IF-MAP Overview

Jan Ursi

Technical Director EMEA

IF-MAP: A Powerful New Standard

- **IF-MAP = Interface to Metadata Access Points**

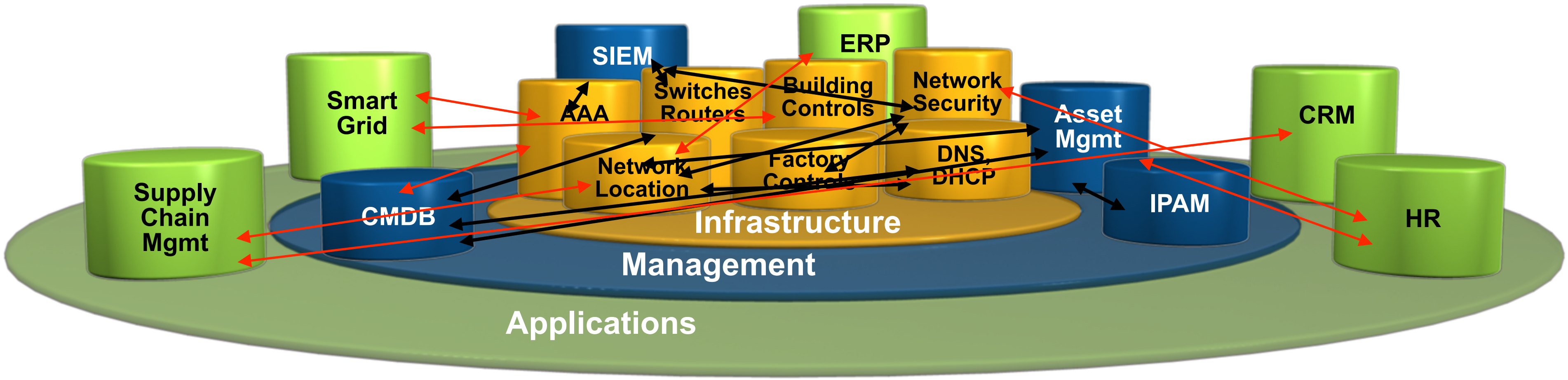
- **An open protocol standard published (free) by the Trusted Computing Group**
  - Available since April, 2008
  - Version 2.0 released August, 2010

- **Pub/sub database - Like Facebook for IP devices and systems**

- **Supports a wide array of applications:**
  - Multi-Vendor Network Security (NAC)
  - Compliance Management
  - Asset Management
  - Smart Grid
  - Network Automation / Cloud Computing

Could do for data sharing what IP did for connectivity

The Integration Challenge

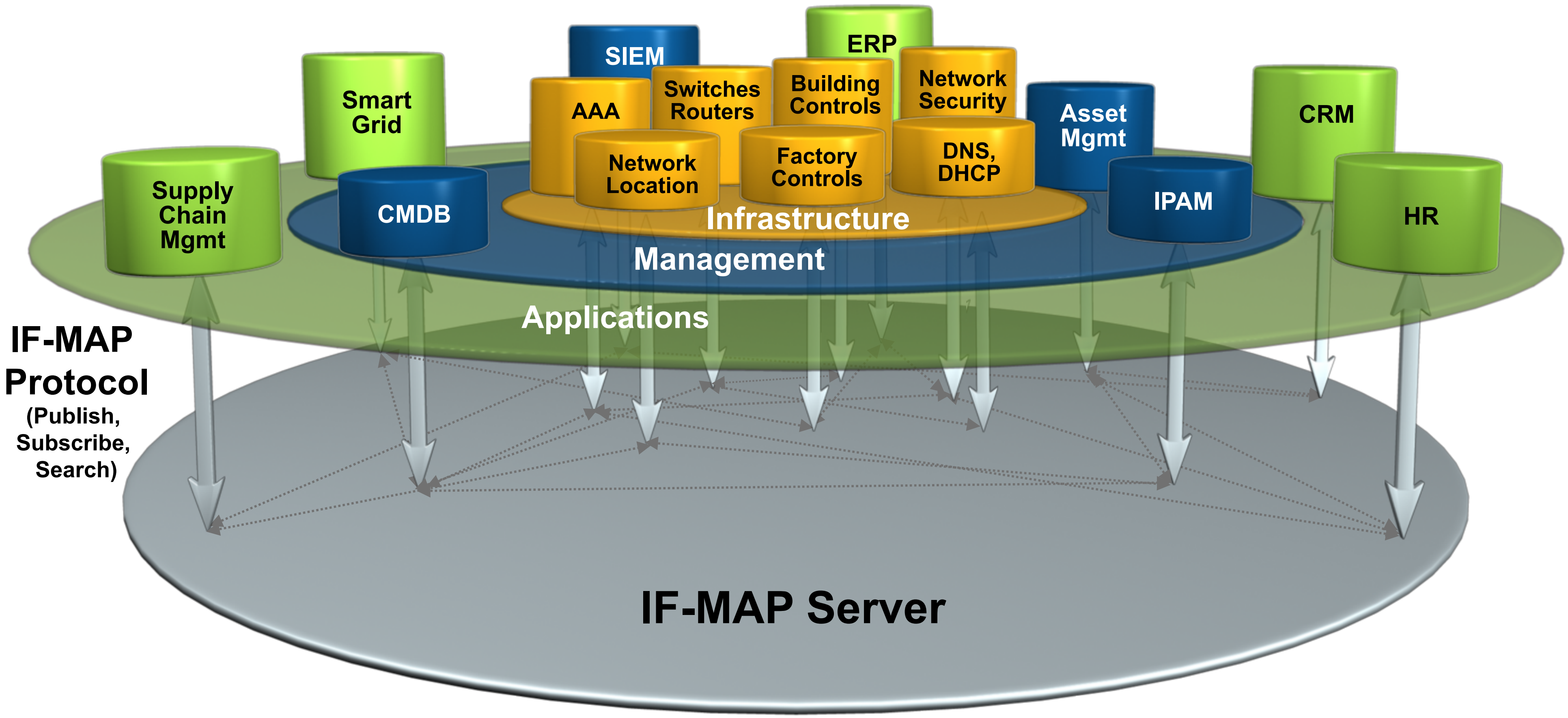


SNMP, Syslog, Netflow

Custom Integration – API's, Scripts

- Complex
- Costly
- Brittle
- High Maintenance

From Integration to Orchestration with IF-MAP



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

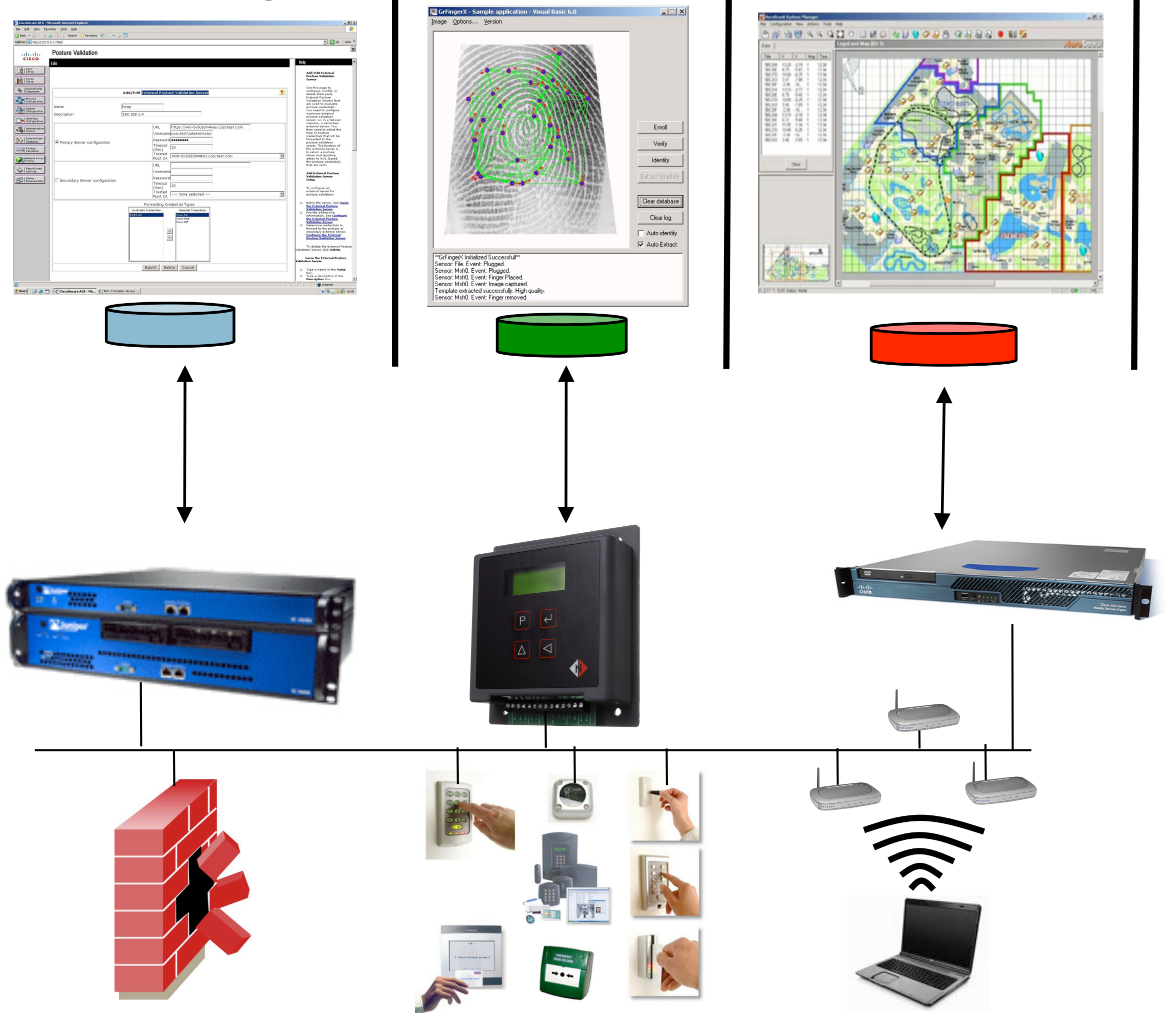
Today, Systems Share the IP Network, But Don't Share Data

