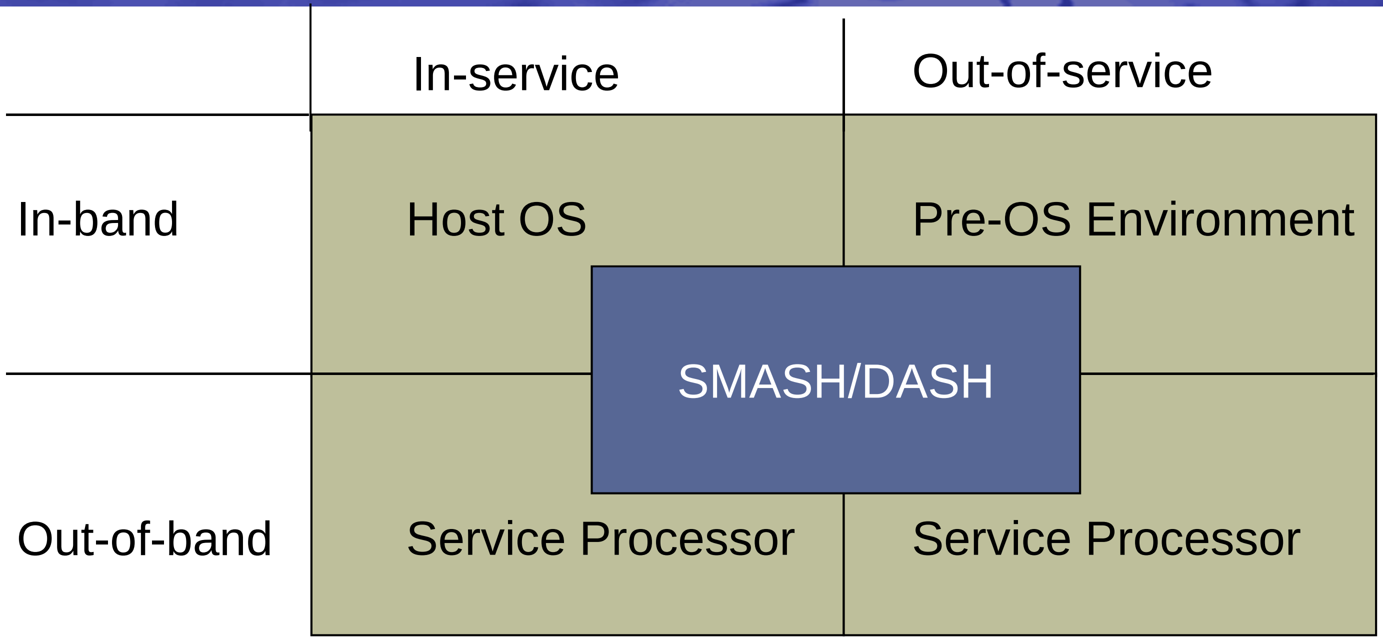
Agenda

- Introduction
- SMASH/DASH architecture overview
- Management protocols
- CIM profiles
- Discovery
- Security requirements
- New CIM profiles
- Future SMASH/DASH specifications
- Conclusion

DMTF Management Initiatives

- Built upon DMTF technologies.
- Deliver functionality to specific domains.
- Current DMTF management initiatives
  - CLOUD: Cloud management
  - CDM: Common Diagnostics Model
  - CIM: Common Information Model
  - DASH: Desktop and mobile Architecture for System Hardware
  - SMASH: Systems Management Architecture for Server Hardware
  - VMAN: Virtualization Management
- SNIA SMI is also recognized as a management initiative.

Industry-Standard Alignment Platform Manageability



	In-service	Out-of-service
In-band	Host OS	Pre-OS Environment
Out-of-band	Service Processor	Service Processor

SMASH/DASH

- DMTF driving a consistent interface/view.
  - Independent of platform state/access method
- Align industry around key elements.
  - Protocols: WS-Management and SM-CLP
  - Data model: Common Information Model (CIM)

What is SMASH?

- Systems Management Architecture for Server Hardware
  - A suite of specifications that deliver industry-standard protocols/profiles to unify the management of the data center
  - Vendor independent
  - Platform neutral
  - Independent of machine state
- SMASH specifications consist of:
  - SMASH Implementation Requirements specification
  - Architecture white paper
  - CIM profiles
  - WS-Management specifications
  - SM CLP and SM CLP mapping specifications
- The SMASH specifications utilize the CIM data model and industry-standard transports and security mechanisms.
  - Align out-of-service with in-service manageability.
  - Align in-band with out-of-band manageability.
  - Customer driven
- www.dmtf.org/standards/smash

What is DASH?

