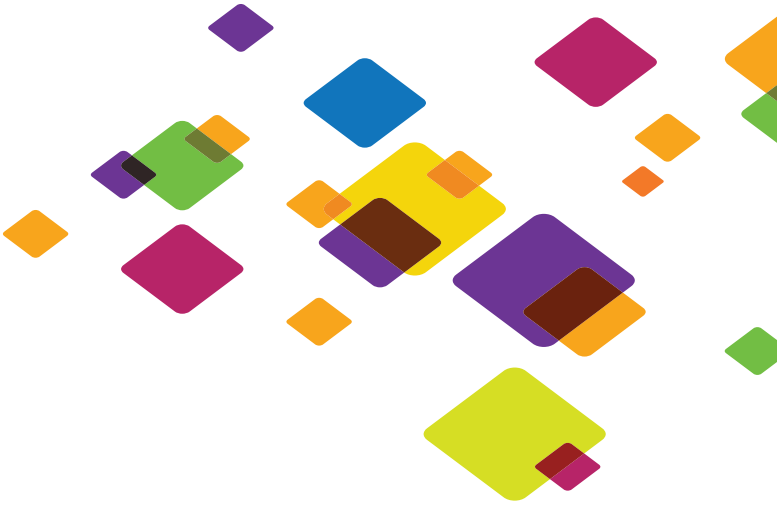
Infoblox
CONTROL YOUR NETWORK

WHITEPAPER

IF-Map and the Orchestration Era



Overview

Organizations have made dramatic improvements in efficiency and customer satisfaction by breaking down application and database silos. By linking Customer Relationship Management (CRM) systems with order status, inventory and logistics systems, for example, customers can see product availability and track their shipments accordingly. Organizations gain can through reduced inventories, shortened delivery times, and lower customer support costs. Customers benefit from an improved shopping experience.

Still, many aspects of IT infrastructure and business operations do not benefit from integration and coordination. Many organizations lack real-time or historic visibility into their infrastructure or assets, and those that do have such visibility often see only "slices" of their infrastructure at a time because it's difficult to integrate data across different systems. Critical systems such as network infrastructure, network security, building controls, power systems, physical security systems, asset management and others still operate largely in silos. The need to further increase productivity and the requirements for ever more detailed audit and compliance reporting drive the need to break down silos and integrate information across different systems. As such, organizations often end up with complex, brittle, and expensive customized solutions —or else spend an increasing amount of valuable time doing things manually.

Numerous management and monitoring standards and approaches have existed for some time, but none have provided the complete set of capabilities needed to enable easy integration, correlation, and sharing of data across multiple, disparate systems, securely, and in real-time. The lack of an effective solution is widely recognized as an issue. In a series of phone interviews of 50 senior IT managers across the United States an independent research consultancy[1] found that 87 percent of respondents viewed an automation standard as either important or very important, and nearly three quarters (70 percent) indicated that they would be willing to pay 10 percent more for product that complied with such a standard.

Over the last several years, the Trusted Network Connect (TNC) group, a sub-group of the Trusted Computing Group (TCG), has been developing a suite of standards to facilitate open information exchange between multi-vendor systems used in network security applications. One of the TNC protocols, called Interface to Metadata Access Point—or IF-MAP—serves the role of collecting, aggregating and distributing data among different systems in real-time. IF-MAP is already being deployed in multi-vendor security implementations, and is receiving significant attention for use in other applications including IT automation, compliance reporting, cloud computing, supply chain management, smart grid, and others.

Key Criteria for an Integration Standard

IT organizations have benefited greatly from the availability of broadly supported industry standards, which lower costs and enable new applications. Vendors in turn have gained from the new, large, fast-growing markets for compatible products. Judging by the success of the Internet Protocol (IP), an effective standard for integration has the potential to provide substantial benefits for end users and vendors.

Prior to IF-MAP, no technology has had all that is needed to provide an effective integration standard. To address these shortcomings, the guiding principles behind IF-MAP were as follows:

Automatically Aggregate and Correlate Data from Disparate Systems

Monitoring and control standards, such as SNMP and Syslog, define specific message formats and metadata elements, but they don't provide a standardized way to aggregate and correlate information from different sources. As such, developers must write code that will parse all of the incoming messages, normalize them into a common data representation, associate related data items and trigger alerts to other systems when something changes. It can be done, but it takes a lot of work and requires significant ongoing maintenance. The IF-MAP standard defines a client/server protocol, and the server side is a database that supports publish, subscribe, and search operations. An IF-MAP server is able to automatically associate related information and thereby builds up a comprehensive view of all of the data related to an object such as the user, their role, their privileges, their IP address, the MAC address, the device, session information, and events from disparate and potentially unrelated sources.