Network Security | Physical Security | Network Location | …

Provisioning, Visualization & Analytics (Management)

Decisions (Control)

Sensors & Actuators



```
**GrFingerX Initialized Successfull**
Sensor: File. Event: Plugged.
Sensor: Msfr0. Event: Plugged.
Sensor: Msfr0. Event: Finger Placed.
Sensor: Msfr0. Event: Image captured.
Template extracted successfully. High quality.
Sensor: Msfr0. Event: Finger removed.
```

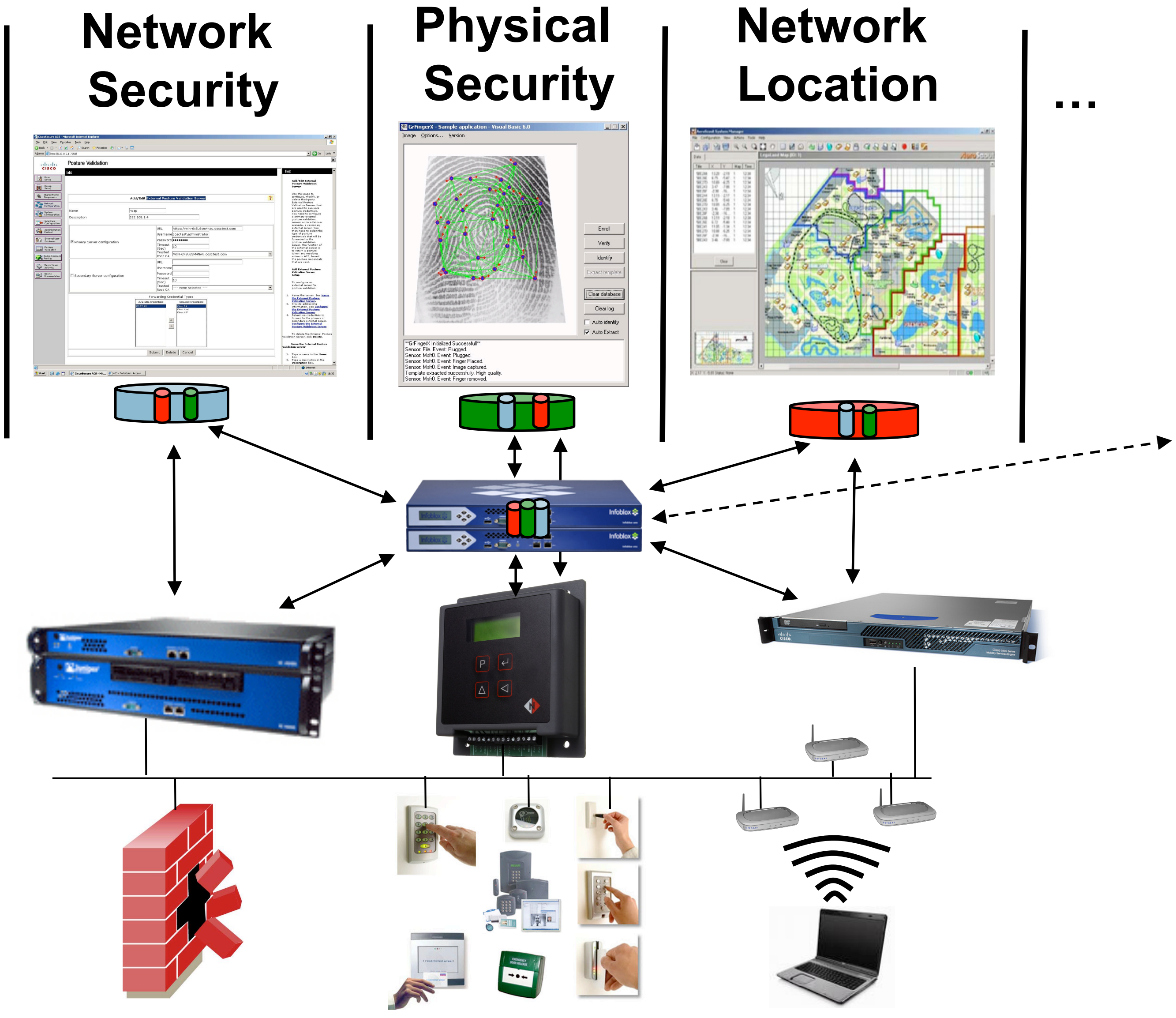
IF-MAP Doesn’t Replace Existing Systems & Applications – It Enables Them to Easily Share Data

Provisioning, Visualization & Analytics (Management)

IF-MAP Server

Decisions (Control)

