



IF-MAP and GENI

Richard Kagan – Infoblox



- **Define data models for objects**
 - Devices, aggregates, slices, experiments, measurements, ...

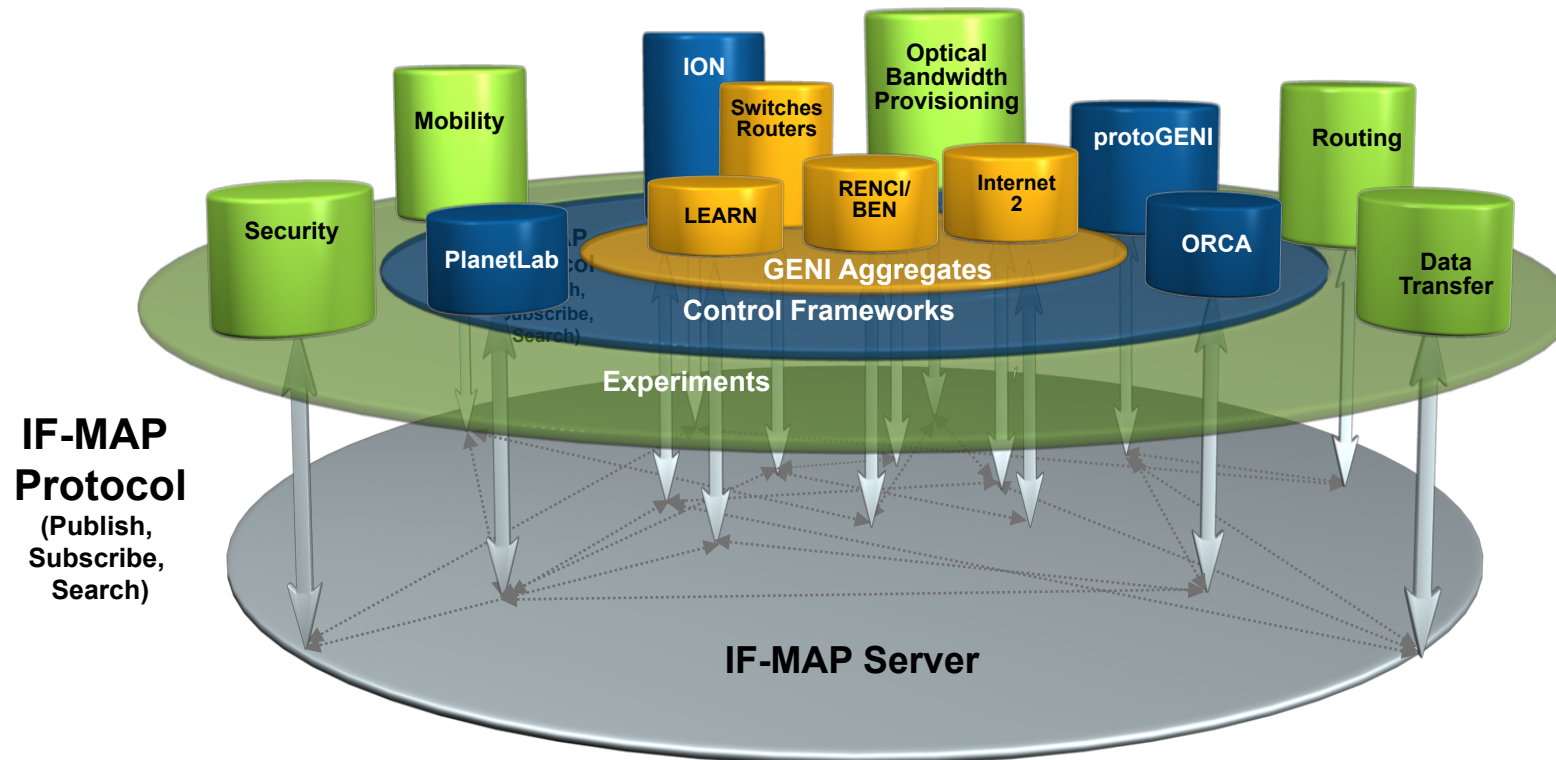
- **Create associated schemas**

- **Enable data sharing at varying levels of scale**
 - Within & across slices, aggregates, control frameworks, etc.

- **Accommodate a number of desired characteristics, e.g.:**
 - Expressive, extensible modeling language
 - Frequent/rapid schema changes
 - Scalable and real-time
 - Message bus *and* database services
 - Multi-layer security (authentication, authorization, transport security, etc.)
 - Easy to implement & debug
 - Available, tested, supported/supportable code

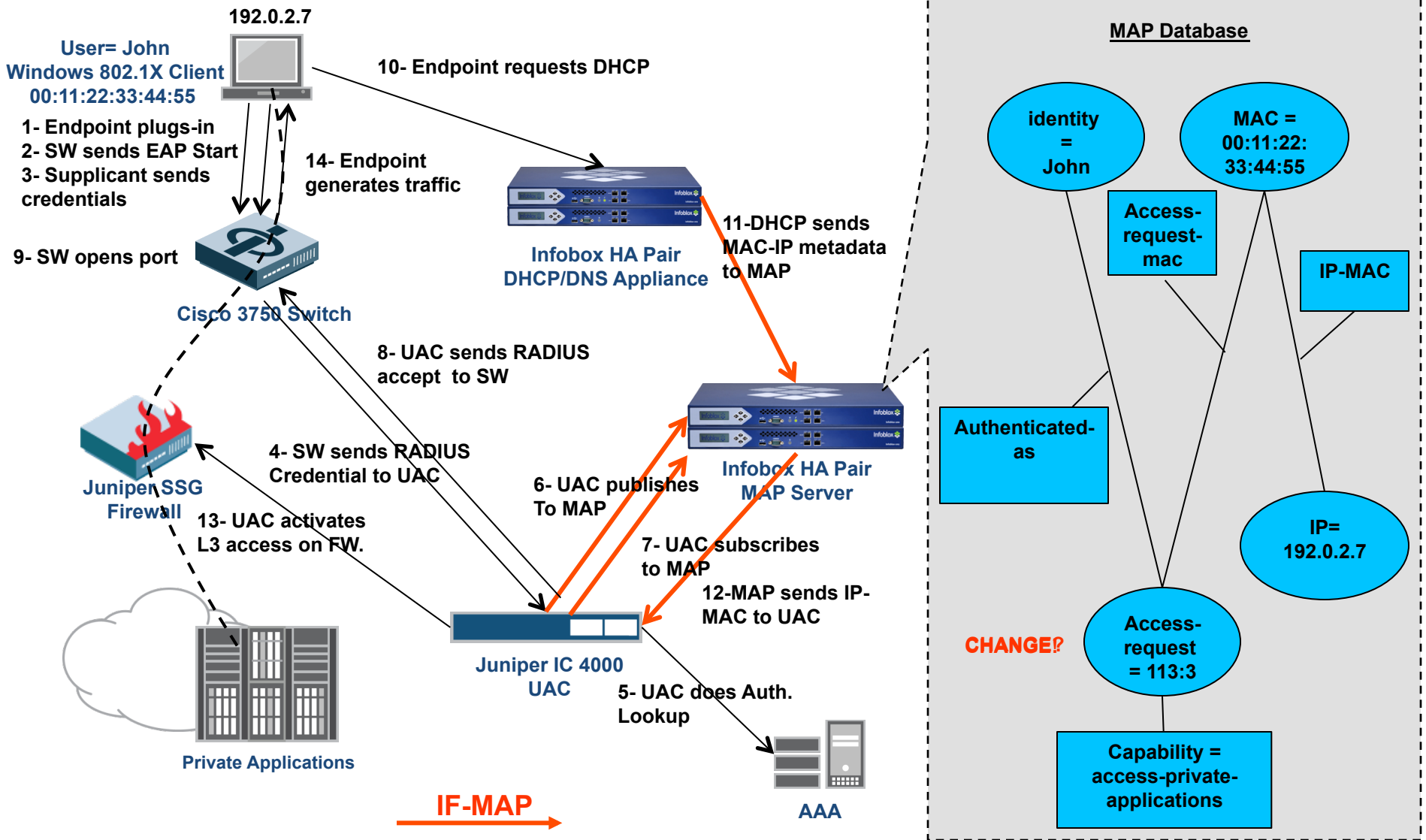
- **IF-MAP = “Interface to Metadata Access Point”**
 - Open standard published by the Trusted Computing Group (TCG)
- **Version 1.0 released in 2008, 1.1 in 2009, 2.0 in 2010**
- **Key features:**
 - Client/server protocol, very lightweight client
 - Pub/sub paradigm, with or without persistence (e.g. bus and database)
 - Eliminates the need for polling = real time, scalable
 - All objects & metadata expressed as XML documents
 - Current binding is to SOAP/HTTPS; Other bindings supported (e.g. SOAPless)
 - Graph structure with automatic correlation
 - No pre-defined global schema
 - Federation, authorization,
- **Available in open-source and commercial implementations**
 - Used in production today (Boeing, LANL, Deutsche Bank, etc.)