Easily Accommodate User and Vendor Extensions to Support New and Emerging Use Cases

Previous attempts to standardize data exchange have faltered because of the need to agree ahead of time on the structure and semantics of all possible data items before the standard can move forward. There are simply too many items and too many parties of interest in the world to make such an effort practical. The IF-MAP standard started with the definition of a few key metadata elements—specifically, those of interest in network security applications, but was designed to easily accommodate user and vendor-specific extensions, even prior to their incorporation into the formally published standard. This enables the standard to rapidly evolve to address new applications without requiring vendors to rebuild their IF-MAP implementations to accommodate schema extensions. By using XML documents to represent all information, data items can be self-documenting and easily understood.

Provide Standardized Support for Common, Well-understood Items

There have been efforts over time aimed at standardizing the representation of basic IT elements such as users, addresses, names, and the like. Rather than re-invent the wheel, IF-MAP builds upon prior work and accommodates existing representations of metadata and also allows for new representations.

Provide Automatic Notification of Changes

Systems relying on polling do not discover changes in real-time and are extremely difficult to scale. The IF-MAP 'subscribe' function enables client systems to be notified whenever an item of interest changes—say, a device or process gets a new IP address, or a user's role goes from "employee" to "terminated". Subscriptions eliminate the need for continuous polling and ensure real-time notification of changes.

Eliminate the Need to Develop and Maintain a Pre-defined Global Hierarchy or Data Schema

One of the main limitations of directories (such as LDAP) is that they can only store and process data and relationships that conform to a pre-defined global schema. In essence, this requires one to define all of the data elements and all of the possible relationships that can be expressed, before the system is ever deployed. As anyone who has ever tried to do so knows, changing a database schema once it has been deployed can be a very painful process. IF-MAP is specifically designed such that no global schema ever needs to be defined. The schema—i.e. the data elements and their relationships—evolve organically as information is added by various systems to the MAP database. In this way, an IF-MAP database is able to reflect the true, real-time state of a system as it evolves, and as such it can reveal patterns and support applications that were never anticipated.

Emanate from a Recognized Standards Organization

Today's networks are built from such a vast diversity of legacy and new systems that no one vendor can supply the full spectrum of possible solutions. Any attempt at coordinating activities across different systems and domains must be widely supported by the industry and the only way to achieve that adoption is through an open standard from a credible industry standards organization. The TCG, which publishes the IF-MAP standard, is a respected standards body, responsible for standards such as the Trusted Platform Module (TPM), which is the means used to provide hardware-based security in virtually all enterprise computing systems. The TPM is available in desktop, notebook and tablet PCs from Dell, Fujitsu, Gateway, HP, Intel, Lenovo, Toshiba and others. The TCG also maintains certification testing standards for TPM and has established certification procedures for the Trusted Network Connect (TNC) protocols. In addition, several of the TNC standards related to IF-MAP are now being adopted in the IETF, and IF-MAP is likely to follow a similar path to IETF recognition.

Overview of the IF-Map Protocol

The IF-MAP specification defines a client/server protocol. The MAP Server, or simply MAP, stores and distributes metadata that reflects the real-time state of devices, users, and traffic flows in a network. This information can be wide and varied, a key benefit to the IF-MAP design, and includes things such as device characteristics and state, authentication and authorization status, and virtually any kind of metadata, namely physical location, conformance with policy, and recent behavior. IF- MAP Clients are the systems or applications that publish information to a MAP Server, search the information in a MAP Server, and subscribe to notifications from a MAP Server when information stored in the server changes. MAP clients can be end nodes, such as PCs, but more commonly IF-MAP is integrated natively into sensors, like intrusion detection systems, policy engines, and systems that have some level of aggregated data, such as authentication servers, security management systems, asset management systems, and network location systems. Over time though, IF-MAP may well be implemented natively in routers, firewalls, IDPs, and other network and computing infrastructure elements, in effect as a "next generation" of SNMP.

In normal operation, IF-MAP clients perform three operations: Publish, Search, and Subscribe. These are the operations used to populate the MAP server and to cause the MAP server to notify systems when changes of interest occur.