- Desktop and mobile Architecture for System Hardware
  - A suite of specifications to unify the management of desktop and mobile platforms
  - Vendor independent
  - Platform neutral
  - Independent of machine state
- DASH specifications
  - Build on Web-services-based programmatic interface.
  - Utilize the CIM data model.
  - Leverage industry standard transport and security mechanisms.
- DASH specifications consist of:
  - DASH Implementation Requirements specification
  - Architecture white paper
  - CIM profiles
  - WS-Management specifications
- www.dmtf.org/standards/dash

State of SMASH

- SMASH 1.0 published in December 2006.
  - Architecture white paper.
  - SM CLP, 1.0 final standard – ANSI & ISO Standard!
  - SM ME addressing, 1.0 standard.
  - Profiles and mapping specifications, 1.0 standards.
  - Released standard in October 2009.
- Interoperability Forum formed in the DMTF (SMF).
  - Working to develop compliance tests.
- SMASH 2.0 published in September 2007.
  - Includes WS-Management support – ANSI & ISO Standard!
  - Added discovery.
  - Additional profiles:
    - PCI, LED, KVM Redirection, Watchdog, OS Status, Indications.
    - Added reference to SMI-S Host Hardware Raid Profile.
  - Updated white paper.
  - Released standard in August 2009.
- SMASH 2.1 scoping in progress.
- SMASH CIM profiles: ANSI approved/ISO effort is in progress.

State of DASH

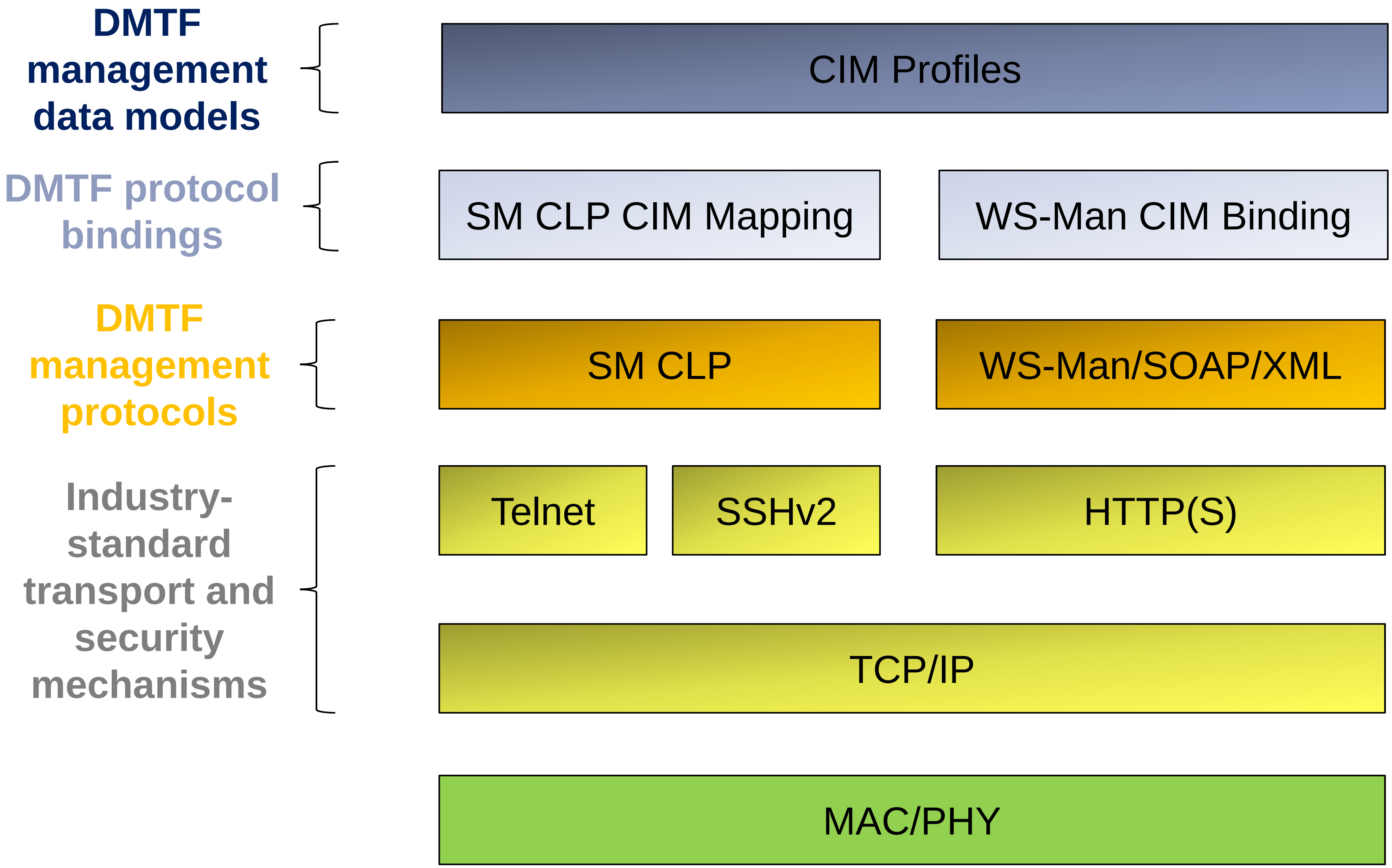
- DASH 1.0 specifications:
  - Architecture white paper
  - CIM profiles
  - Implementation Requirements Specification
    - First published in April 2007; released standard in May 2009.
  - Message registry
- DASH 1.0 specifications cover:
  - Inventory, power control, and boot control.
  - User account management and indications.
- Interoperability forum formed in the DMTF (SMF).
  - Working to develop compliance tests.
- DASH 1.1 Implementation Requirements Specification
  - Published in December 2007; released standard in June 2009.
- DASH 1.1 specification additionally covers:
  - Software update, OS status, additional inventory, and IP configuration.
  - Opaque management data.
  - BIOS management.
  - Text console, media, USB, and KVM redirections.
- DASH 1.2 scoping is in progress.
- DASH CIM profiles: ANSI approved/ISO effort is in progress.