IF-MAP Could Address a Number of GENI Use Cases



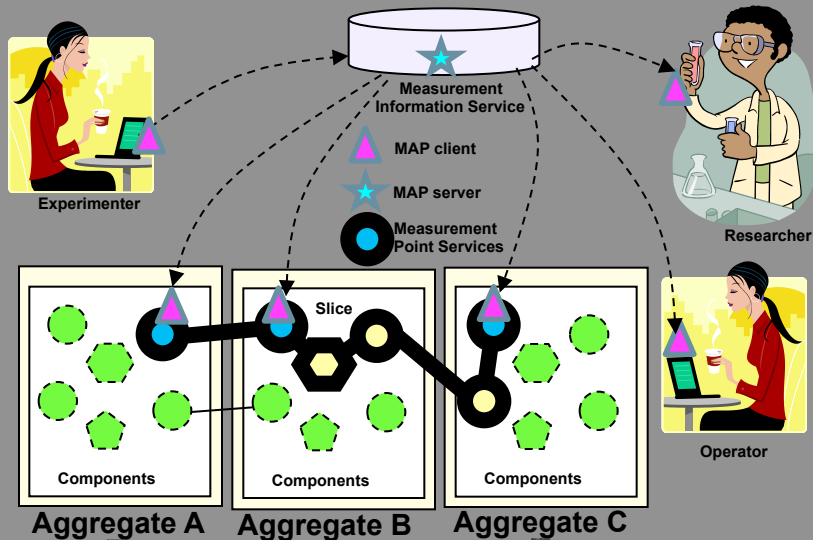
Possible Use Cases: GENI Clearinghouse, Measurement Information Service , GMOC Interface ...many more

A Network Security Use Case: Dynamic, Policy-Based Access Control for Unmanaged Endpoints



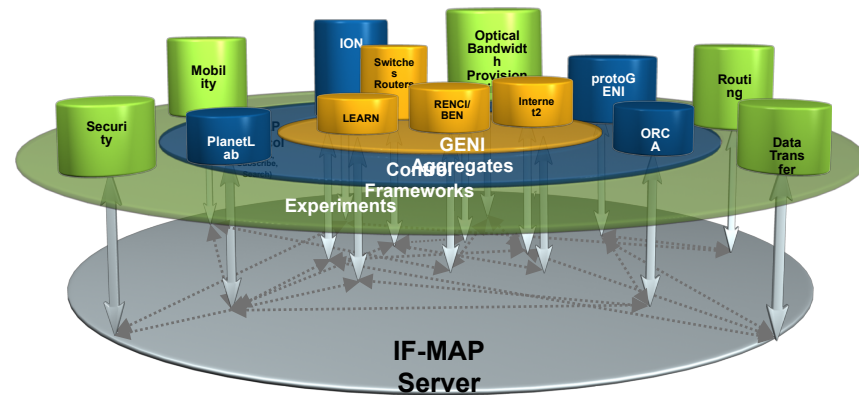
Preview of Tonight's Demo: MDOD Repository for I&M

I&M WG EXPERIMENTER USE CASE



IF-MAP

Open protocol standard published by the Trusted Computing Group
Pub/sub database - Like Facebook for IP devices and systems



Automatically aggregates, correlates, and distributes data to and from different systems, in real time

IF-MAP Server may be: GENI Clearinghouse / Measurement Information Service / Measurement Data Archive Service / Measurement Analysis and Presentation Service ...many more

EXPERIMENTER

Start experiment, publish initial MDOD on MAP server

Update/Publish MDOD by Measurement Point Service to MAP server

Delete all MD at MAP server

OPERATOR

Modify MDOD schema: extend attributes and metadata

Subscribe to MDOD

Modify MDOD schema: add any number of attributes

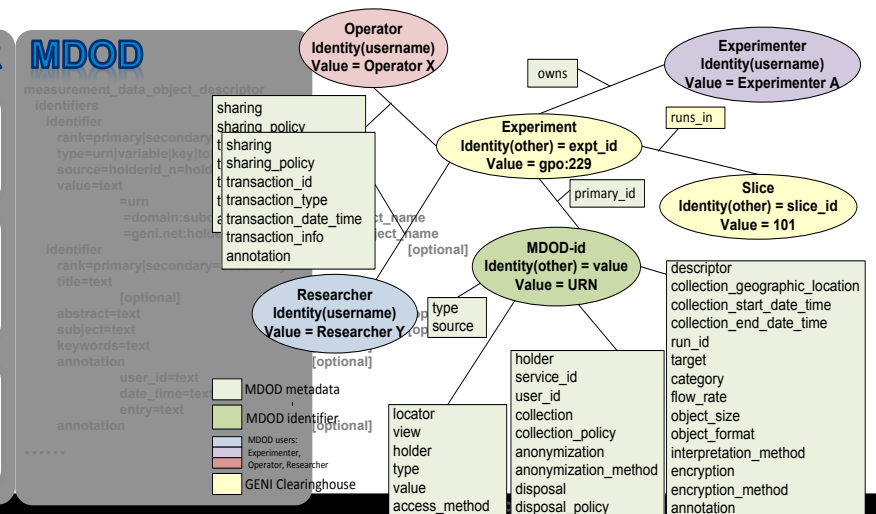
RESEARCHER

Subscribe and/or search MDOD

Persistent query on MDOD updates

Search MDOD with filter options

MDOD





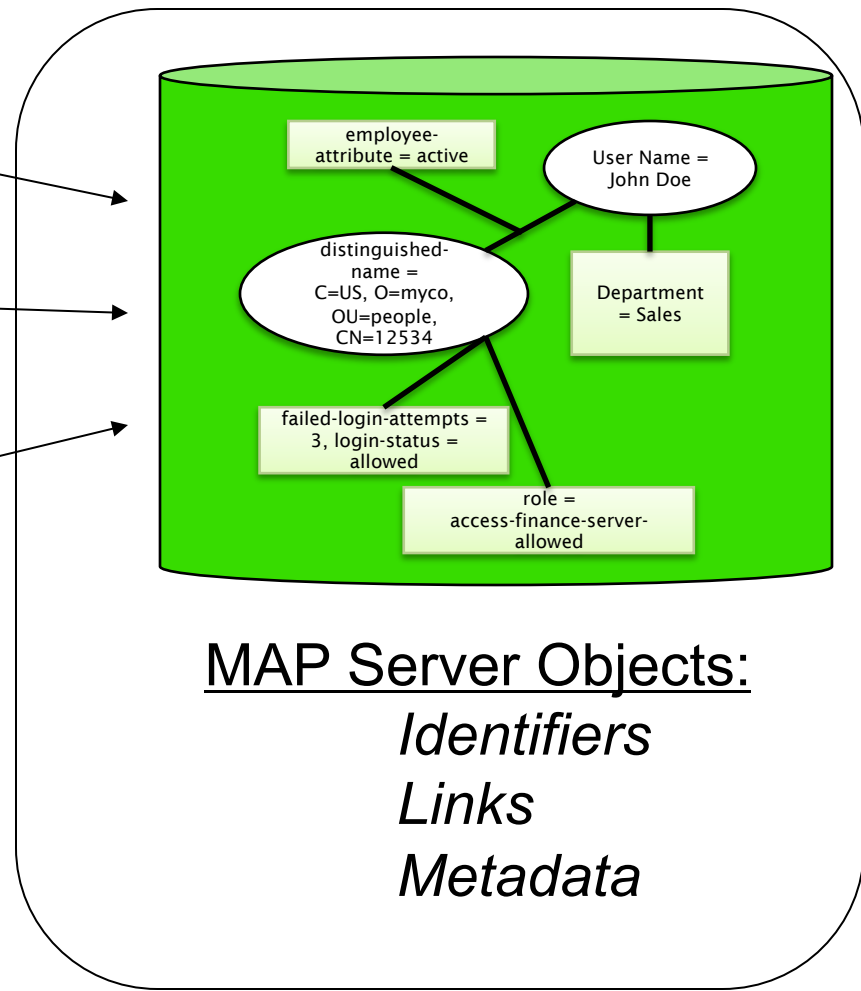
IF-MAP Technology Overview



IF-MAP Client(s)



IF-MAP Server



- **Publish:**

Tell others that...<metadata...>

- Clients store metadata into MAP for others to see
 - Example: Authentication server publishes when a user logs in (or out)

- **Search:**

Tell me if...*match*(metadata pattern)

- Clients retrieve published metadata associated with a particular identifier and linked identifiers
 - Example: An application can request the current physical location of the user

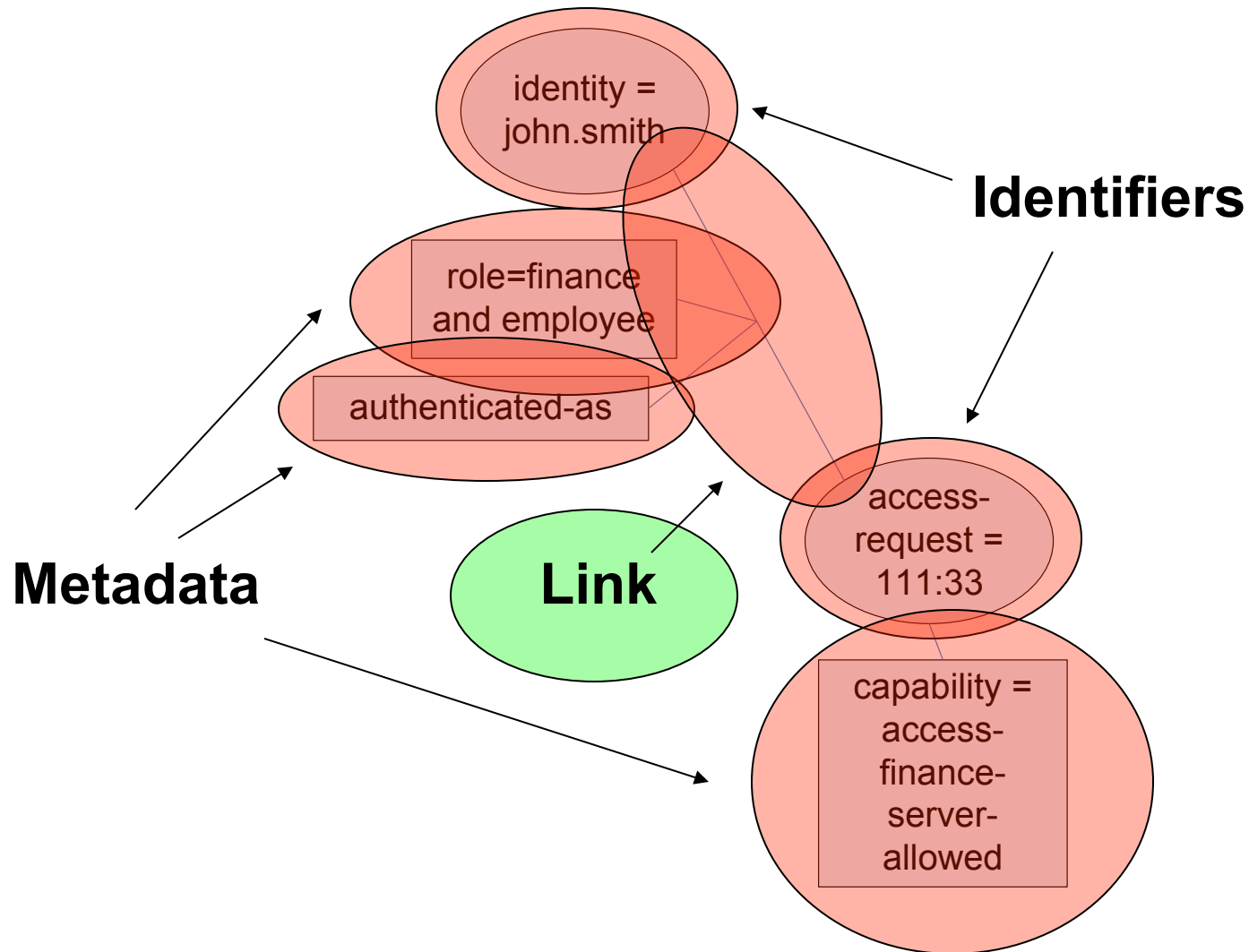
- **Subscribe:**

Tell me when...*match*(metadata pattern)