Sensors & Actuators



Network Security

Physical Security

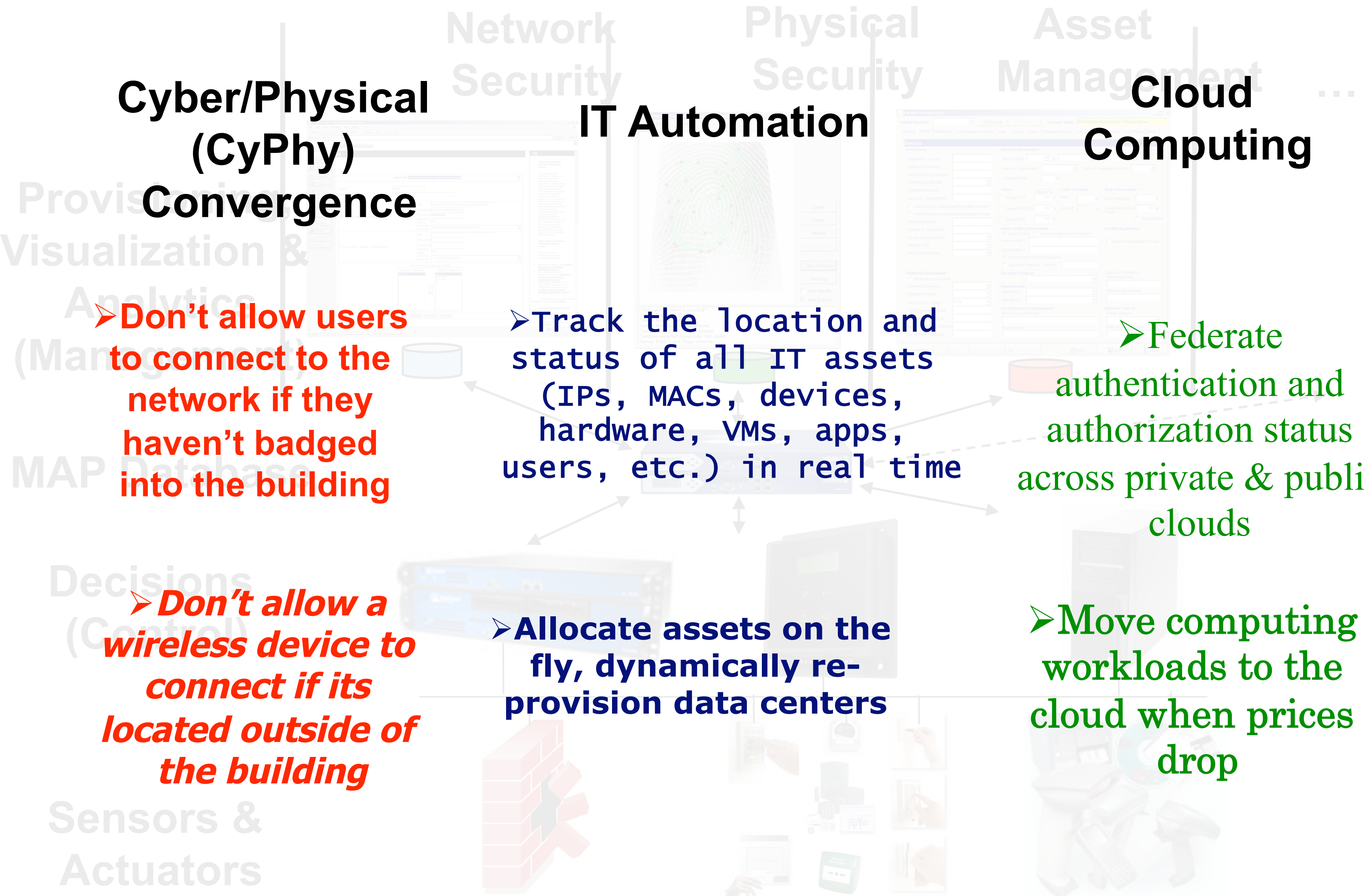
Network Location

…

GrFingerX - Sample application - Visual Basic 6.0

```
**GrFingerX Initialized Successfull**
Sensor: File. Event: Plugged.
Sensor: Msfr0. Event: Plugged.
Sensor: Msfr0. Event: Finger Placed.
Sensor: Msfr0. Event: Image captured.
Template extracted successfully. High quality.
Sensor: Msfr0. Event: Finger removed.
```

Many New Applications are Emerging – Just the Tip of the Iceberg…



Cyber/Physical (CyPhy) Convergence

- Don’t allow users to connect to the network if they haven’t badged into the building
- ***Don’t allow a wireless device to connect if its located outside of the building***

IT Automation

- `Track the location and status of all IT assets (IPs, MACs, devices, hardware, VMs, apps, users, etc.) in real time`
- **Allocate assets on the fly, dynamically re-provision data centers**

Cloud Computing

- Federate authentication and authorization status across private & public clouds
- Move computing workloads to the cloud when prices drop

Vendor Support for IF-MAP is Growing

Vendor	Product/Function	IF-MAP Client	IF-MAP Server	Avail
Byre Security	SCADA Security	X		Now
Great Bay	Endpoint Discovery	X		Now
Hirsch Electronics	Physical Access Control	X		Now
Infoblox	DHCP Server (NIOS)	X		Now
Infoblox	Orchestration 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		H1-11
NCP	VPN Client	X		H1-11
Open Source	IF-MAP Client Stack (PERL)	X		Now
Open Source	IF-MAP Client Stack (C++)	X		Q1-11
Open Source	IF-MAP Server (Omapd, Irond)		X	Now
Open Source	SNMP/IF-MAP Bridge	X		Now
Q1 Labs	SIEM	X		Q1-11

Some Infoblox IF-MAP Projects

- **Large Aircraft Manufacturer (In Production)**
  - Security for factory control (SCADA) traffic over wireless factory network
  - Firewall configurations loaded dynamically from IF-MAP server
  - Uses firewall/VPN gateways from Byres Security (Tofino)
- **Software Development Company (In Production)**
  - Network access control without software agents on endpoints
  - Uses Infoblox DHCP server, Juniper UAC, Juniper firewalls
- **Las Vegas Hotel and Casino (In Production)**
  - Differentiated IP services for every room (3000 Juniper firewalls)
  - Uses Infoblox DHCP, Juniper UAC and firewalls (3000), Logisense registration/billing portal
- **Global Bank (Starting Rollout)**
  - Dynamic, secure desktops – deploying to 8000 users
  - Uses QIP DHCP, Juniper UAC and firewalls
- **JANET - National ISP for Higher Education in UK (Pilot)**
  - Federation of authentication data for EDUROAM service
  - Uses IF-MAP federation
- **Real-Time CMDB (Pilot)**
  - Real-time discovery of devices joining the network
  - Uses Infoblox DHCP, IF-MAP client and OneCMDB (Open Source CMDB)

Infoblox®

IF-MAP Protocol Overview

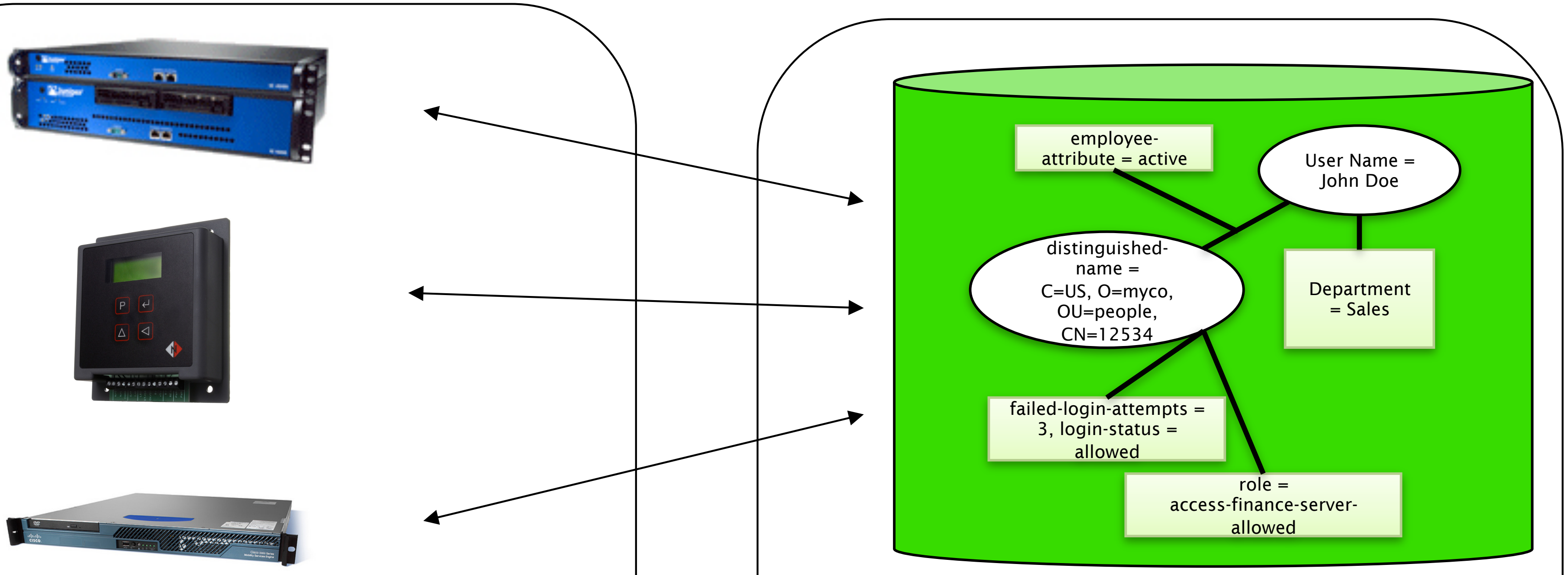
Unique Characteristics Cited by IF-MAP Supporters

1. Open, standard protocol
2. Lightweight, easy to implement
3. No global schema – supports emergent structures
4. Pub/sub paradigm

IF-MAP Components

IF-MAP Client(s)

IF-MAP Server



employee-attribute = active

User Name = John Doe

distinguished-name = C=US, O=myco, OU=people, CN=12534

Department = Sales

failed-login-attempts = 3, login-status = allowed

role = access-finance-server-allowed

3 MAP Client Operations:

Publish
Subscribe
Search

3 MAP Server Objects:

Identifiers
Links
Metadata

IF-MAP Access Operations

- **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"