SMASH/DASH Architecture Models

- In-Band/Out-Of-Band Management model
- Manageability Access Point (MAP) model
  - Common transport/protocol: WS-Management
- Operational model
  - Job-oriented for certain functions
- Session model
  - Concurrent sessions
- Resource handling
- Security model

HS1

SMASH/DASH Stack



DMTF management data models — CIM Profiles

DMTF protocol bindings — SM CLP CIM Mapping | WS-Man CIM Binding

DMTF management protocols — SM CLP | WS-Man/SOAP/XML

Industry-standard transport and security mechanisms — Telnet | SSHv2 | HTTP(S)

TCP/IP

MAC/PHY

Slide 11

HS1 Add a key and fix colors.

Hemal Shah, 7/8/2013

Management Protocols

- WS-Management
  - Stands for Web Services Based Management.
  - Common programmatic interface:
    - Leveraged by both SMASH and DASH.
  - Normative references and mapping information in:
    - SMASH & DASH implementation requirements.
- SM CLP
  - SMASH also includes the SM CLP.

What is WS-Management?

- Specification of a core set of web services for a common set of system management operations.
- Comprises the abilities to:
  - Manipulate management resources.
    - Create, destroy, rename, get, and put.
  - Enumerate the content of instances of classes, containers, or collections (logs or tables).
  - Subscribe/unsubscribe to events.
  - Execute specific management methods.

TCP Ports for SMASH/DASH

- Embedded DASH implementations operate on well-known TCP ports for WS-Man.
  - Repurposed ASF TCP ports (include discovery)
  - One for HTTP (623)
    - Could be configured to support discovery only.
  - One for HTTPS (664)
- Embedded SMASH implementations.
  - Standard HTTP (80)/HTTPS (443) ports for WS-Man
  - Standard TCP ports for SM CLP telnet/SSHv2

What is SM CLP?

- Server Management Command Line Protocol
  - Designed for a human (primary) or a script (secondary).
  - Working over, but not limited to, Telnet & SSHv2.
  - Exposes CIM data model in a human friendly fashion.
- SM CLP is not a full-featured programming I/F.
  - Lightweight: Some semantics were intentionally left out.
  - A programmatic interface is still required for some operations.
  - But input and output can be fully parsed by a machine.
- However, all of the hardware operations (provisioning, allocation, configuration, inventory, state change, and security) can be done with the SM CLP.
  - By a human, script, or program.
  - Because there is a grammar that defines input & XSD output.
- Very lightweight implementations can be done.