- Clients request asynchronous results for searches that match when others publish new metadata
 - Example: Tell me when any user's status goes from "employee" to "terminated"

- ***Notify (a special case of 'Publish'):**

- Clients publish metadata, usually transient events, that are not stored in the MAP database (but they trigger subscriptions – like a message bus)

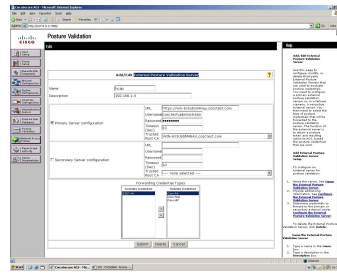


Today, Systems Share the IP Network, But Don't Share Data

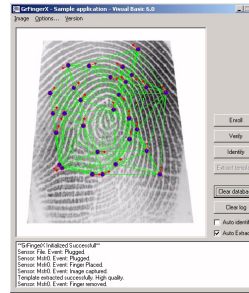


**Provisioning,
Visualization &
Analytics
(Management)**

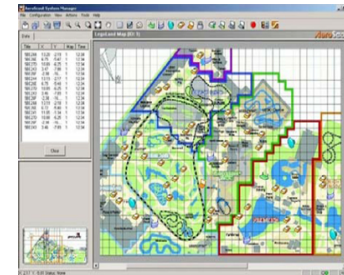
Network Security



Physical Security



Network Location

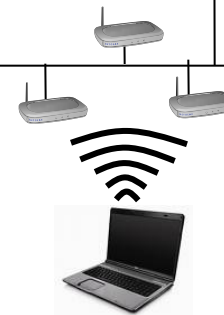


...

**Decisions
(Control)**



**Sensors &
Actuators**



IF-MAP Doesn't Replace Existing Systems & Applications – It Enables Them to Easily Share Data

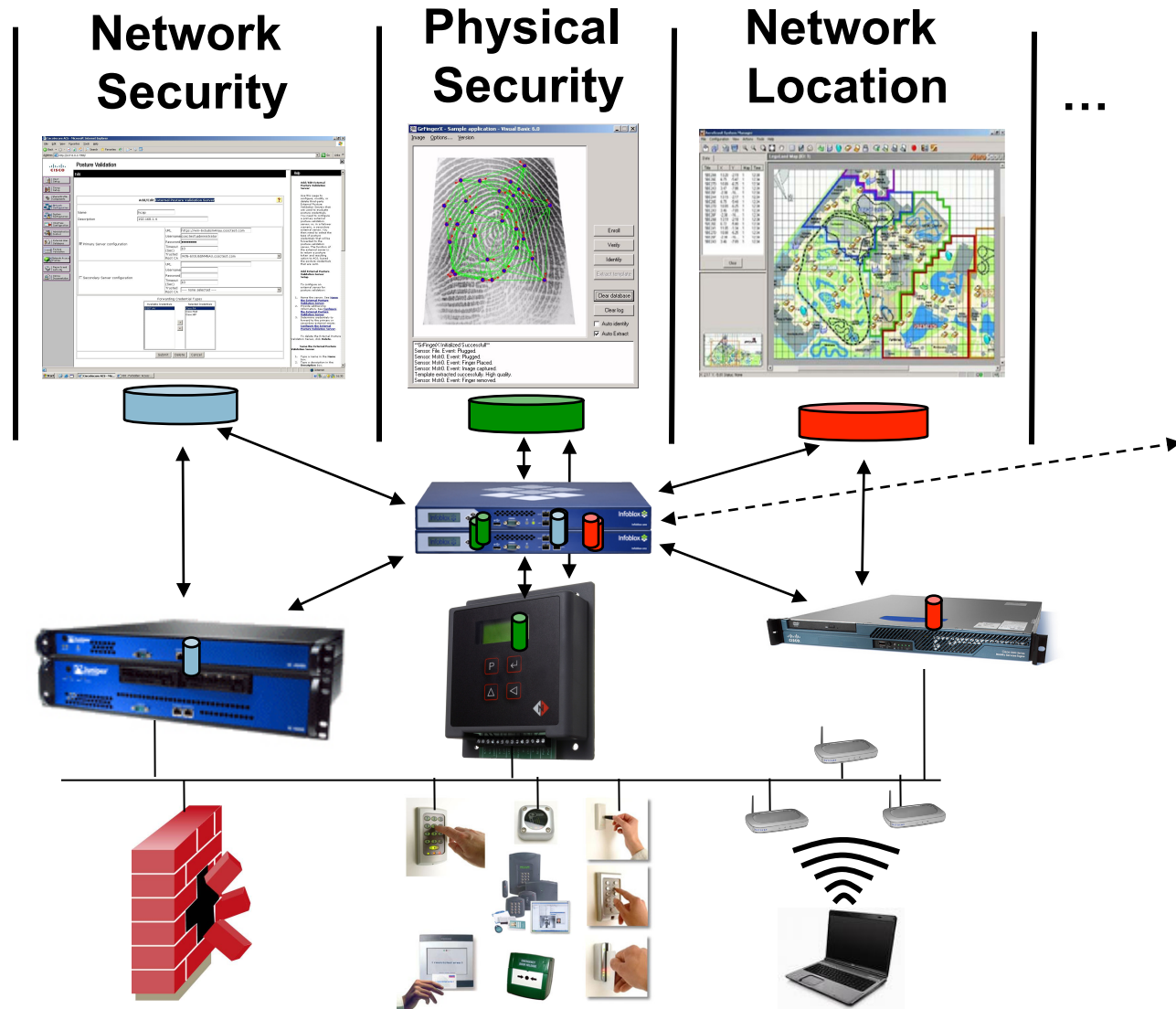


**Provisioning,
Visualization &
Analytics
(Management)**

IF-MAP Server

**Decisions
(Control)**

**Sensors &
Actuators**



Vendor and Open Source Support for IF-MAP is Growing

Vendor	Product/ Function	IF-MAP Client	IF-MAP Server	Avail
Byres Security	SCADA Security	X		Now
Enterasys (Siemens)	Network Access Policy Engine	X		Now
Great Bay	Endpoint Discovery & Behavior Detection	X		Now
Hirsch Electronics	Physical Access Control	X		Now
Infoblox	DHCP Server (NIOS), Infoblox NCCM (NetMRI)	X		Now
Infoblox	MAP Server (IBOS)		X	Now
Juniper	Infranet Controller (Policy Server)	X	X	Now
Logisense	Registration Portal, Billing System	X		Now
Lumeta	Network Discovery & Leak Detection	X		Now
Mikado	NAC Solution	X		H2-11
NCP	VPN Client	X		Now
Open Source	IF-MAP Client Stacks (PERL, C++, java)	X		Now
Open Source	IF-MAP Server (Omapd, Irond)		X	Now
Open Source	VMware/IF-MAP Bridge	X		Now
Open Source	SNMP/IF-MAP Bridge	X		Now
Q1 Labs	SIEM	X		H2-11
Tripwire	Security & Compliance Automation	X		H2-11

▶ **Additional vendors are working with IF-MAP (e.g. Arista, Aruba, ...)**

CONFIDENTIAL

Dynamic Network Security Use Cases in Fed, Finance and Manufacturing Verticals are Driving Adoption

CUSTOMER	SOLUTION	NOTES
Boeing	SCADA Security (in production)	Auto configuration of security gateways collapses two separate networks to one
Cosmopolitan Hotel & Casino, Las Vegas	Differentiated network services for visitors & guests (in production)	Dynamic firewall config per user/guest enables more chargeable services, greatly reduces CAPEX and OPEX
Deutsche Bank	Secure Desktop on Demand (pre-production pilot)	Dynamic firewall config supports consumerization of IT & de-perimeterization of the datacenter
Los Alamos National Labs	Dynamic network access control	Separation of Red, Yellow and Green networks
NSA	Trusted Computing Solutions (Solution Showcase)	Comply-to-connect, LAC/PAC integration, inter-agency data sharing
General Dynamics, CACI, DiData	Security Solutions (IF-MAP Practice)	Network access control, leak detection, LAC/PAC



IF-MAP is Being Actively Pursued in Key Academic & Commercial Research Programs

ORG	FUNCTION	PROGRAM
JANET	ISP for higher-Ed & research in UK; 650 orgs, 2 million subs	Federating user authentication status across independent organizations (pilot)
ESUKOM	German-government funded project studying impact of smartphones on enterprise security	Detecting and mitigating smartphone security threats; Implemented IF-MAP client for Android (pilot)
GENI	NSF-funded research program for next generation Internet, 20+ participating institutions	University of Houston - Using IF-MAP for measurement metadata and as a cross-cloud registration system (active research project)
ONF	Non-profit org founded in 2011 by Deutsche Telekom, Facebook, Google, Microsoft, Verizon, and Yahoo; Pushing standards for Software Defined Networks (SDN) using OpenFlow	IF-MAP proposed for fundamental infrastructure component for SDN (active research project)

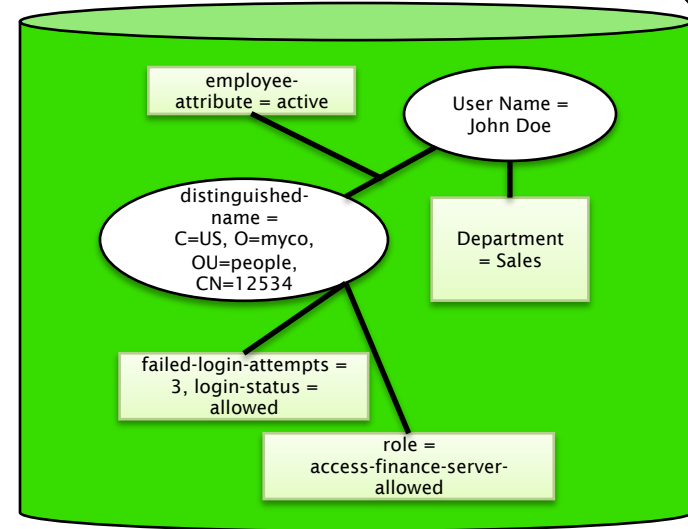
IF-MAP Client(s)



IF-MAP Client Operations:

Publish
Subscribe
Search

IF-MAP Server



MAP Server Objects:

Identifiers
Links
Metadata

- **Publish:**

Tell others that...<metadata...>

- Clients store metadata into MAP for others to see
 - Example: Authentication server publishes when a user logs in (or out)