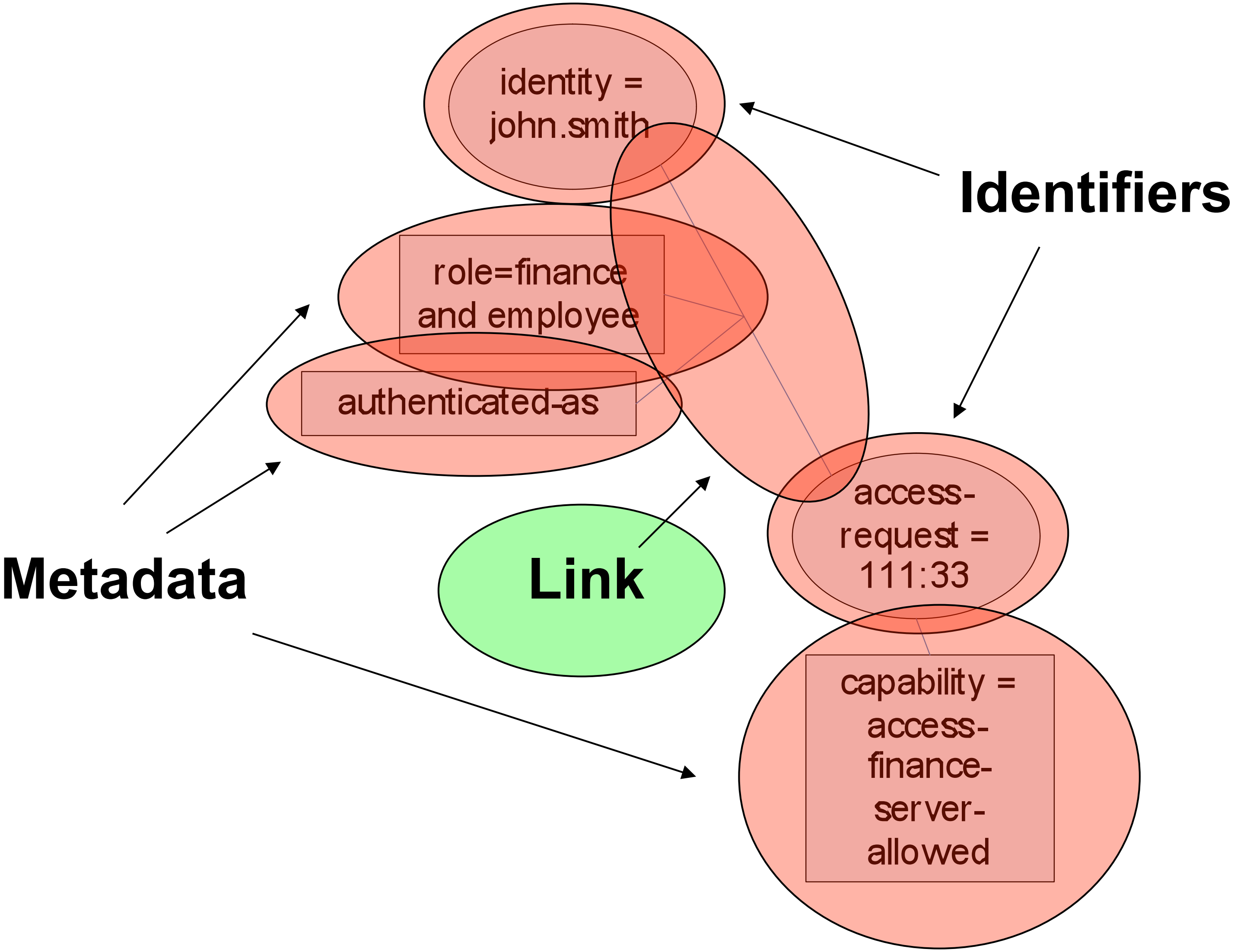
IF-MAP Server Objects

○	**Identifiers**	All objects are represented by unique identifiers
—	**Links**	Connote relationships between pairs of identifiers
🟦	**Metadata**	Attributes attached to Identifiers or Links

Typical Data Types:

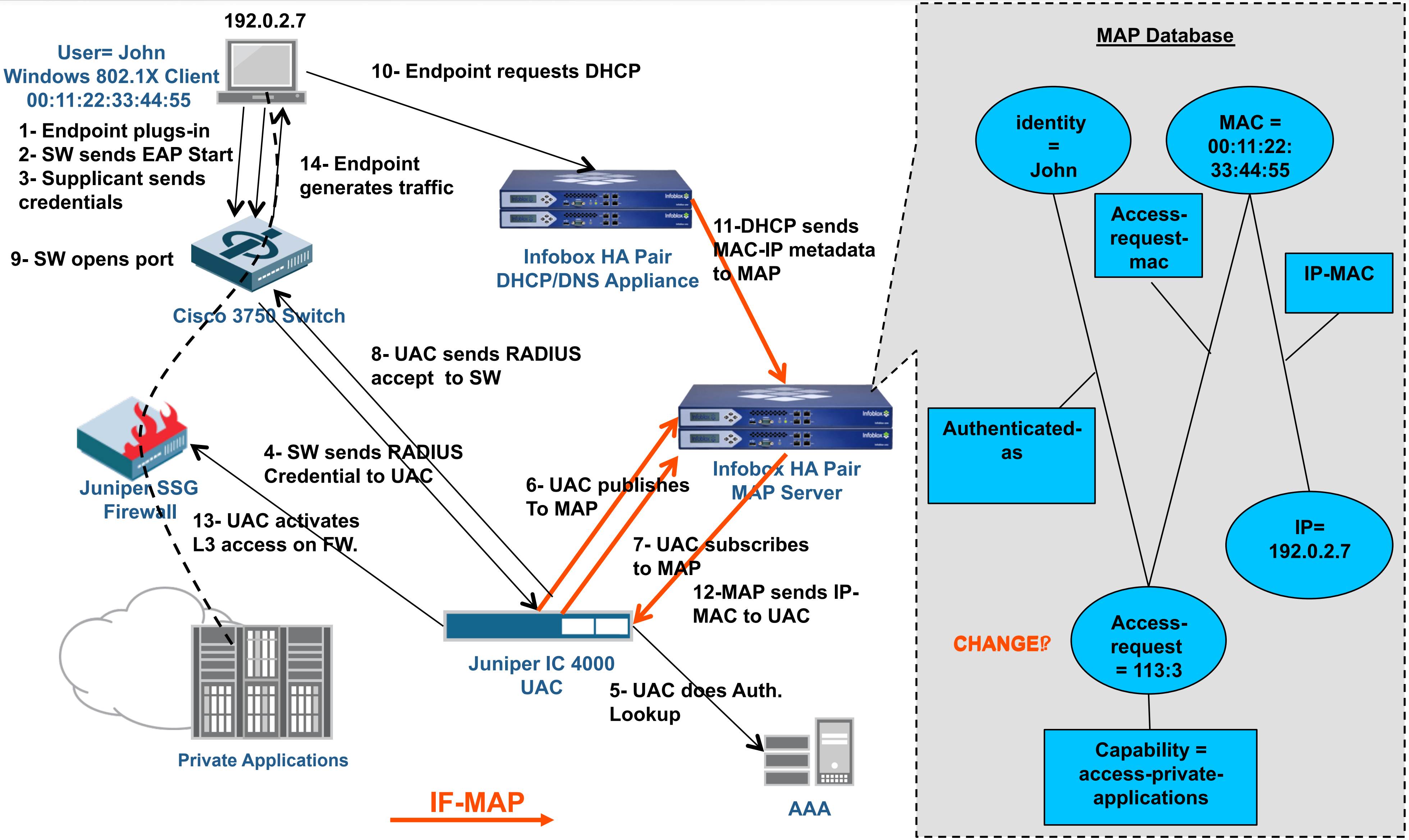
- Identifiers: Identity, IP address, MAC address, Session ID, Device
- Metadata:
  - AAA info (authenticated, role, capabilities/policies)
  - Device info (AV running, OS level, screen size, etc.)
  - Event info (unauthorized access attempt, etc.),
  - Layer 2 info (port, VLAN), location, etc.
  - Many others, plus user-defined