Profile Support

- A profile is a specified subset of CIM schema elements.
  - Describes a standard implementation for interoperability and conformance verification.
  - Common Information Model (CIM) defines the language and methodology for describing management data.
  - CIM schemas provide the actual model descriptions.
- A profile contains:
  - Required and conditional CIM element properties and methods.
  - Class and instance diagrams.
  - Profile usage guide and *profile registration profile* compliance.
- DMTF is producing profiles.
  - Strong desire to have common set of profiles.
  - Synergy with SMASH, DASH, and SMI efforts.
  - Definition of optional elements to support scaling from desktop and mobile platforms up to stand-alone, modular, and partitionable servers.

SMASH Profiles

High-Level Profiles

1. **CLP Service**
2. **Base Server**
3. **Modular System**
4. **Service Processor**
5. Physical Asset
6. Boot Control
7. SM CLP Admin Domain
8. SMASH Collection
9. CPU
10. System Memory
11. Fan
12. LED
13. Power Supply
14. Power State Management
15. Record Log
16. Sensor
17. Watchdog
18. Host Hardware Raid (Reference)
19. OS Status
20. PCI Device
21. Software Update
22. Software Inventory
23. Host LAN Network Port
24. IP Interface
25. Ethernet Port
26. DHCP Client
27. DNS Client
28. SSH Service
29. Telnet Service
30. Role Based Authorization
31. Simple Identity Management
32. Shared Device Management
33. Pass-Through Module
34. Device Tray
35. Text Console Redirection
36. KVM Redirection
37. Profile Registration
38. Computer System
39. Indications

* Underlining indicates SMASH 2.0 profile; BOLD is autonomous profile.

DASH Profiles

High-Level Profiles

1. Base Desktop & Mobile

Component Profiles

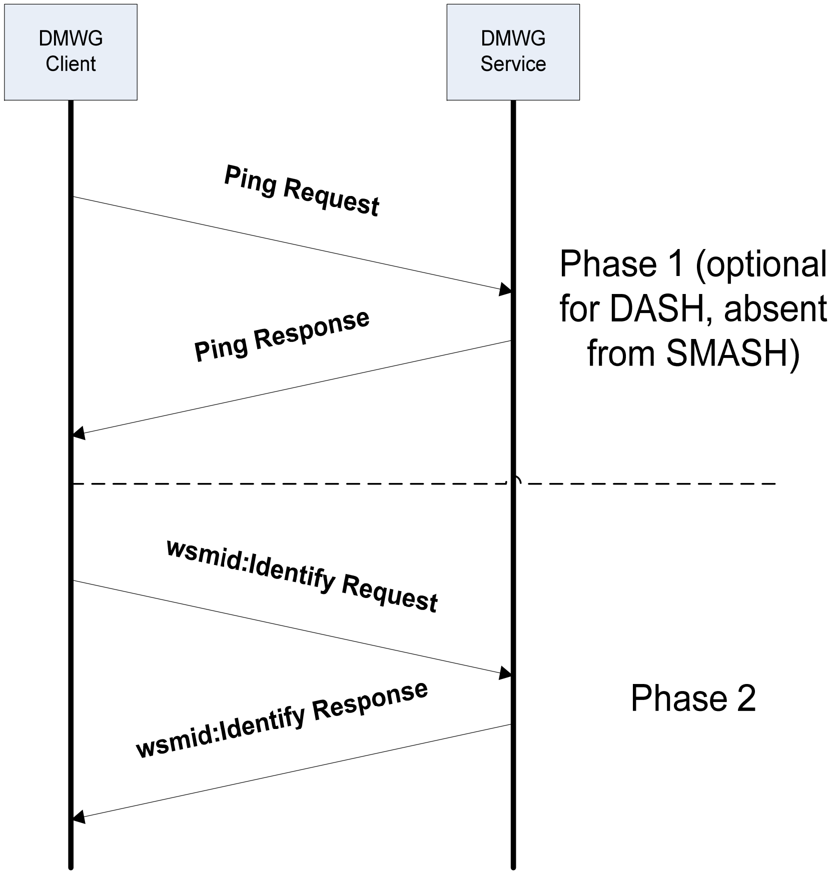
2. *Physical Asset*
3. *Boot Control*
4. *CPU*
5. *System Memory*
6. *Fan*
7. *Power Supply*
8. *Power State Management*
9. *Sensor*
10. Battery
11. BIOS Management
12. Opaque Management Data
13. *OS Status*
14. *Software Update*
15. *Software Inventory*
16. *Host LAN Network Port*
17. *IP Interface*
18. *Ethernet Port*
19. *DHCP Client*
20. *DNS Client*
21. *Role Based Authorization*
22. *Simple Identity Management*
23. *Text Console Redirection*
24. *KVM Redirection*
25. Media Redirection
26. USB Redirection
27. *Profile Registration*
28. *Computer System*
29. *Indications*
30. Wi-Fi