- **Search:**

Tell me if...*match*(metadata pattern)

- Clients retrieve published metadata associated with a particular identifier and linked identifiers
 - Example: An application can request the current physical location of the user

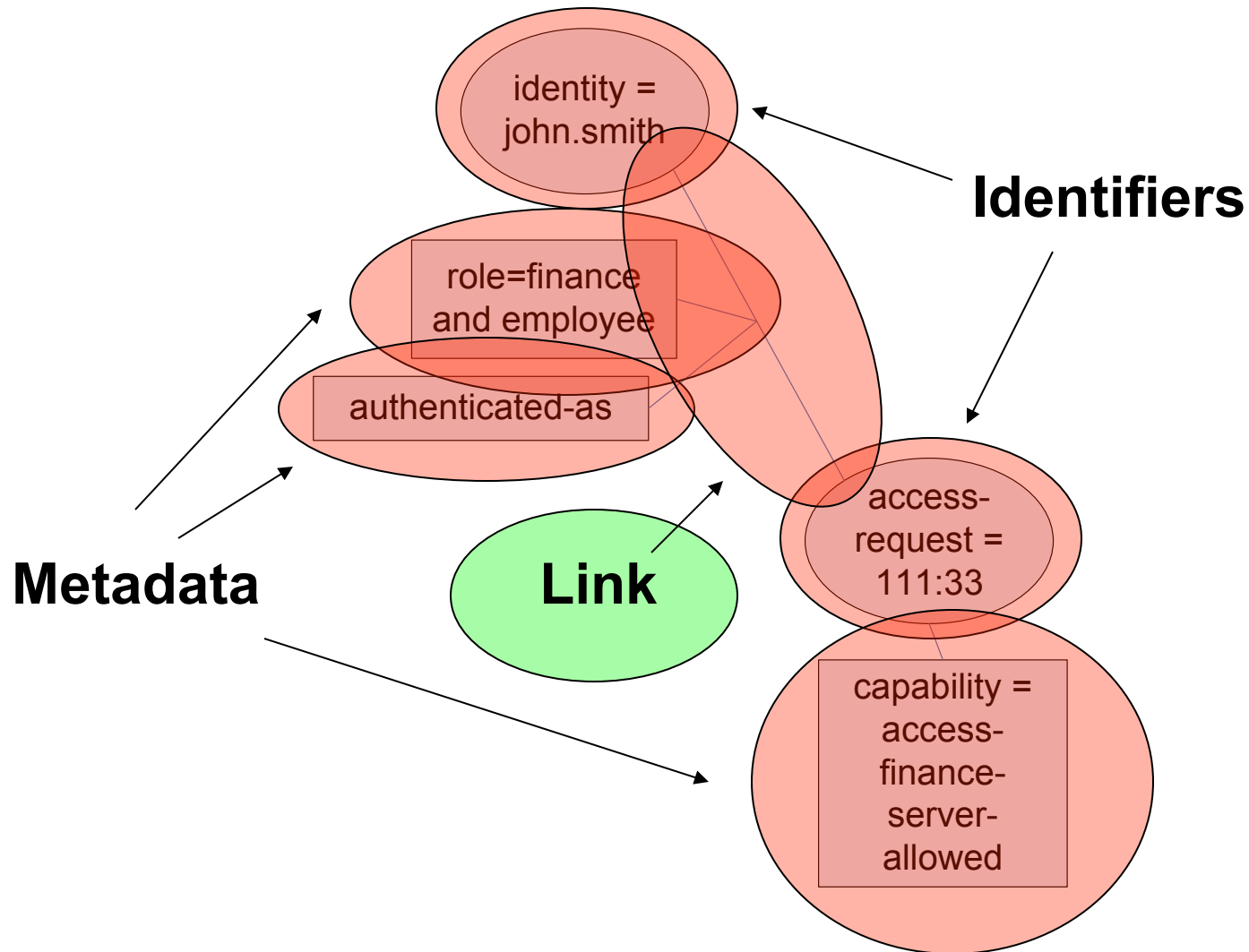
- **Subscribe:**

Tell me when...*match*(metadata pattern)

- Clients request asynchronous results for searches that match when others publish new metadata
 - Example: Tell me when any user's status goes from "employee" to "terminated"

- ***Notify (a special case of 'Publish'):**

- Clients publish metadata, usually transient events, that are not stored in the MAP database (but they trigger subscriptions – like a message bus)



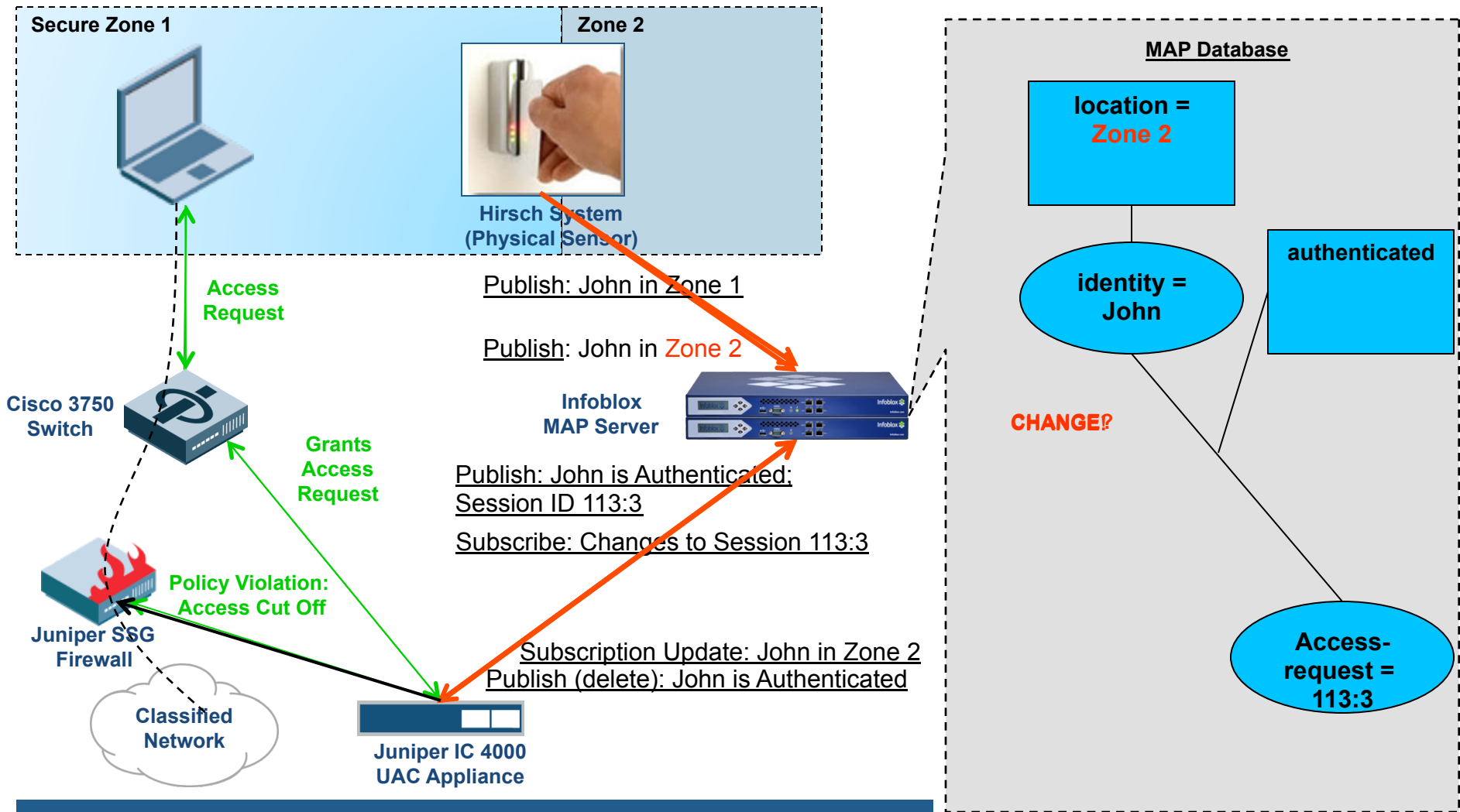
- **The official TCG standard is divided into two categories:**
 - IF-MAP “Base Protocol” (only one spec)
 - IF-MAP Metadata for <XXX> (where XXX=some industry or use case)
- **The Base Protocol specifies basic IF-MAP operations:**
 - Publish, Subscribe, Search, Session Management, etc.
 - Also defines the 5 standard Identifier Types:
 - Identity (i.e User – 12 different possibilities including email address, FQDN, Kerberos principal, etc.)
 - IP Address (v4 or v6)
 - MAC address (AA:BB:CC:DD:EE)
 - Access Request (Authenticator ID, Flow ID)
 - Device (ASCII String)
- **Metadata specs are published independently from the Base Protocol**
 - Today, one spec has been published: IF-MAP Metadata for Network Security 1.0
 - Others are in process:
 - IF-MAP Metadata for Industrial Control Systems
 - IF-MAP Metadata for Trusted Multitenant Infrastructure (i.e. Clouds)
 - Any vendor, customer or industry group can define their own metadata

- **Any compliant IF-MAP server will accept user-defined metadata**
 - All that is required is a unique name within a specified namespace, and conformance with a few simple rules (number of attributes, length, etc.)
 - IF-MAP server will support all operations: publish, subscribe, search, notify
 - No need to configure IF-MAP server to support custom metadata
- **Some examples of user and industry-defined metadata**
 - Student ID (for University XYZ)
 - Asset tag number (for company ABC)
 - Software Version # (for vendor PQR)
 - Operating Parameters 1,2,3,4,.... (for product PPP)
- **If an industry group agrees, they can submit metadata definitions to the TCG for publication as “IF-MAP Metadata for <My Industry>**
- **No need to wait for TCG ratification to use custom metadata**
- **This is a VERY powerful feature of IF-MAP**



