Dynamic Provisioning for Mobility:
Mobile and Directory (MaD) Challenge

Catalyst 2003 - San Francisco, CA - July 9, 2003

Chris Apple
MaD Technical Coordinator
Principal Architect
DSI Consulting, Inc.
capple@dsi-consulting.net
http://www.dsi-consulting.com/

Andrea Westerinen
MaD Information Architect
Senior Architect
Cisco Systems
andreaw@cisco.com
http://www.cisco.com/
Agenda

• Introduction: The MaD Challenge Effort (CA)
• Dynamic Provisioning Scenarios (CA)
• Challenge Scenario: Airport/Airplane (CA)
• Project Status (CA)
• MaD Information Model (InfoMod) (AW)
• MaD InfoMod Validation (CA)
• Call for Participation (CA)
The MaD Challenge Effort

• Concept:

• Purpose:
  – Demonstrate through scenarios and a framework the use of directory services to support roaming in a IP-based mobile environment.

• Goals & Objectives
  – Define:
    • a provisioning information model for mobility management
    • operational models for storage and retrieval of dynamic provisioning information
    • contextual usage models for directory services
  – Understand end-user requirements
  – Evangelize a standards-based architectural vision
  – Demonstrate the concept using standards-based technology
  – Build a demo system using technologies commercially available now or near-term
The MaD Challenge Effort (cont.)

• Challenge Partners:
  - THE Open Group
  - DMTF
  - NAC

• Challenge Audience:
  - Enterprises/IT Customers
  - Wireless Internet Service Providers (WISPs)
  - Directory vendors
  - Management infrastructure tool vendors
  - Consulting firms
The MaD Challenge Effort (cont.)

- **Challenge Team:**
  - Chris Apple  
    DSI Consulting/The Open Group
  - Winston Bumpus  
    Novell/DMTF/The Open Group
  - Felix Gaehtgens  
    Symlabs/The Open Group
  - Chris Harding  
    The Open Group
  - Ed Harrington  
    EPH Associates/The Open Group
  - Jim Keeler  
    Wayport
  - Martin Kirk  
    Pegasus/The Open Group
  - Roger Mizumori  
    Waterforest Consulting/The Open Group
  - Mez Morrell  
    Nexor/The Open Group
  - Doug Obeid  
    NAC
  - Pat O’Kane  
    ePresence/NAC
  - Steve Omrani  
    IBM/The Open Group
  - Richard Paine  
    Boeing/NAC/The Open Group
  - Karl Schopmeyer  
    Pegasus/The Open Group
  - Skip Slone  
    Lockheed Martin/The Open Group
  - Gavenraj Sodhi  
    Business Layers/The Open Group
  - Andrea Westerinen  
    Cisco/DMTF
  - Fred Wettling  
    Bechtel/NAC
Dynamic Provisioning Scenarios

- **Customer Relationship Management (CRM):**
  - Sales Force Automation (SFA):
    - Consumer Packaged Goods Field Sales
    - Real Estate Agents
  - Field Service Automation (FSA):
    - Insurance Claim Adjustment
    - In-Home Appliance Repair

- **Travel-Related Services:**
  - IP-based Application Session Roaming
    - Traveling Sales Executive:
      - Office-to-Airport
      - Airport-to-Airplane
      - Airplane-to-Airport
MaD Challenge Scenario

Airport Wireless LAN

- Directory
  - Mobile Device
  - Computer
  - Org Entity
  - Address
  - ISP
  - WISP
  - Policies
  - Switch
  - Router
  - Radio Info
  etc.

- Dynamic Datastore
  - Radio Info
  - Wireless QoS
  - Location

Airplane Wireless LAN

- Directory
  - Mobile Device
  - Computer
  - Org Entity
  - Address
  - ISP
  - WISP
  - Policies
  - Switch
  - Router
  - Radio Info
  etc.