- Underlining is DASH 1.1 profile
- BOLD is autonomous profile
- Italics show common profiles between DASH/SMASH

Discovery Overview

- When discussing discovery, it is important to divide the discussion into three broad groups:
  - Network addressable endpoint discovery.
  - Classification (type discovery).
  - Service discovery.
- These broad groups can be further broken down with each layer of discovery providing more information, including:
  - The existence of the network addressable endpoint.
  - The type of device (classification).
  - The services (capabilities) of the device as a whole.
  - The device in the context of topology (for example, a MAP in a client machine).

Two-Phase Discovery



Phase 1 (optional for DASH, absent from SMASH)

Phase 2

SMASH/DASH WS-Management Security Requirements

- HTTP 1.1 is the required transport.
- Two classes of SMASH and DASH defined WS-Management security levels:
  - Class A, HTTP only
  - Class B, HTTPS or IPSec
- A SMASH or DASH implementation must be compliant with at least one of the security classes.
- A SMASH or DASH implementation should be Class-B compliant for privacy/confidentiality and additional security.

Classes of Security Profiles

- Class A: HTTP digest authentication (user authentication)
- Class B: Support for at least one of security profiles below
  - HTTP_TLS_1
    - Two-level auth + encr: HTTP digest auth. + TLS server/client certs (X.509) + TLS 1.0 (implementation of client cert is optional.)
    - Cipher suites
      - TLS_RSA_WITH_AES_128_CBC_SHA
  - HTTP_TLS_2
    - Two-level auth + encr: HTTP basic auth. + TLS server/client certs (X.509) + TLS 1.0 (implementation of client cert is optional.)
    - Cipher suites
      - TLS_RSA_WITH_AES_128_CBC_SHA
  - HTTP_IPSEC
    - Two-level auth + encr: HTTP 1.1 over IPsec with HTTP digest authentication
      - IPsec ESP transport mode: Authentication + Encryption
    - Cipher suites: One of the following:
      - AES-GCM (key size: 128 bits, ICV, or digest len: 16B)
      - AES-CBC (key size: 128 bits) with HMAC-SHA1-96

SMASH/DASH Authentication Requirements

- Required user account management profiles
  - Role Based Authorization profile
  - Simple Identity Management profile
- Three roles are defined for DASH and SMASH:
  - Administrator: Mandatory for SMASH and DASH
  - Operator: Optional for SMASH and DASH
  - Read-only: Mandatory for SMASH, optional for DASH

Indications

- Two major categories of indications for the CIM model:
  - Alert
  - Life-cycle
- Alert indications
  - Message ID/string-oriented class design.
  - The underlying event and its data may or may not be modeled in the CIM class hierarchy.
  - Includes handles pointing to the alerting managed element.
  - Includes support for specifying recommended actions.
- Lifecycle indications
  - Generated based on changes in instantiated objects.
  - Indication class includes the object instances and handles pointing to the objects.
  - For changes in existing objects, the indication class also includes the object instance before the change.
  - Predominant approach used by SNIA, generally focused on:
    - Object creation and deletion.
    - Value changes to the OperationalStatus and HealthState properties.

Alert Indications

- Platform Alert Message Registry – DSP8007
  - Standardized message IDs and message strings.
  - Published recommended “Perceived Severity” mappings.

- Included in DASH 1.0 and 1.1 and SMASH 2.0 specifications.

- Published recommended message registry mappings.
  - Recommended PET Frame Values Mapping specification.