Basic Components of MAP Content

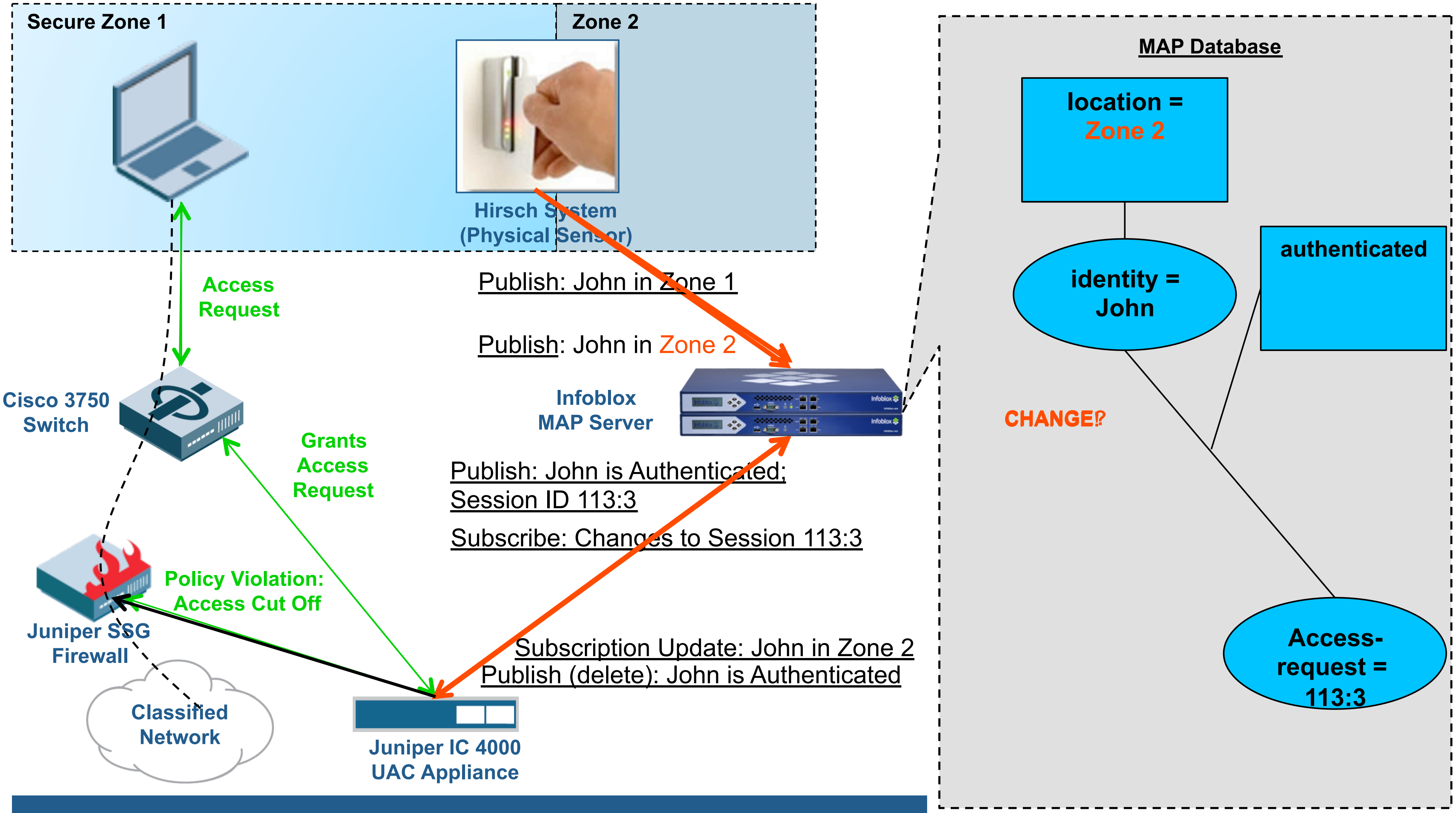


IF-MAP Use cases

Use Case – Solution for Policy-Based Remote Access

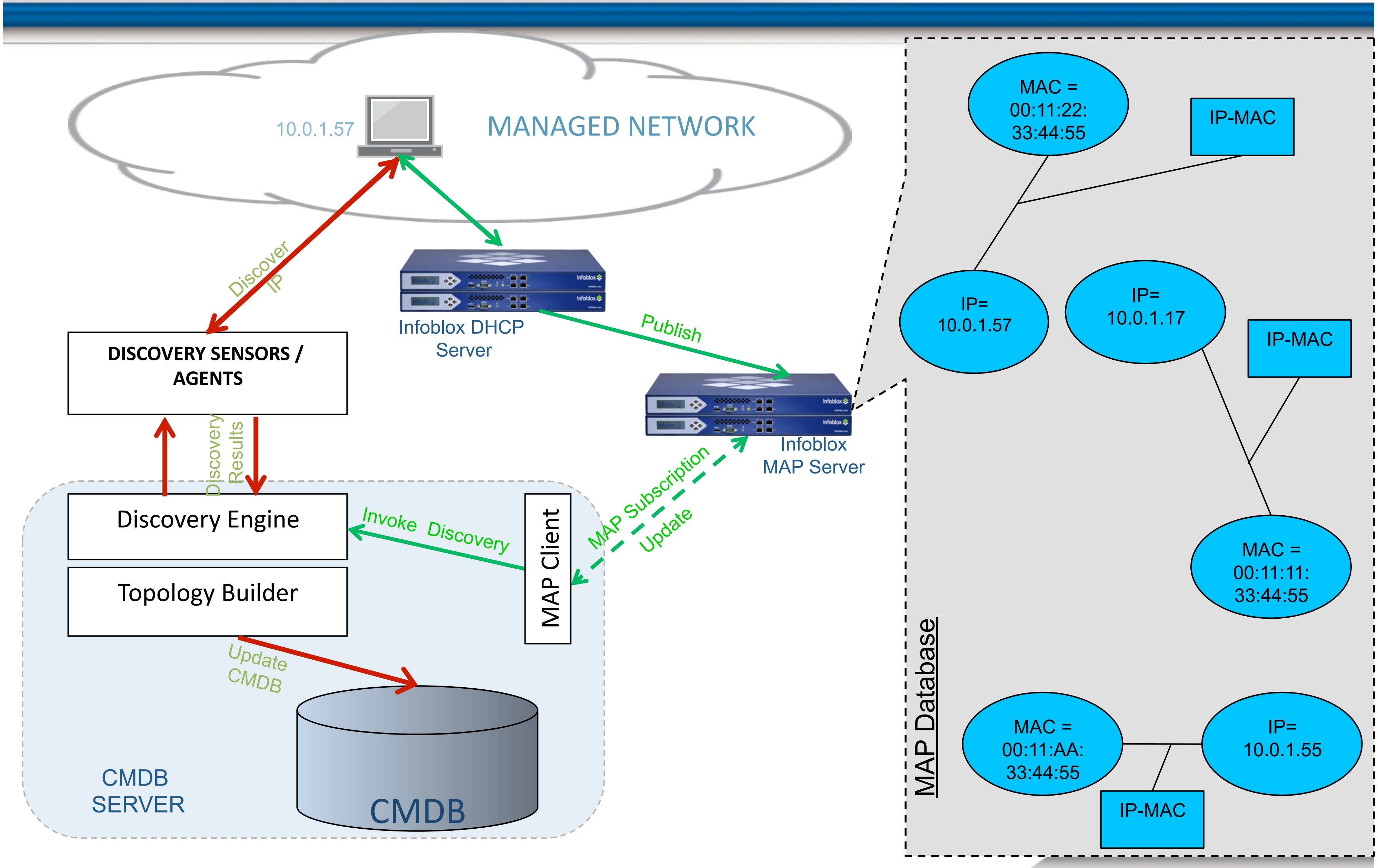


Use Case – Integrated Network / Physical Security Solution



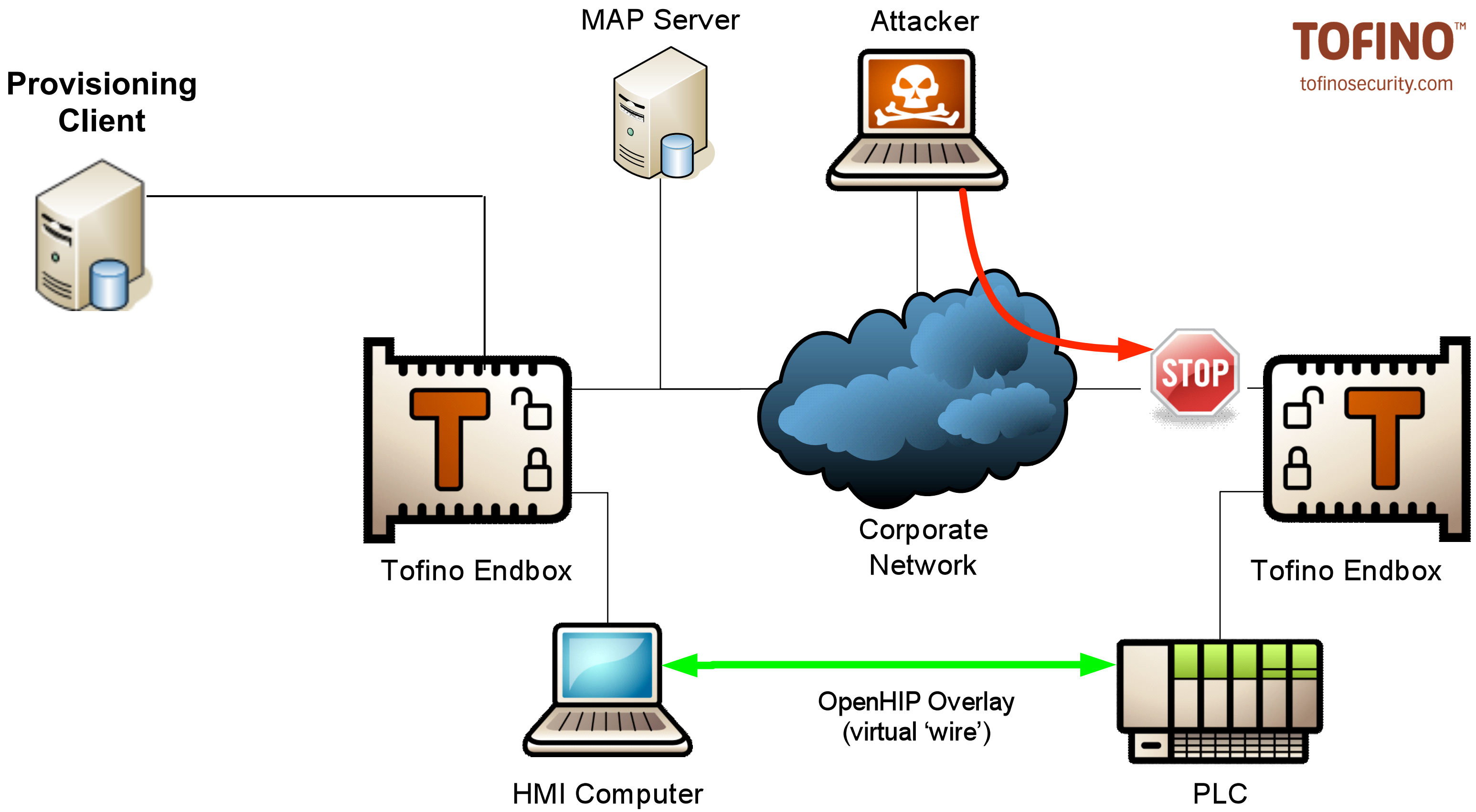
10- MAP updates UAC about the location change