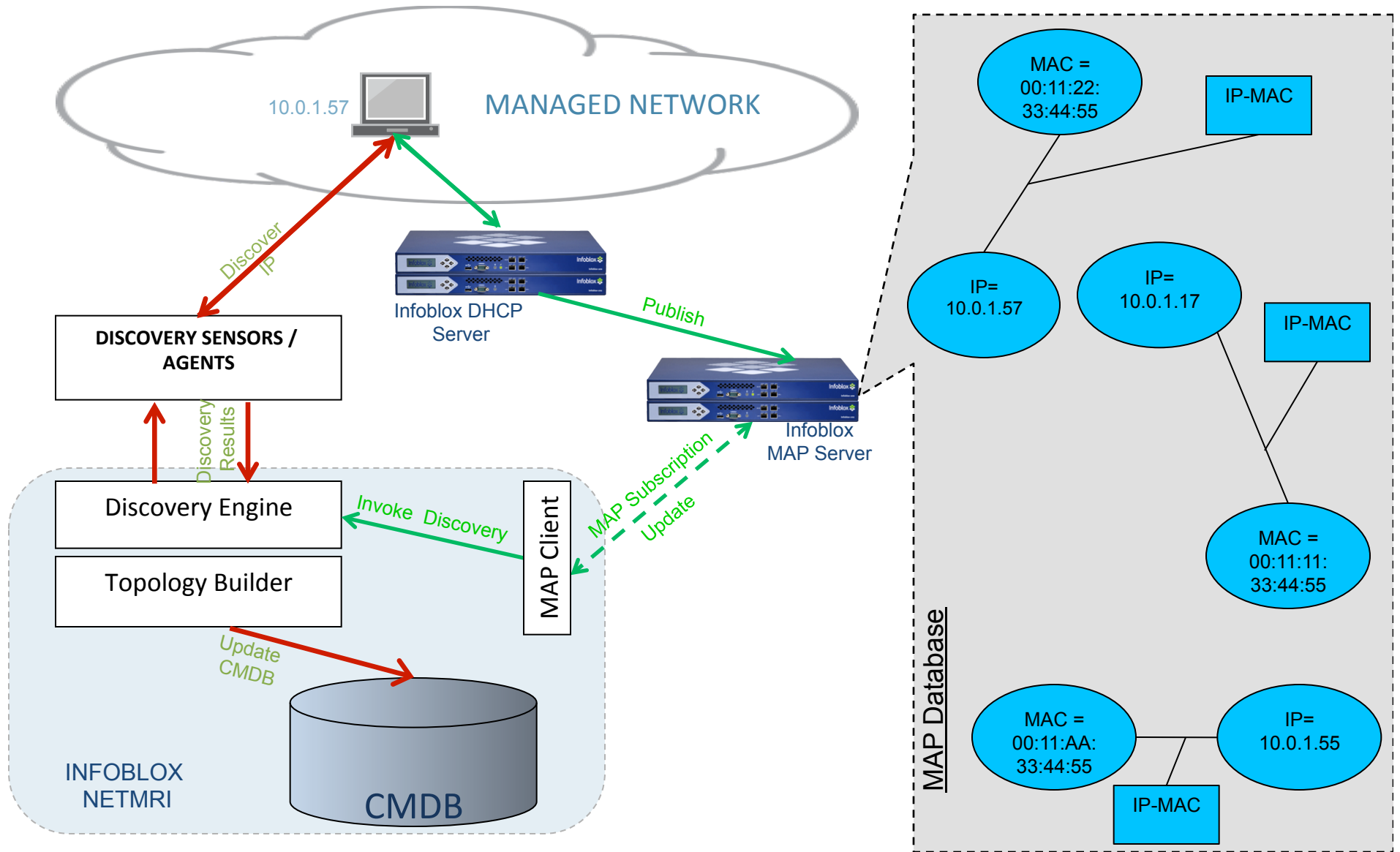
IF-MAP Sample Use Cases

Use Case – Integrated Network / Physical Security Solution

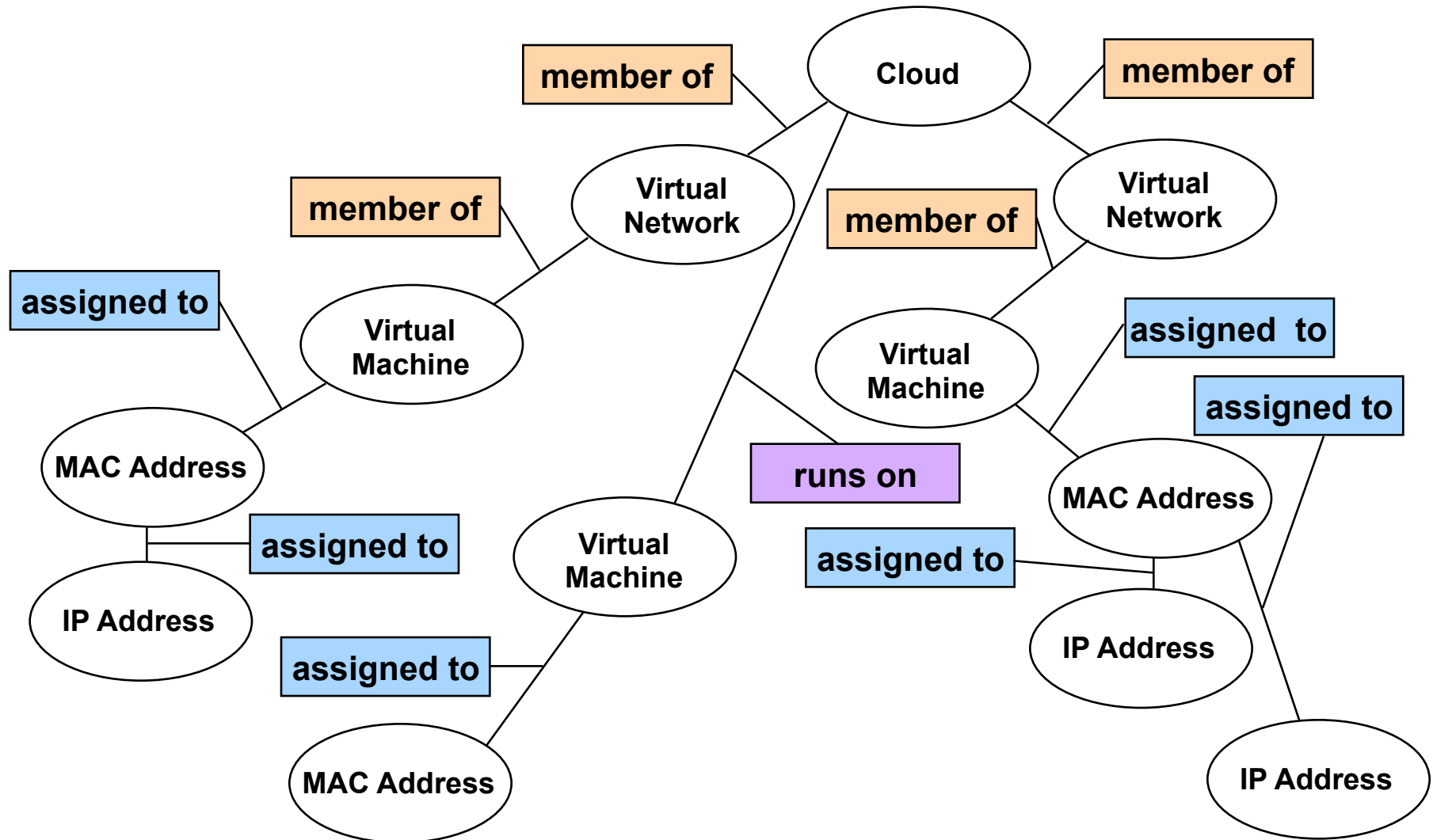


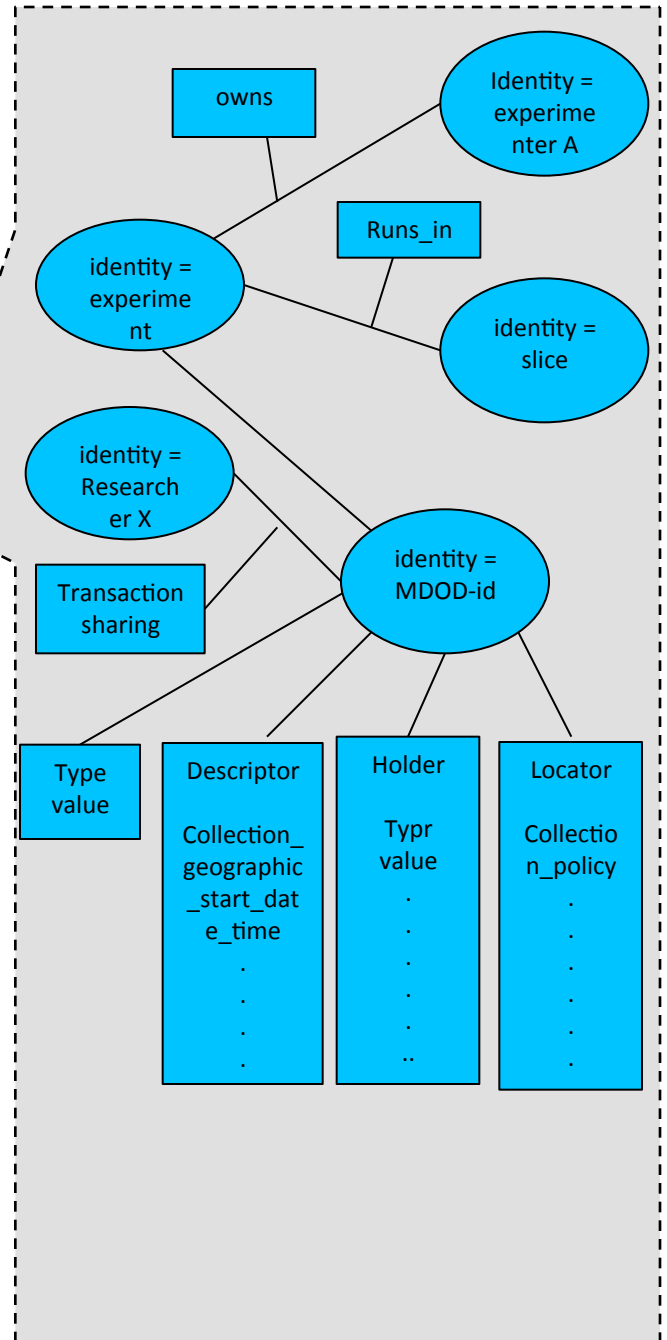
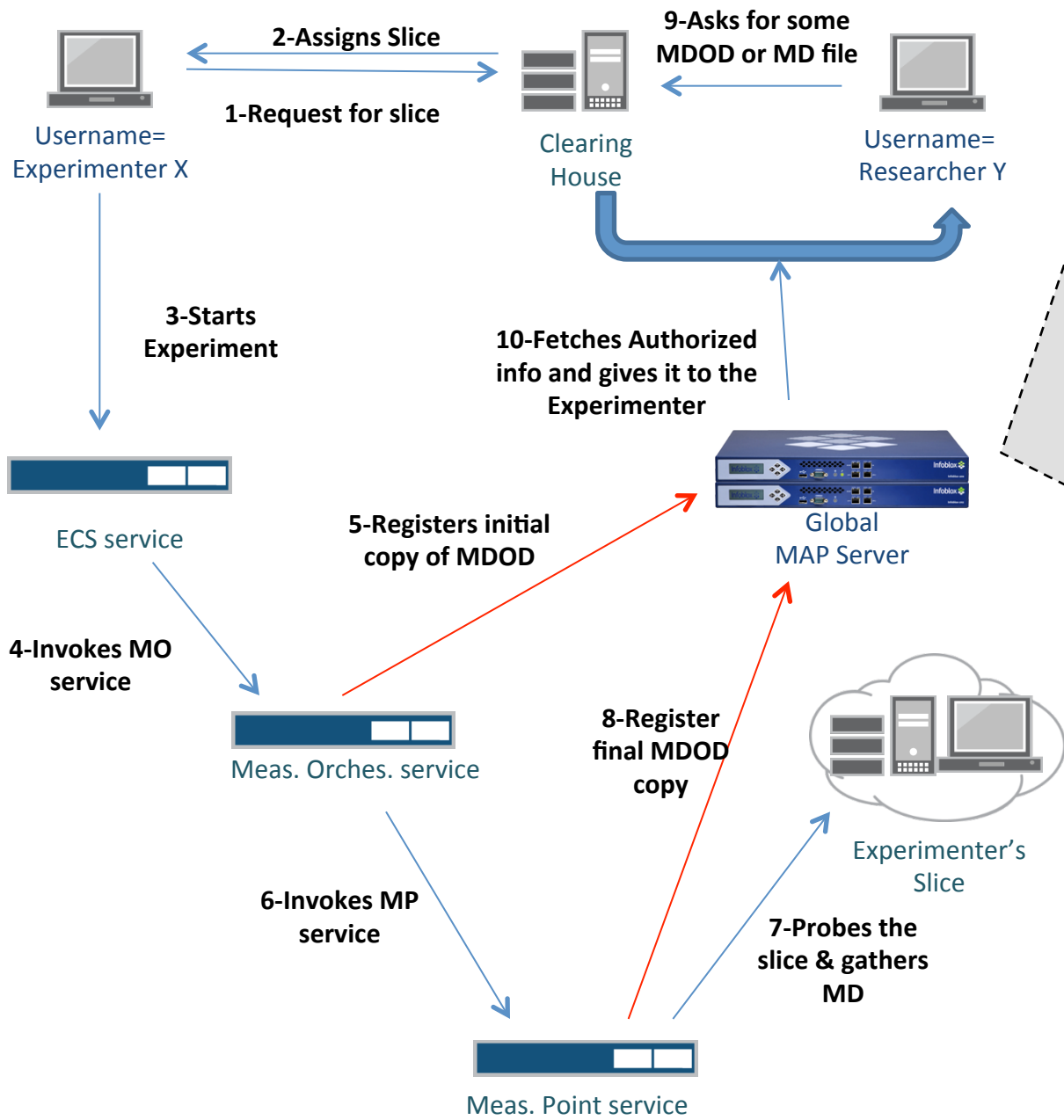
10- MAP updates UAC about the location change