New Profiles

- Physical Computer System View 1.0
- Power State Management 2.0
- Record Log 2.0
- OS Status 1.1
- Service Processor 1.1
- IP Configuration 1.0

Physical Computer System View (PCSV) Profile

- A simple profile for using CIM in data centers.
- Focused scope of profile.
  - Most common use cases (“80% case”)
  - DCMI equivalence
  - View class with methods and writable properties
  - Conditional behavior (not optional) well defined
- Meant to complement current profiles.
- Shows relationships and capabilities not possible with bitwise protocols IPMI/DCMI.

PCSV Profile Overview

Features

- Discovery (inventory, FRU)
  - Common inventory (CPU, memory)
  - FRU & serial number
- Machine state
  - Health state and status
  - Sensors
- Chassis power
  - State and reset
- Boot control
  - Current order and order change
- Logging
  - Get and clear records
- Firmware and BIOS
  - Version and update method
- OS
  - Type and status

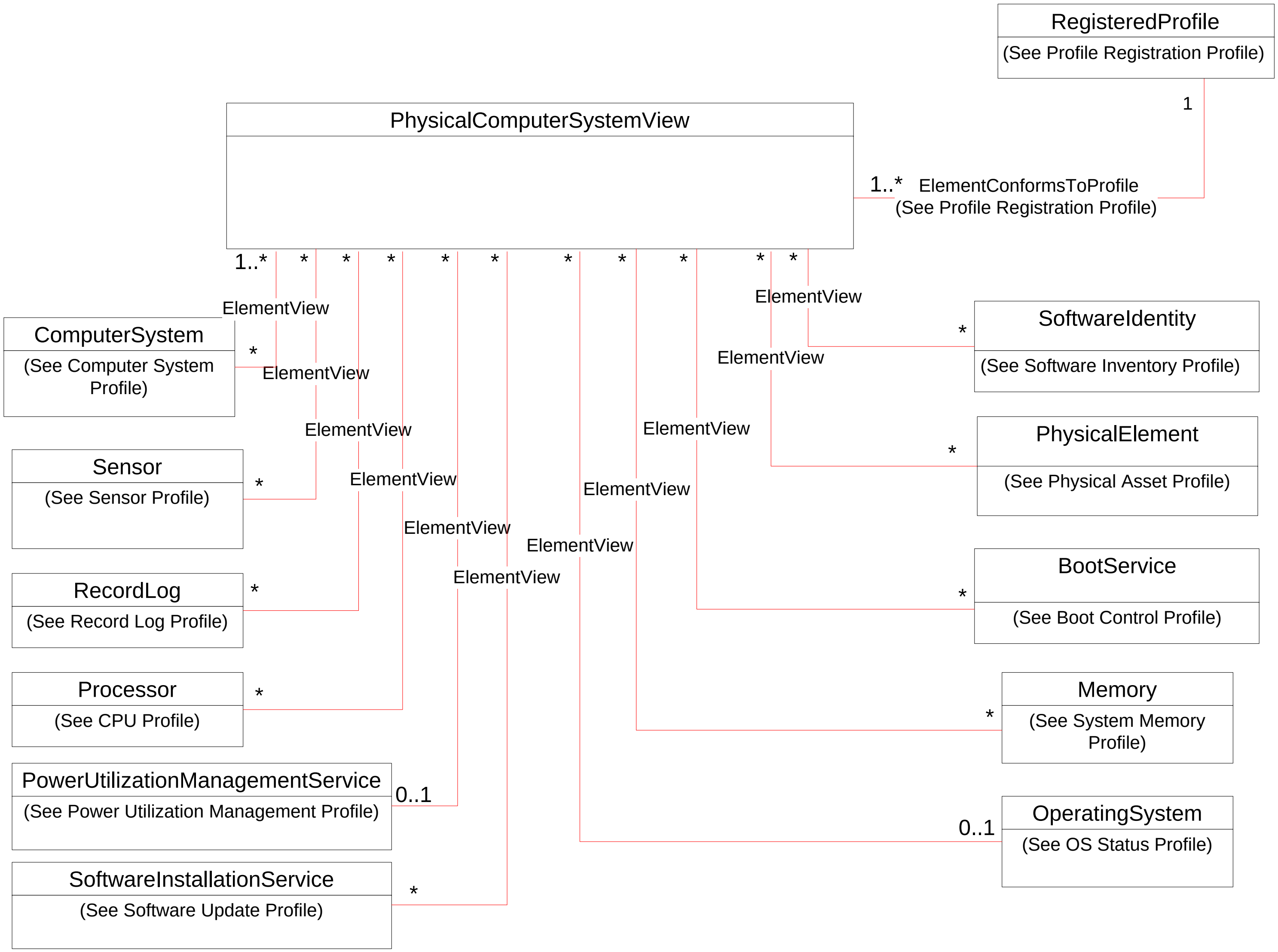
Registered Profile

- CIM_RegisteredProfile ImplementedFeatures property will indicate conditional behavior.
- Eliminates need for Capabilities class.