- Dynamic Datastore
  - Radio Info
  - Wireless QoS
  - Location
MaD Challenge Architecture

Airport Infrastructure
- Internet
- Directory
- Dynamic Datastore
- AAA Server
- NOC
  - Infrastructure Management
  - User Administration

Airplane Infrastructure
- Internet (via satellite)
- Directory
- Dynamic Datastore
- AAA Server
- NOC
  - Infrastructure Management
  - User Administration
MaD Design Toolkit

• Defining the interfaces and shared data using standards
  – Address hardware, security, and registration assumptions

• Mediation layer
  – Common Information Model (CIM)
  – Pegasus (XML CIM)
  – Open Group and Open Source

• Use cases, application and information flow analysis

• Databases

• Directories, Virtual Directories, Meta Directories

• Managed WiFi LAN Equipment
MaD Challenge Demo

Gate Counter
Airport AP
Ramp
Directory
Network
Control
Center
Screens
Network
Chairs
Main
Screen
Airline AP

 dsicfzi.png
THE Open GROUP... working for interoperability

NAC
DMTF
distributed management task force, Inc.
Cisco Systems
MaD Challenge Project Status

• Concept, Purpose, Goals, & Objectives Defined
• High-Level Architecture Completed
• Preliminary Demo Planning Completed
• Information Model (InfoMod) Drafted
• InfoMod Validation Testing In-Progress
• Detailed Architecture/Design Commencing
MaD Information Model Overview
Why CIM?

- Internet- and enterprise-wide management
  - Wide breadth of objects + repository independent
  - Unifies and extends existing standards (MIBs, X.500, M.3100, …)
- OO design
  - Abstraction, inheritance, ability to “classify”, extensibility via subclassing
  - Well-defined “locations” and usage semantics for classes and associations
- Associations depict relationships
  - Dependencies, topologies, aggregations, scoping, …
- “Standard”, inheritable methods
CIM on the Wire and in the Directory

- “Web-Based Enterprise Management” (WBEM) and “Directory Enabled Networking” (DEN)
- CIM to present and organize data
- Use of XML and HTTP, SOAP, LDAP, DSML and/or other web technologies

Data Description

CIM

HTTP

LDAP Directory

LDAP/DSML

DBEM Transport Encoding

LDAP Directory

DEN Mapping + Repository

LDAP/DSML

DEN Access

<xmlCIM>

Dsi Consulting, Inc.

THE Open Group

NAC

DMTF

Cisco Systems
How Is CIM Defined?

- MOF - Managed Object Format (ASCII or Unicode)
  - Human and machine readable definition of the classes
  - Format: Class “qualifiers” (meta-data), name and superclass / Property “qualifiers”, datatype and name / Method name, return code, “qualifiers” and parameters
  - http://www.dmtf.org/standards/cim_schema_v27.php

- UML - Unified Modeling Language diagrams
  - Rendered using VISIO and also translated into PDF

- Whitepapers
MaD InfoMod: DMTF CIM Profile

// Qualifiers to define class, property and method "meta-data"
#pragma include ("Core27_Qualifiers.mof")

// Core classes as the “top of the tree” – Most are abstract
// ManagedElement, Dependency/ConcreteDependency,
// Component/ConcreteComponent, ManagedSystemElement,
// LogicalElement, EnabledLogicalElement, System, AdminDomain,
// SystemComponent, Service, HostedService, ServiceComponent,
// ServiceServiceDependency, ServiceAvailableToElement,
// ServiceAccessPoint, RemoteServiceAccessPoint, RemotePort,
// HostedAccessPoint, ServiceAccessBySAP, SAPSAPSAPDependency,
// ActiveConnection, ProtocolEndpoint, BindsTo,
// SettingData, Profile, ElementSettingData and ElementProfile
// (from Core27_CoreElements.mof)
#pragma include ("MaD_Core.mof")
Describes physical location, locations within “larger” perspectives (ContainedLocation), packaging (instantiate Card and Chassis) and the containment of cards in a chassis (via the Container association). To tie the physical packaging to a system, use the SystemPackaging association.
MaD InfoMod: DMTF CIM Profile

// Miscellaneous - Logical information:
//   SoftwareIdentity (from Core27_Software.mof),
//   ComputerSystem (from System27_SystemElements.mof), and
//   LANEndpoint and IPProtocolEndpoint (from
//   Network27_ProtocolEndpoints.mof)
// New subclass of SettingData - ChallengeUserPreferences
#pragma include ("MaD_Logical.mof")

Describes basic software assets/inventory, general ComputerSystems (tied to a location using the ElementLocation association in the Physical MOF), and the Ethernet LAN and IP Endpoints in use