Use Case: Real-Time CMDB



Inter-Cloud Registry Helps Cloud Providers and Users to Match Workload Needs with Cloud Assets



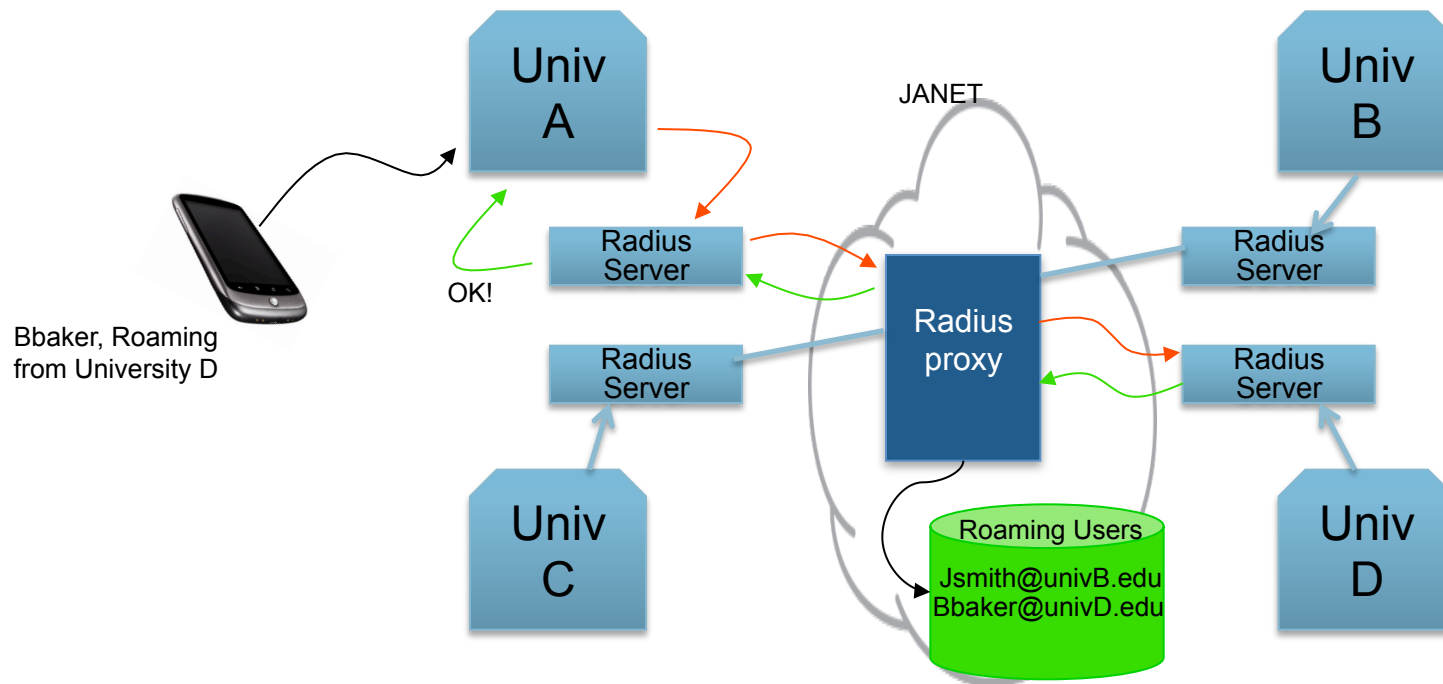


I&M Service Events

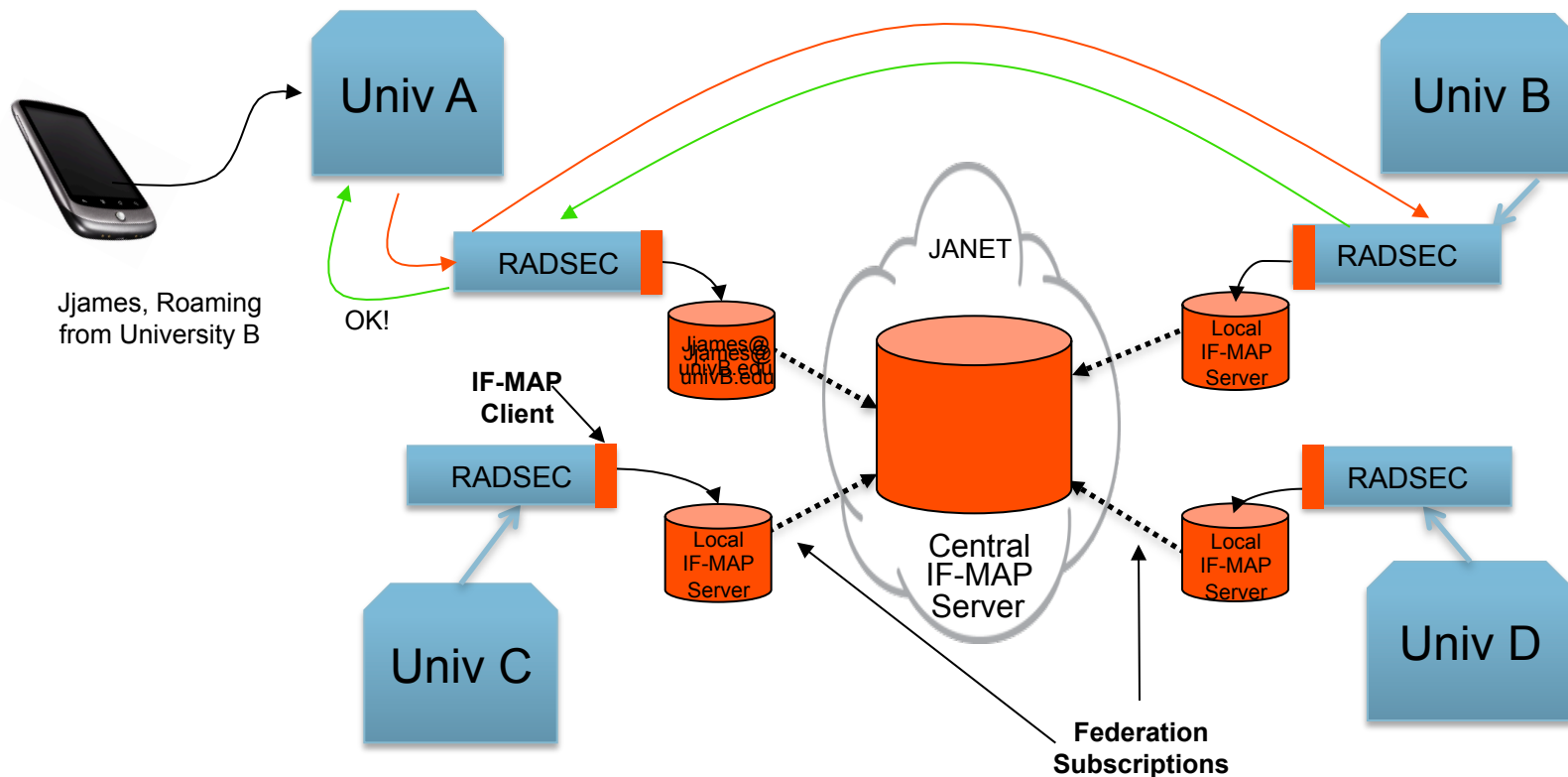
MAP DATABASE

Use Case: Federated IF-MAP Servers for UK EDUROAM Service

- Enables login at remote universities / research centers using home login credentials
- Serves 1.9 million users across 850 locations
- Enabled today using RADIUS Proxy
- Service provider (JANET) maintains database of roaming activity