The MAP server contains 3 types of objects: Identifiers, Metadata, and Links.

- **Identifiers** are global, unique values within a given dataset. An IP v4 or v6 address, for example, would be an Identifier within the dataset (called the Identifier Type) of IP Addresses. Other standard identifiers defined by IF-MAP are:
  - MAC address (in colon-delimited format)
  - Device (in the form of a TCG AIK-Name or string)
  - Access Request (in the format 'publisher-ID:UID', where the publisher ID is the client and the UID is a session number)
  - Identity (in one of many forms, including TCG AIK Name, X.500 Distinguished Name, DNS name, email address, Kerberos principal, etc.)

- **Links** are simply a unique association between a pair of identifiers, such as between an IP address and a MAC address, or an IP address and a user identity, or a MAC address and a device, etc. There is only one link allowed between any two Identifiers, but any given Identifier can have many links to other unique Identifiers.

- **Metadata** is information associated with an identifier or a link. Many different types of metadata have been defined in version 1.1 of the IF-MAP specification, a number of which are primarily related to network security, including:
  - **Access Request** (MAC, Device, or IP)—this is essentially a session ID used to refer to a specific network flow or access attempt. There are three AR metadata types, one defined for association with a MAC address identifier (typically published following a layer-2 event such as 802.1x authentication), another defined for association with a device identifier and another defined for association with an IP address identifier.
  - **Authenticated-as/Authenticated-by**—these metadata types are published on a link to associate an Access Request identifier with an Identity (such as user). This metadata can be used to search for other information related to a specific user engaged in a particular session, such as their role (which is another metadata type). The "Authenticated-by" metadata type is published on a link between an Access Request identifier and an IP address identifier, and indicates that IP address is that of the system that authenticated the user. This is useful in posting subscriptions to be advised of changes associated with specific endpoints.
  - **Capability**—this is a set of privileges associated with the granting of an access request. The capabilities are typically drawn from a AAA or some other provisioning system that holds information about users and policies. Capabilities can be unique to an organization and even unique among different parts of the same organization. Capabilities can define things like "restricted-access" or "top-secret-clearance" or "guest-only", or "9-5_MTWTF", as an example.

- **Device Attribute**—this is used on Access-Request and Device identifiers to convey information of interest to policy engines, such as "AntiVirusRunning" or "PatchesUptoDate" or "PDA". Users can define their own Device Attribute values.
- **Event**—this is used to associate activity of interest with an access request, a device, an IP or a MAC address. There are a number of pre-defined events, such as virus attack detected, policy violation, or behavioral change. There is also an event type "other" that allows for vendor-defined event values.
- **Layer 2 Info**—this is used to associate information such as VLAN and switch port with an Access Request or IP Address identifier.
- **IP-MAC link**—this metadata type is published on a link between an IP and MAC address, and contains data typically associated with DHCP leases, such as start time and end time.
- **Role**—this metadata type is typically published on Identities such as user names. Organizations can define their own types such as "Employee", "Contractor", or "Terminated".

In addition to the above pre-defined types, vendors and users can define their own metadata types and the values for those types. If one or more metadata types are agreed upon by a community, such as building automation vendors or hypervisor vendors or smart electric meter vendors, they can include those extensions in the IF-MAP standard in two ways. They can submit these metadata types to the TCG for formal inclusion in the standard or create their own metadata standards that bind to IF-MAP publish/subscribe/search primitives.

It is important to realize that metadata conforming to user and/or vendor-defined types can be published to, searched for, and subscribed to without any changes to the configuration of a MAP server—again, because no pre-defined global schema is required. [NOTE: An IF-MAP server implementation may include schema validation features that would restrict clients to only being able to publish specified metadata types and reject all others—but this kind of functionality is specific to the MAP server implementation.