Use Case: Real-Time CMDB



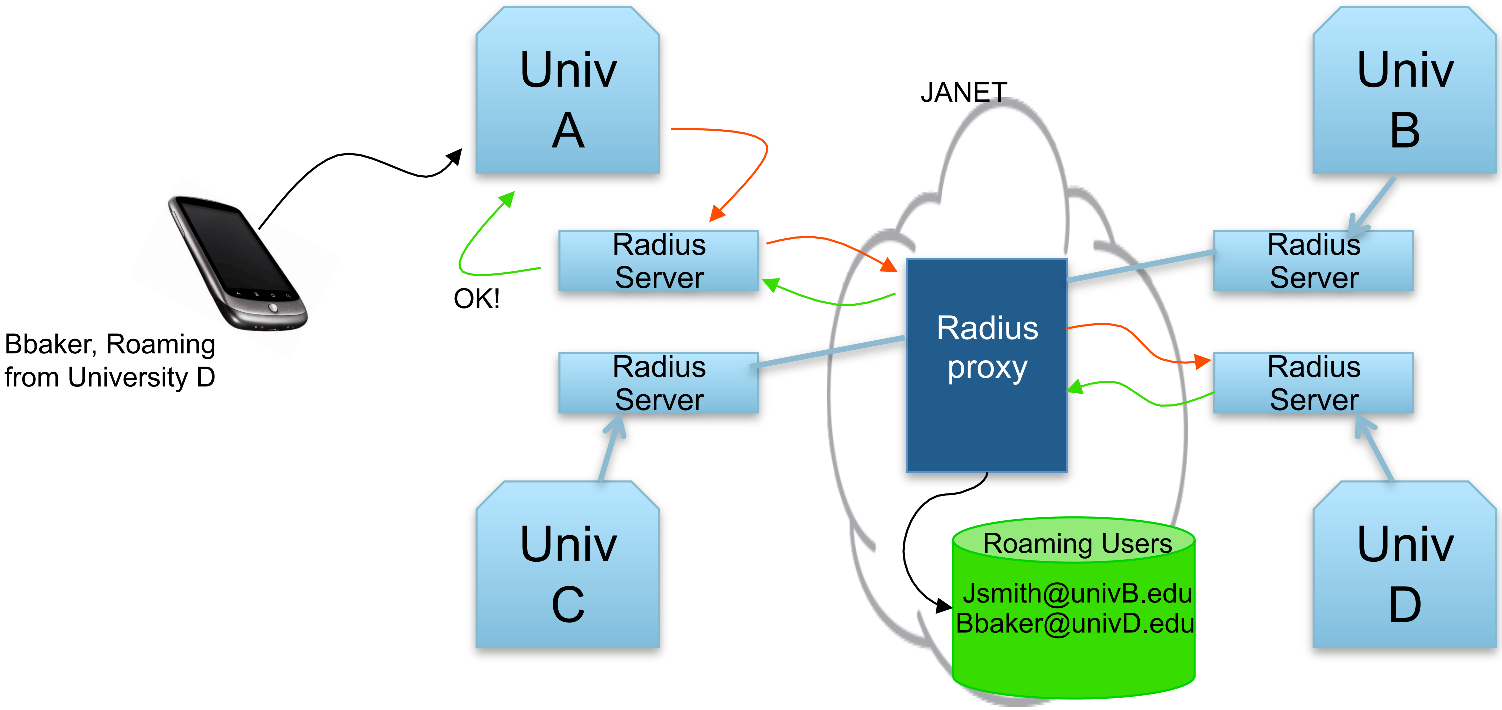
Use Case: SCADA Security

- IP-based industrial control traffic shares the general IT network in the factory
- “Endboxes” provide VPN/firewall security
- Endbox configurations dynamically loaded from MAP server – based on user, role, etc.



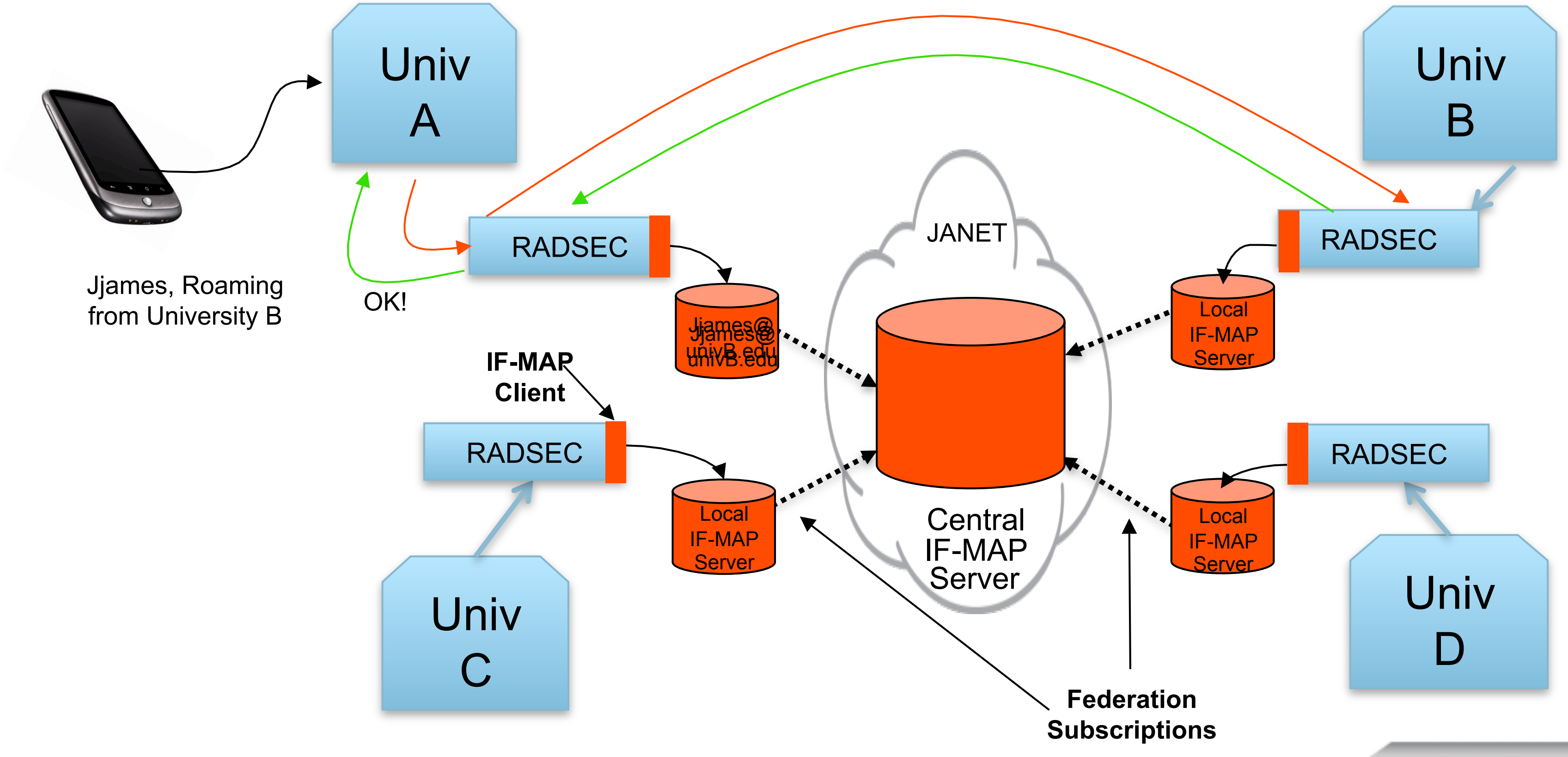
Use Case: Federated IF-MAP Servers for UK EDUROAM Service

- 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



IF-MAP Federation for Next Gen EDUROAM Service

- 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



Univ A

Univ B

Univ C

Univ D

RADSEC

RADSEC

RADSEC

RADSEC

JANET

Jjames, Roaming from University B

OK!