Also, the challenge-specific setting, DHCP and wireless classes will be included in this MOF
MaD InfoMod: DMTF CIM Profile

// WBEMService, ObjectManager,
// ObjectManagerCommunicationMechanism,
// CIMXMLCommunicationMechanism,
// CommMechanismForManager,
// Namespace, SystemIdentification, NamespaceInManager, and
// SystemInNamespace (from CIM_Interop27.mof)
// New classes – DirectoryService and
// DirectoryCommunicationMechanism (LDAP, DSML or both)
#pragma include ("MaD_Interop.mof")

Data provided by Pegasus and minimal information about the directories in the challenge
Identities are instantiated based on some or no credentials. If we want to use credentials (such as a boarding pass), reviewing these and entering OK in an application could cause the Identity’s TrustEstablished boolean to be True. Use the AssignedIdentity association to tie the Identity to real Person.
MaD InfoMod: DHCP Schema

Service

[Core Model]

Associate to Settings and PolicySets for address and option assignment

DHCPService (New)

ProtocolEndpoint

[Core Model]

DHCPAddress (New)

ServiceManagesAddress

Subclass of Dependency

Name: string {=IP Address}
AddressState: uint16[] {enum = Unknown, Other, Reserved, Free, Active, Assigned, Unassigned, Not Assignable, Expired, Released, Reset, Abandoned, Backup}
ExpirationTime: datetime
StartTimeOfState: datetime
LastTransactionTime: datetime
SetByBootp: uint16 {enum = Unknown, T, F}

AddressLease

0..1

ComputerSystem

Associate to Settings regarding DomainName sent to client, configured to update DNS, ...

Can instantiate LogicalIdentity relationship between DHCPAddress on the server and the IPProtocolEndpoint on the client

In MaD_Logical.mof
MaD InfoMod: Wireless Schema

NetworkPort (Device Model)
- Speed
- MaxSpeed
- PortType
- LinkTechnology
- ...

WirelessPort (New)
- SignalStrength: {Percentage}
- RoleClass: uint16 {enum = Unknown, Other, Client Station, Repeater, Access Point, Bridge Host, Bridge, Bridge Root}

SystemModel

ProtocolEndpoint
- [Core Model]

ComputerSystem
- [System Model]

WirelessLANEndpoint (New)
- Name: string {MacAddress}
- WEPEnabled: uint16 {enum = Unknown, T, F}
- WEPKeyMixEnabled: uint16 {enum = Unknown, T, F}
- SSID: string
- ...

ActiveConnection

In MaD_Logical.mof
MaD InfoMod Validation
MaD InfoMod Testing

Early Stage Testing:

• Baseline LDAP Data Interchange Format (LDIF) file with LDAPv3-compliant schema elements

• Tweak LDIF files as needed for various LDAPv3 server implementations

• Target directory platforms for loading schema:
  – IBM Directory Server 5.1
  – iPlanet Directory Server 5.1 SP2
  – Microsoft Active Directory (W2K Server, Windows Server 2003, ADAM Beta)
  – Novell eDirectory 8.7
  – OpenLDAP 2.1.21
  – OctetString Directory Server Express 2.0.1
MaD InfoMod Testing (Cont.)

Next Steps:

• Develop LDIF files with entries compliant with the MaD Schema
• Load entries into various LDAPv3 directory servers
• Test search/retrieval capabilities
• Set up managed WiFi LAN equipment
• Use virtual directory, meta directory, and/or directory server replication technologies to automate dynamic provisioning of directory information
  – from WiFi equipment through management interfaces
  – associated with:
    • identity and identity assertions
    • hand-offs of authentication credentials and authorization assertions
Call for MaD Participation

• Near-Term Activities:
  – MaD InfoMod validation testing
  – Detailed architecture/design
  – Demo system development, integration, and testing

• MaD Project Team Needs:
  – END USER REPRESENTATION
  – Wireless Roaming Business Model Input
  – Wireless Roaming Billing, Accounting, and Settlement Input
  – Additional Wireless Communications Equipment Vendor Participation
Questions?

- Contact information after the session:
  - Chris Apple  capple@dsi-consulting.net
  - Andrea Westerinen  andreaw@cisco.com