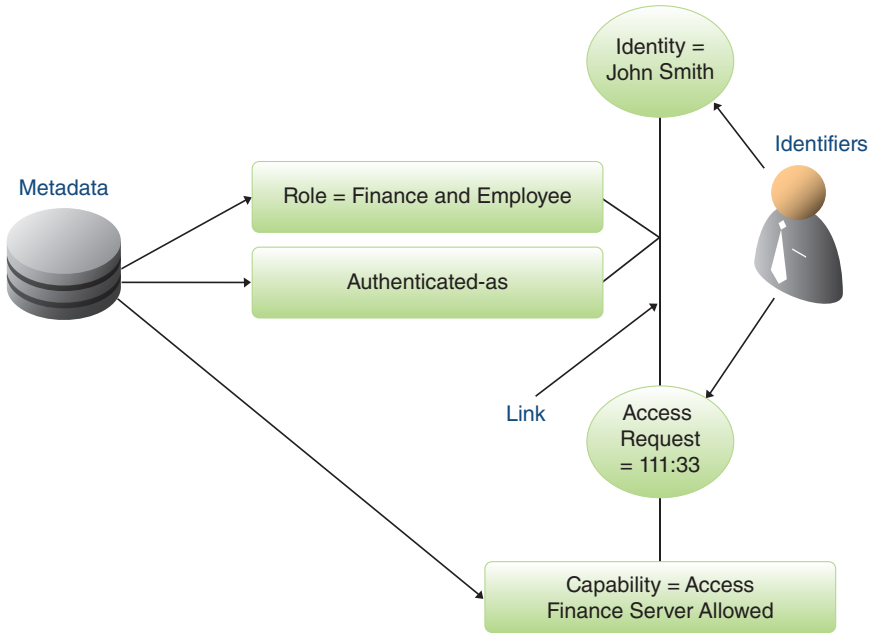


Figure 1: The structure of an IF-MAP database emerges as different systems publish metadata on identifiers and links.

These simple primitives—Publish, Subscribe, and Search—are used for the vast majority of IF-MAP transactions. The Publish operation is used by clients to create, modify or delete metadata associated with an Identifier or a Link. The Search operation always starts with a specific identifier (like a user or IP address) and returns identifiers, links and their associated metadata that match a client-specified search pattern and an optional result filter. The Subscribe operation is essentially a persistent search, which is triggered whenever the subscription is polled by the client or when the results of the search change (i.e. because something related to the search was modified by a Publish operation from the same or another client). The Subscribe operation is a key feature that enables IF-MAP deployments to scale, because it removes the load on clients and the network that would result from having to continuously search and poll the IF-MAP server for changes.

Security Considerations

By consolidating networking data into a single, logically-centralized database, IF-MAP becomes a powerful mechanism for sharing data amongst a wide variety of client systems. On the other hand, the extreme value of the information contained within the database makes the MAP an attractive point of attack. To defend against potential threats, the IF-MAP specification includes built-in security.

From a protocol perspective, there are three primary security challenges:

1. Ensure that the MAP server only allows connections from authorized clients;
2. Ensure that clients only communicate with an authorized MAP server; and,
3. Ensure the privacy and integrity of data transmitted between IF-MAP clients and servers.

The issues above are addressed by using HTTPS to communicate between an IF-MAP client and the server. Both ends of the connection must authenticate either using password-based authentication or bidirectional certificate-based authentication. After successful authentication, communications between client and server are secured using SSL encryption.

In addition to security features built into the protocol, specific MAP implementations may include additional security measures. The Infoblox IF-MAP server (the Infoblox Orchestration Server), for example, is available as a dedicated appliance delivered on a hardened operating system that provides no root access. The Infoblox Orchestration Server also provides fine-grained authorization that enables the administrator of the IF-MAP server to define read-only/read/write/deny policies for each identifier and metadata element for each IF-MAP client that connects to the server. This is particularly important in organizations where security and privacy restrictions force a firm segregation between information from different systems and different departments.

What an IF-MAP Server Doesn't Do

It's important to note that an IF-MAP server is not a policy engine and as such does not make decisions about the Identifiers or Metadata that it stores. Instead the IF-MAP server is a place where information from various systems is aggregated and re-distributed to other systems that make decisions—or that take action or report based on the data. A policy engine or reporting server or other such system may include a MAP server, but it doesn't need to. Furthermore, a plurality of policy engines may work with the IF-MAP sever without having to explicitly combine policies.

It's also important to note that an IF-MAP server can never take the place of a directory, such as Microsoft Active Directory, or any other authoritative provisioning system, whether it be for provisioning identity, policy, configuration, or anything else. By its nature, an IF-MAP server is never authoritative for the data that it contains; rather, it is a place for aggregating, correlating and disseminating the real-time state and changes that occur across a range of disparate systems, including directories, sensors, controllers, policy servers and other systems and devices.