- Local RADIUS servers replaced by RADSEC servers
 - ✓ RADSEC servers communicate directly – no need for proxy
 - JANET no longer sees RADIUS transactions, no view of who is roaming
- IF-MAP Federation provides a solution:
 - Local RADSEC servers publish user/location data to local MAP server
 - JANET's central MAP server subscribes to changes on university MAP servers



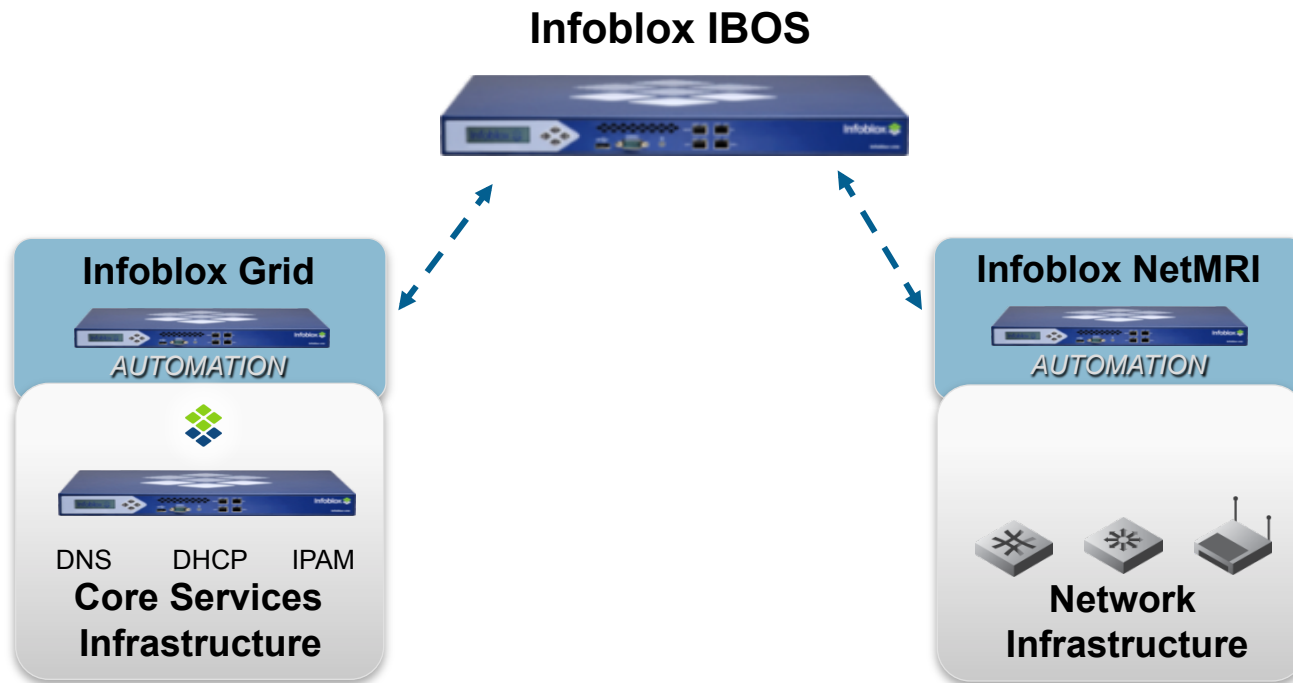


Infoblox IF-MAP Products

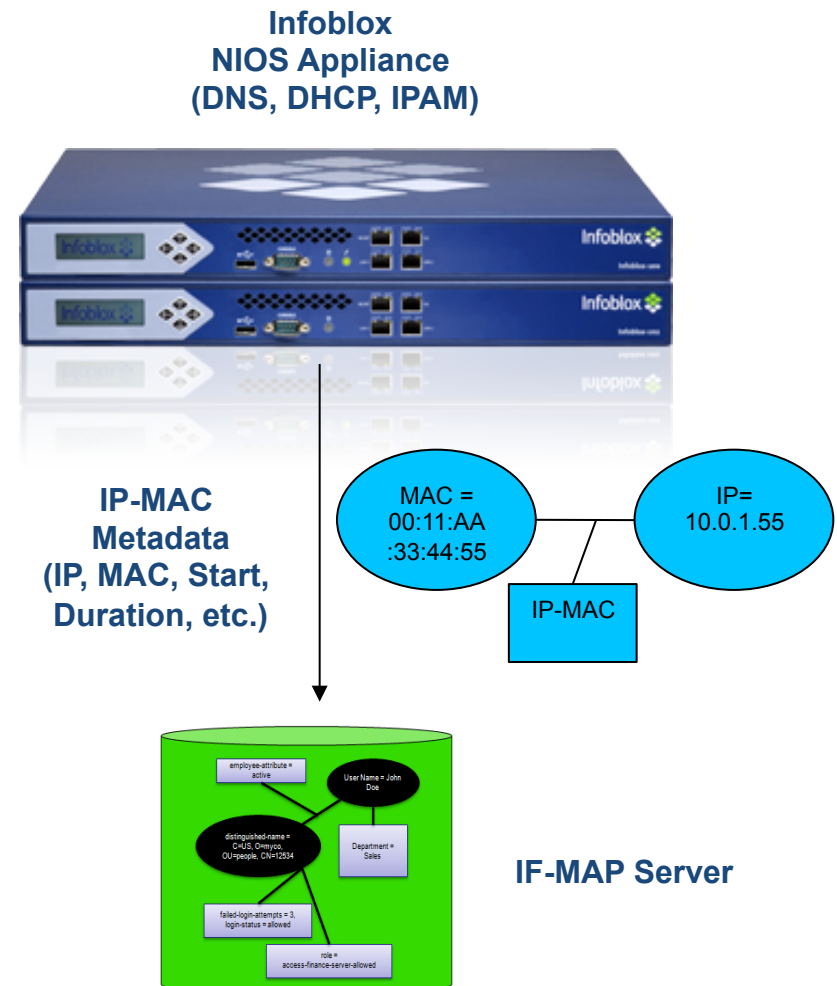


Real-Time Network Automation

Innovation increases network visibility and control

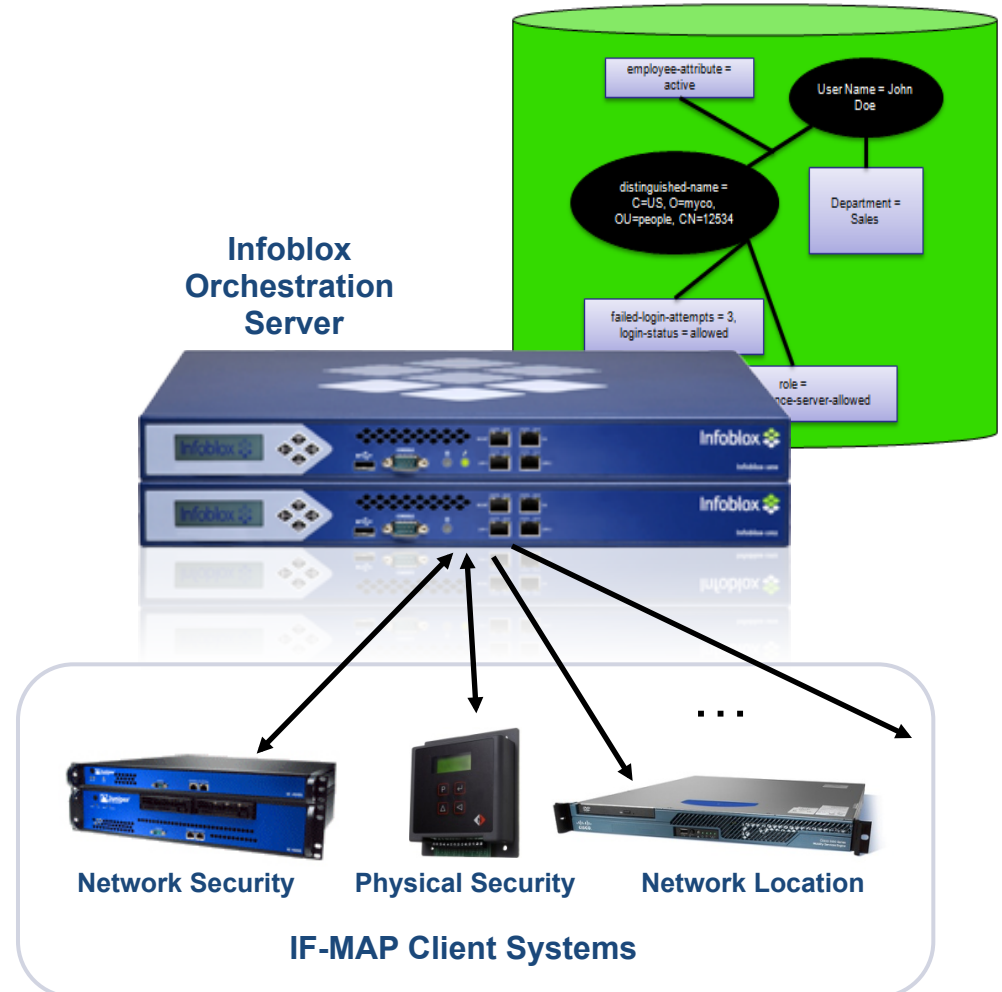


- **NIOS DHCP server dynamically updates IF-MAP server when IPs are allocated, renewed, or released**
- **Config Options**
 - Publish data at Grid/Member level for selected Networks/Ranges
 - Cert based authentication
 - Delete previously published data
- **Publish IPv6 data (NIOS release)**
 - DUIDs
 - MAC addresses extracted from DUIDs
 - IPv6 addresses



Infoblox Orchestration Server (IBOS™) is the World's First Commercial MAP Server Appliance

- ▶ Sold as a series of hardware appliances
- ▶ Also available as VMware software appliances
- ▶ Unique Infoblox capabilities far outstrip any other offerings
 - ▶ 2 patents in process
- ▶ Deployed in production today, numerous POCs in process