View Class Support

- Streamlined common use cases.
- Model shows relationship with referenced profiles.
- Referenced profiles handle other cases like:
  - Power/cooling relationships for complex chassis.
  - Complex/Multiple firmware elements.

PCSV Profile – Class Diagram



RegisteredProfile
(See Profile Registration Profile)

PhysicalComputerSystemView

ComputerSystem
(See Computer System Profile)

Sensor
(See Sensor Profile)

RecordLog
(See Record Log Profile)

Processor
(See CPU Profile)

PowerUtilizationManagementService
(See Power Utilization Management Profile)

SoftwareInstallationService
(See Software Update Profile)

SoftwareIdentity
(See Software Inventory Profile)

PhysicalElement
(See Physical Asset Profile)

BootService
(See Boot Control Profile)

Memory
(See System Memory Profile)

OperatingSystem
(See OS Status Profile)

Power State Management Profile 2.0

- Power State Management Profile 1.0 defines:
  - Behavior of power management service.
  - Classes used to:
    - Describe/control power state.
    - Manage computer-system hardware reset.
  - Methods that constitute a pending power-state change and an immediate power-state change.
- Power State Management Profile 2.0:
  - Adds properties for the available requested power states and transitioning to a power state.
  - Refines ACPI power-state mapping.
  - Covers additional use cases: displaying, discovering, and changing power state based on the available power states.

Record Log Profile 2.0

- Record Log Profile 1.0 describes:
  - Properties for managing record logs.
  - Association between managed system and logs.
  - Containment of log entries within a Record log.
  - Methods for log state management and clearing.
- Record Log Profile 2.0
  - Added Record log entry format definitions (extensible).
  - Two formats defined:
    - Record Data format – free form format.
    - Standard Message format.
  - A Record log entry shall be compliant to one format.
  - A Record log may contain entries with both types.

OS Status Profile 1.1

- OS Status Profile 1.0 defines:
  - Basic management of the installed OS.
  - Management of running OS state.
  - Discovery of OS capabilities.
- OS Status Profile 1.1 adds:
  - Representation of OS version information.