Jjames@ univB.edu

IF-MAP Client

Local IF-MAP Server

Local IF-MAP Server

Local IF-MAP Server

Central IF-MAP Server

Federation Subscriptions

IF-MAP has Applications in Cloud Computing and IT Orchestration

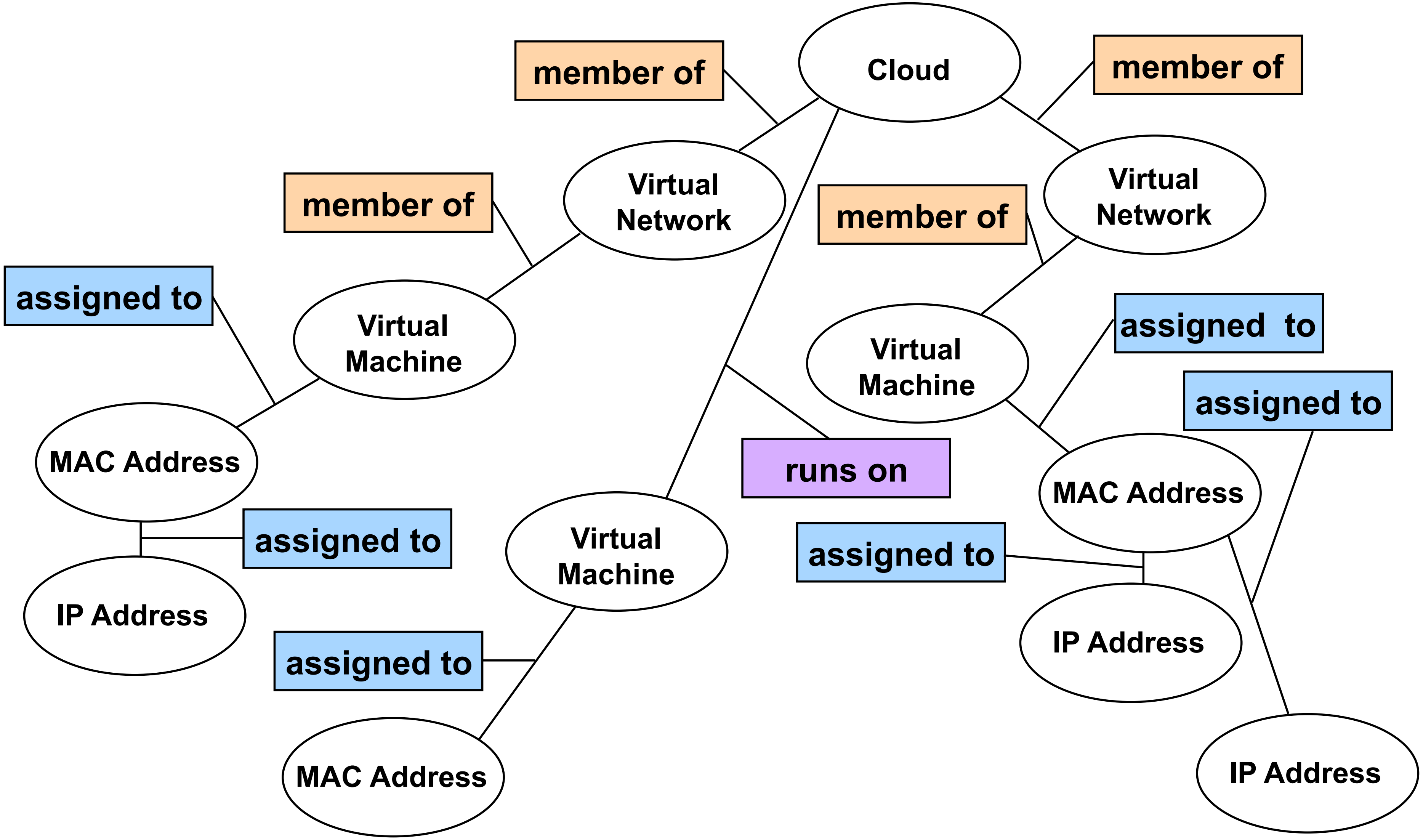
- Infrastructure 2.0 Working Group has been discussing the impact of virtualization & cloud computing on the network

- Members include equipment vendors, cloud providers and end users
  - Infoblox, Cisco, Google, Microsoft, F5, Citrix, Bechtel, Boeing, NASA…

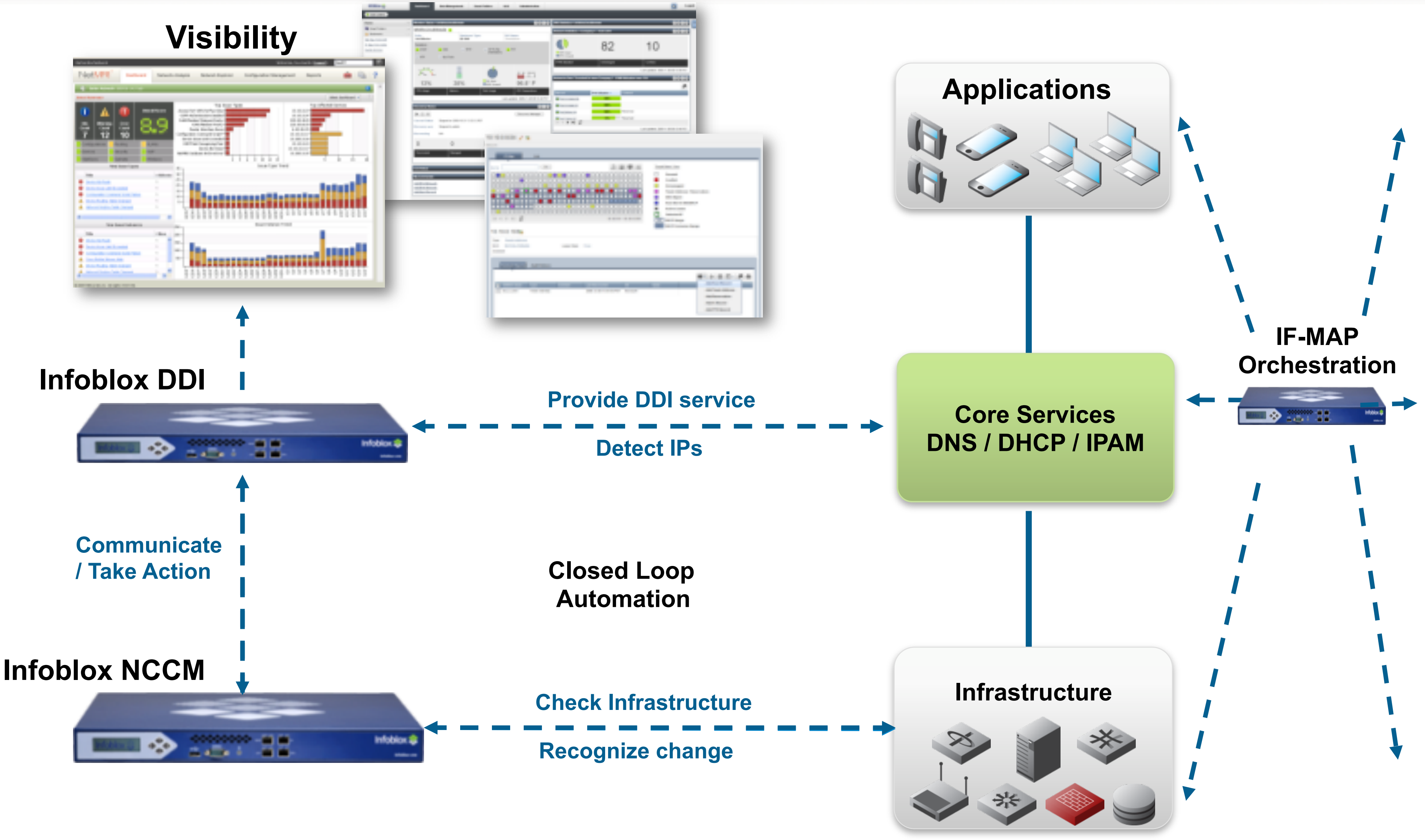
- Developing an “inter-cloud registry service” based on IF-MAP
  - Ongoing project at Open Cloud Consortium in Chicago
  - Co-sponsored by Cisco CTO’s office and UCS group