CONFIDENTIAL

Infoblox IF-MAP Server Offers Significant Advantages

FEATURE	FUNCTION	INFOBLOX	JUNIPER	IROND	OMAPD
Standards Compliance	Support for all versions of IF-MAP (v1.1 and v2.0)	YES	NO (v1.1 only)	NO (v2.0 only)	YES
Authorization	Restrict the operations that each client can do on the server	YES	NO	NO	NO
High-Availability	Automatic failover to a standby MAP server w/no data loss	YES	NO	NO	NO
Federation	Automatic sync of data across independent MAP servers	YES	NO	NO	NO
Custom Identifiers	Support for user-defined identifier types to accommodate new devices	YES	NO	NO	NO
Client Connection Controls	Ensure that temporary client disconnections don't cause data loss	YES	NO	NO	NO
Global Search	Ability to find any piece of data across the MAP	YES	NO	NO	NO
Global Identifiers	Support discovery, alerting and visualization applications	YES	NO	NO	NO
Monitoring Tools	Stats to enable troubleshooting and capacity planning	YES	NO	NO	NO
Transaction Logs	Complete logs (transaction, admin, error) for troubleshooting	YES	NO	NO	NO

Triggered Discovery and Triggered Jobs with Infoblox NIOS™, NetMRI and IBOS™ IF-MAP Server



1. NIOS is configured to publish IP/MAC metadata to IBOS
2. NetMRI is configured to subscribe to the “All IPs” Global Identifier in IBOS
3. Device connects to network (today, endpoint device only), gets IP via DHCP from NIOS
4. NIOS DHCP server publishes IP/MAC metadata to IBOS
5. IBOS updates NetMRI subscription, sends new IP/MAC metadata to NetMRI
6. NetMRI initiates discovery at new IP
7. After discovery, NetMRI can trigger a job:
 - Check MAC address against a set of predefined lists (blacklist, whitelist, etc.) and take appropriate action, e.g. make an API call to NIOS to delete the DHCP lease, initiate a script, etc.
 - Bare metal provisioning of infrastructure devices
 -




vmware®
AUTOMATION



**Server/Applications
Infrastructure**

**Security
Automation**
AUTOMATION




**Security
Infrastructure**

Infoblox Grid
AUTOMATION



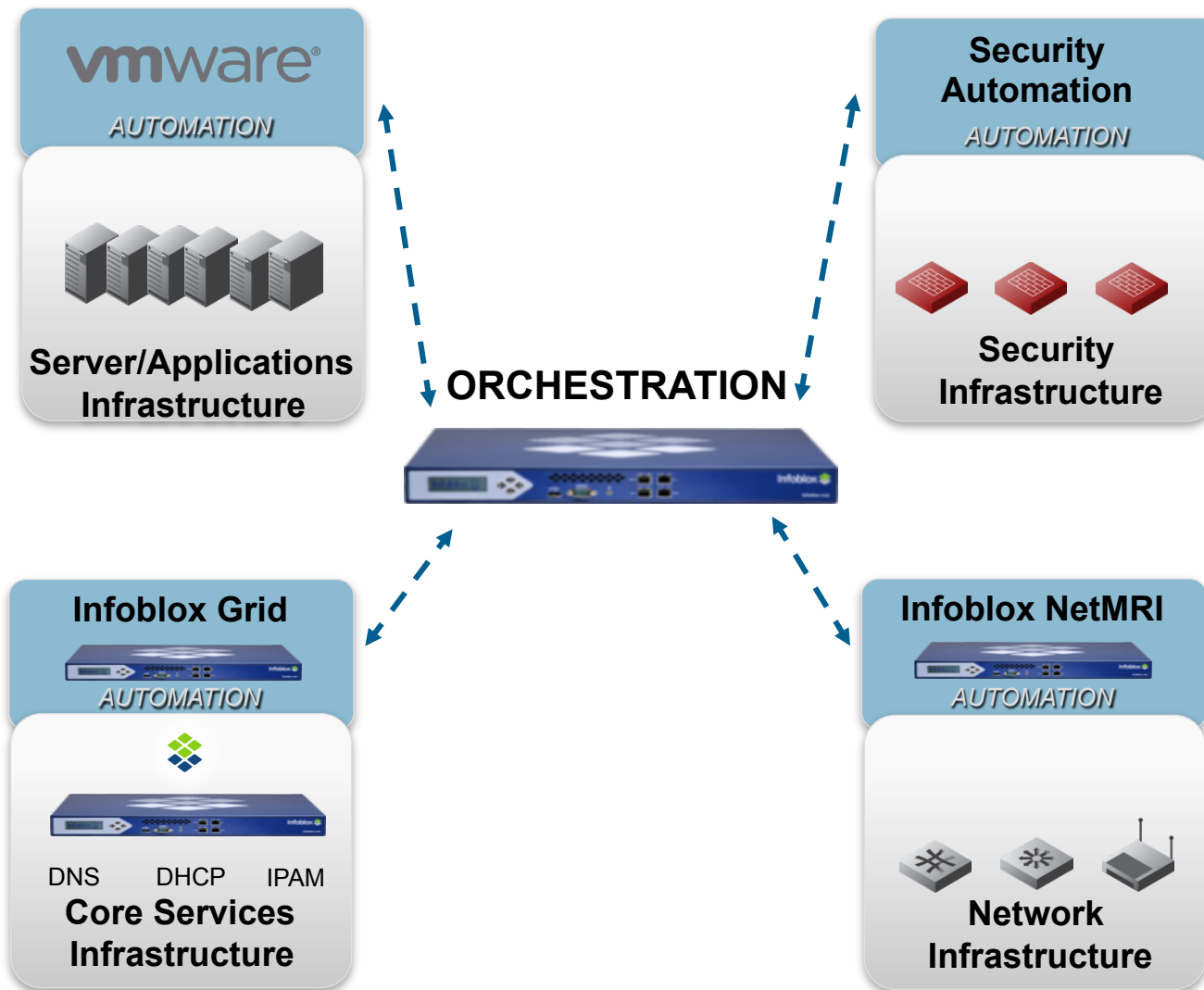
DNS DHCP IPAM
**Core Services
Infrastructure**

Infoblox NetMRI
AUTOMATION

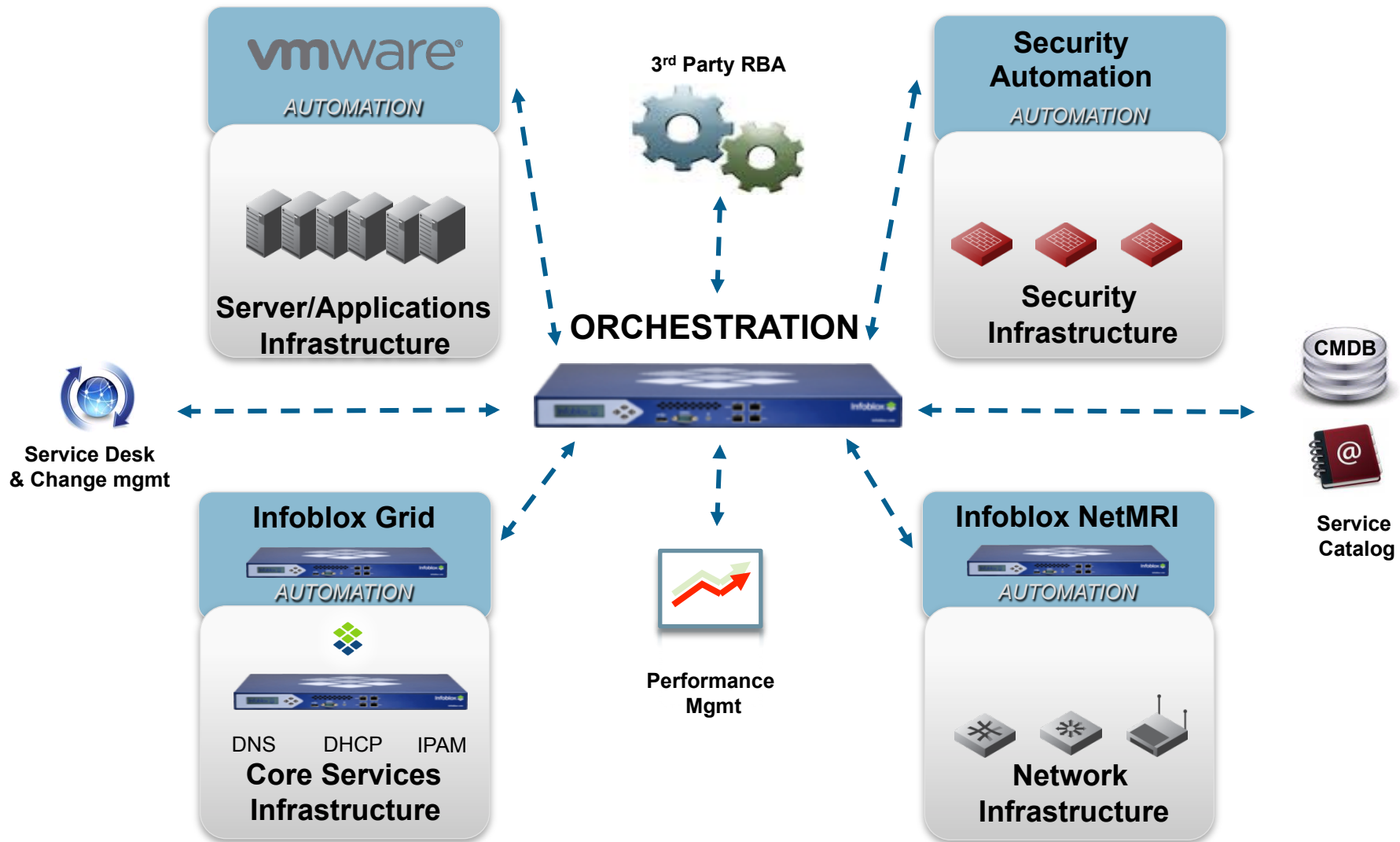


**Network
Infrastructure**

Orchestration is a Key Element of Network Automation



Open Interfaces Support Rich Orchestration – IF-MAP Provides Standardization



- **3 minute video on IF-MAP on Orchestration/IF-MAP Solutions page on infoblox.com**
 - <http://www.infoblox.com/en/solutions/technology-solutions/orchestration-if-map.html>

- **www.if-map.org**
 - IF-MAP community Web site
 - Includes links to open source IF-MAP servers and other resources

- **www.trustedcomputinggroup.org**
 - Complete protocol specs, information on TPM, TNC, Trusted Storage and related topics

- **Infoblox IF-MAP Starter Kit:**
 - Free for 90 days, \$995 in the US for perpetual license, 18% annual support
 - VMware IF-MAP appliance
 - Client simulator
 - Open-source client stacks (PERL, java, C++)
 - Open-source SNMP-MAP Bridge
 - Open-source connector to VMware (August, 2011)