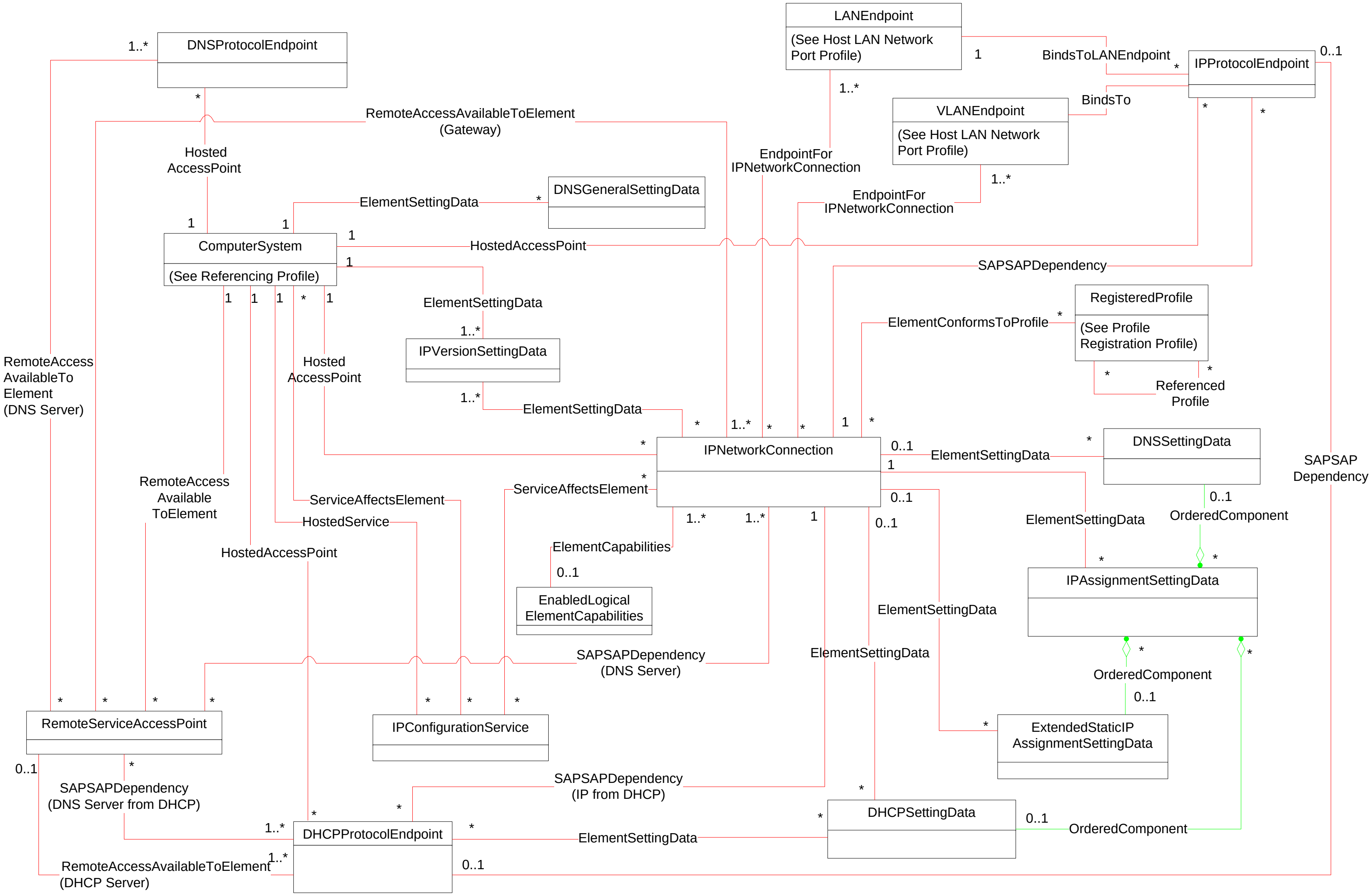
Service Processor Profile 1.1

- Service Processor Profile 1.0
  - Describes the management and configuration of a service processor for a computer system.
    - Computer system may be contained in a single chassis or may comprise multiple chassis or a blade.
  - Covers:
    - Management Controller (MC).
    - Service Processor (SP).
    - Baseboard Management Controller (BMC).
    - Chassis Manager.
  - Includes modeling redundant service processors.
- Service Processor Profile 1.1 adds:
  - Support for PCI device profile.

IP Configuration Profile

- The IP Configuration profile describes an IP network connection and associated IP configuration information in a managed system.
- Functionality within the scope of this profile includes:
  - Settings for IP network connection.
  - Settings for IP versions.
  - Protocol endpoints for IP, a DNS client, and a DHCP client.
- DSP 1036, 1037, 1038 are sufficient to represent IPv4.
- DSP 1116 proposed to cover dynamics of IPv6:
  - Dynamics of IP address assignments.
  - Concurrent settings.
  - Multiple IP address assignments on a network connection.
  - Representation of IP versions.
  - Representation of DNS on a multinetwork system.

IP Configuration Profile Class Diagram



Future SMASH/DASH Specs

- SMASH 2.1 and DASH 1.2 are in progress.
- Inclusion of new and additional profiles.
  - Physical Computer System View
  - IP Configuration
  - Power State Management 2.0
  - Record Log 2.0
  - OS Status 1.1
  - Service Processor 1.1
  - Others under consideration…
- Additional discovery mechanism considered.
  - SLP based
  - Leverage WBEM SLP template

Summary and Call to Action

- Summary
  - DMTF is driving SMASH/DASH standards for server/desktop/mobile platforms management.
  - SMASH/DASH specifications maturing with increased adoption.
  - Updates to SMASH/DASH are in progress.
- Call to action
  - Participate in the SDMP WG.
  - Provide SMASH/DASH implementation feedback.
  - Anticipate SMASH 2.1/DASH 1.2 in the near future.

Q & A

Q & A Session

Thanks to all the members of the SMWG, DMWG, SDMWG, PPPWG, and SDMPWG for their contributions!