- More info at www.infra20.com

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



The Vision: IF-MAP Supports Data Exchange Among Infoblox, and Other Vendors' Products



Visibility

Applications

Infoblox DDI

Provide DDI service

Detect IPs

Core Services
DNS / DHCP / IPAM

IF-MAP
Orchestration

Communicate
/ Take Action

Closed Loop
Automation

Infoblox NCCM

Check Infrastructure

Recognize change

Infrastructure

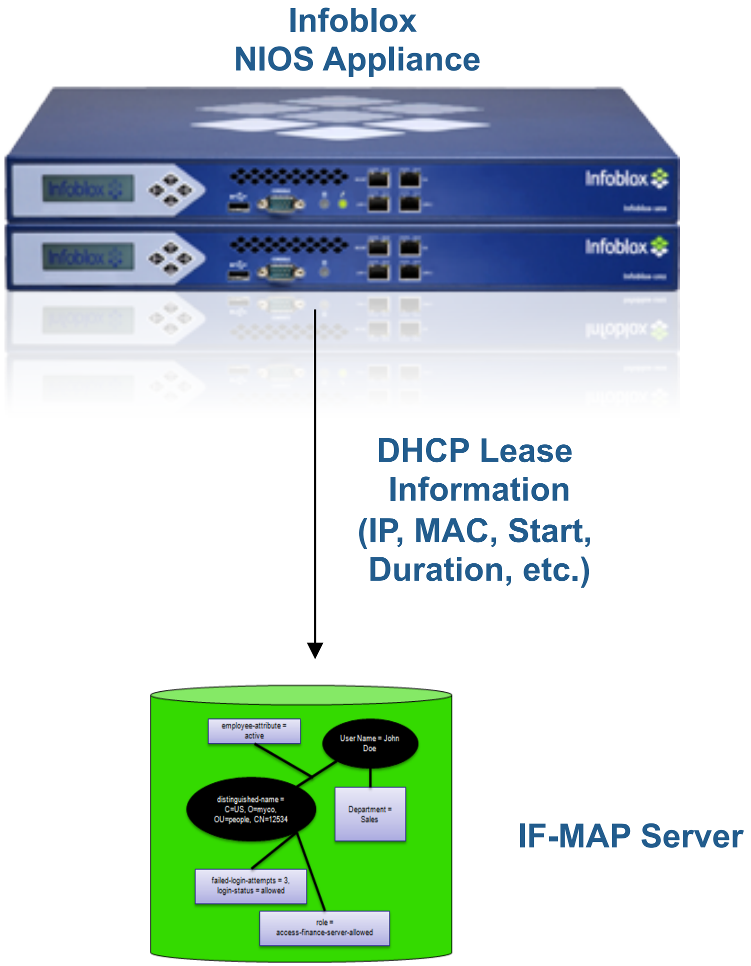
Resources

Infoblox NIOS Appliances Support IF-MAP

- Dynamically updates IF-MAP server when IPs are allocated, renewed, or released by NIOS DHCP server

- Other systems can subscribe to updates and take action in real-time (e.g. discovery, configuration, scanning, open/close ports, etc.)

- Unique to the Infoblox DHCP server (today)



Infoblox
NIOS Appliance

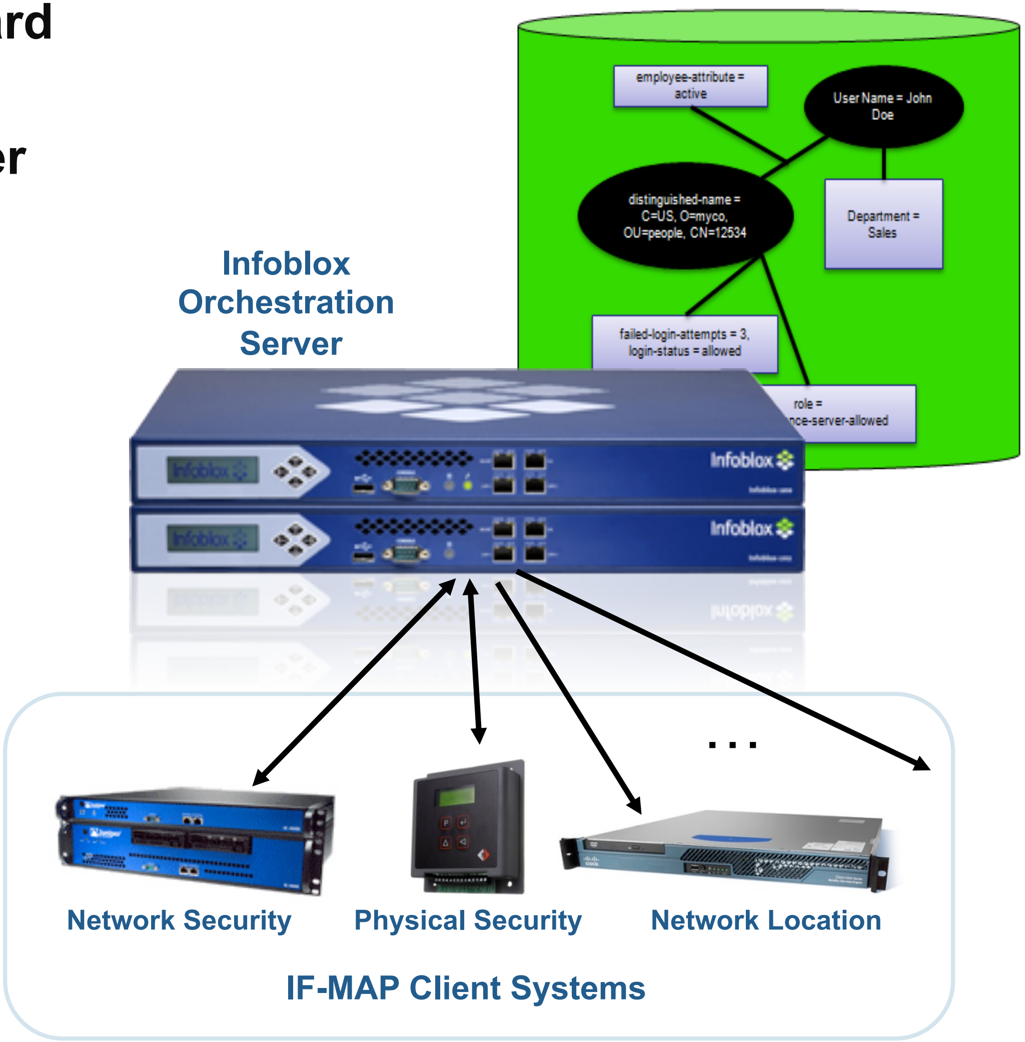
DHCP Lease Information
(IP, MAC, Start, Duration, etc.)

IF-MAP Server

employee-attribute = active
User Name = John Doe
distinguished-name = C=US, O=myco, OU=people, CN=12534
Department = Sales
failed-login-attempts = 3, login-status = allowed
role = access-finance-server-allowed

Infoblox Orchestration Server (IBOS): The World’s Most Powerful IF-MAP Server

- **Fully compliant with TCG standard**
- **Proven interoperability with other IF-MAP compliant products**
- **Unique Infoblox capabilities**
  - IF-MAP 2.0 compliant
  - Lossless HA
  - Fine-grained client authorization
  - Data browser, extensive logging
  - IF-MAP Federation
  - Custom Identifiers


employee-attribute = active
User Name = John Doe
distinguished-name = C=US, O=myco, OU=people, CN=12534
Department = Sales
failed-login-attempts = 3, login-status = allowed
role = nce-server-allowed
Infoblox
Infoblox
. . .

Infoblox Orchestration Server

Network Security

Physical Security

Network Location

IF-MAP Client Systems

Resources – Documentation & Freeware

- **3 minute video on IF-MAP on Orchestration/IF-MAP Solutions page on infoblox.com**
- **www.if-map.org**
  - IF-MAP community Web site
  - Includes links to open source IF-MAP servers and other resources
- **www.juniper.com**
  - Information about Infranet Controller: us/en/products-services/security/uac/#overview
- **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