Deployment Scernarios

As mentioned above, network security was the initial application that drove the development of IF-MAP. However, the standard was designed from the beginning to be general and thus applicable to a wide range of use cases. A few of these are explained below, starting with network security.

Dynamic Network Access Control

Network access control (NAC) is a term that has come to mean many things to many people. For the purposes of this discussion, NAC refers to the ability to apply policies dynamically to grant and maintain (or terminate) endpoint access to networks and applications. While this sounds simple enough in concept, implementing NAC has proved problematic for many organizations. The devil is in the details: Implementing NAC can be straightforward if all of the networking and security equipment in the network is from a single vendor, all endpoints are known and have endpoint security software installed, and if all devices are smart enough to support username/password or a similar type of authentication. In practice, these "ideal" conditions rarely exist:

- Even organizations that have a primary supplier for their networking equipment often use equipment from multiple vendors—for example, many organizations use security equipment such as firewalls and IDP/IDS from "best of breed" suppliers that are different from their network equipment vendor.
- Unmanaged endpoints, such as laptops owned by contractors or joint venture partners, are commonly found in today's corporate network.
- Increasingly, the devices on a network are things such as sensors or machines that don't have an interface or the intelligence to support end-user authentication.

These complexities typically make it necessary to either implement a highly restrictive network environment in which only known devices can connect, or else to implement an environment that leaves many security holes open in order to accommodate unmanaged devices and guest users.

The example below describes a dynamic network access control scenario that leverages IF-MAP to support fine-grained security policies for both managed and unmanaged endpoints, both pre and post admission:

A global organization, call it ABC Co., operates small remote sites around the world, often in spaces shared with competitors. End devices at each remote location, which can include PCs, laptops, printers, bar code scanners and others, connect to a local switch which is in turn connected to a local firewall that provides a VPN tunnel back to the organization's main datacenter. On occasion, users at the remote sites need to "swap" locations with a competitor, who will then plug their devices into the remote firewall. Of course, the competitors should not be granted access to ABC Co's datacenter. ABC Co. needs a way to dynamically establish firewall policies at the remote locations for the managed and unmanaged devices that periodically connect.

The local switches are from several different vendors, so using a single-vendor solution isn't possible. Each of the switches is configured for 802.1x port authentication. Managed PCs and laptops have an 802.1x supplicant and support end-user authentication. Unmanaged devices—either guest PCs without 802.1x supplicants or "dumb" devices (like bar code scanners) authenticate via MAC authentication (i.e. their MAC address is passed to the RADIUS server in response to the 802.1x challenge).

The solution uses three IF-MAP compatible products: A Juniper Infranet Controller (IC) which provides RADIUS-based authentication for 802.1x and also provides a policy engine; an Infoblox Core Network Services appliance with an IF-MAP client integrated with the DHCP server; and an Infoblox Orchestration Server appliance that provides an IF-MAP server.

The Juniper IC has the ability to dynamically configure firewall policies; however, to do so it requires the IP address of an attached device (because firewall rules are based on IP address). This is where IF-MAP comes in. First, the end device plugs into the 802.1x switch, which challenges it to authenticate. If it's a dumb device or any PC without a supplicant (i.e. one not owned by ABC Co.) the device provides its MAC address as part of 802.1x authentication. Based on this the Juniper IC communicates with the switch and enables the port. It also publishes the MAC address and a session ID to the IF-MAP server, and posts a subscription on the MAP server asking for notification of any changes associated with the MAC address just published.

With the switch port enabled, the end device issues a DHCP request, which is fulfilled by the Infoblox DHCP server. The Infoblox DHCP server publishes the IP-MAC address link to the IF-MAP server with metadata indicating that this represents a DHCP lease.

Publication of the IP/MAC link to the IF-MAP server triggers the subscription that had been posted by the Infranet Controller, so the IF-MAP server sends the IP address associated with device's MAC address to the Infranet Controller (along with the session ID). Now, with the IP address known, the Infranet Controller can automatically provision the firewall (and other devices, such as IDS's.) with policies appropriate for the endpoint. The Infranet Controller also posts a subscription on the IP address, so that it can be advised immediately if something happens with that IP. If at some point another IF-MAP enabled device, like an IDS, detects virus or worm traffic from the device's IP, it can publish an event to the IF-MAP server, referencing the IP address. That will trigger the IF-MAP server to send the event to the Infranet Controller, which can then send an update to the firewall, cutting off the endpoint from the rest of the network.

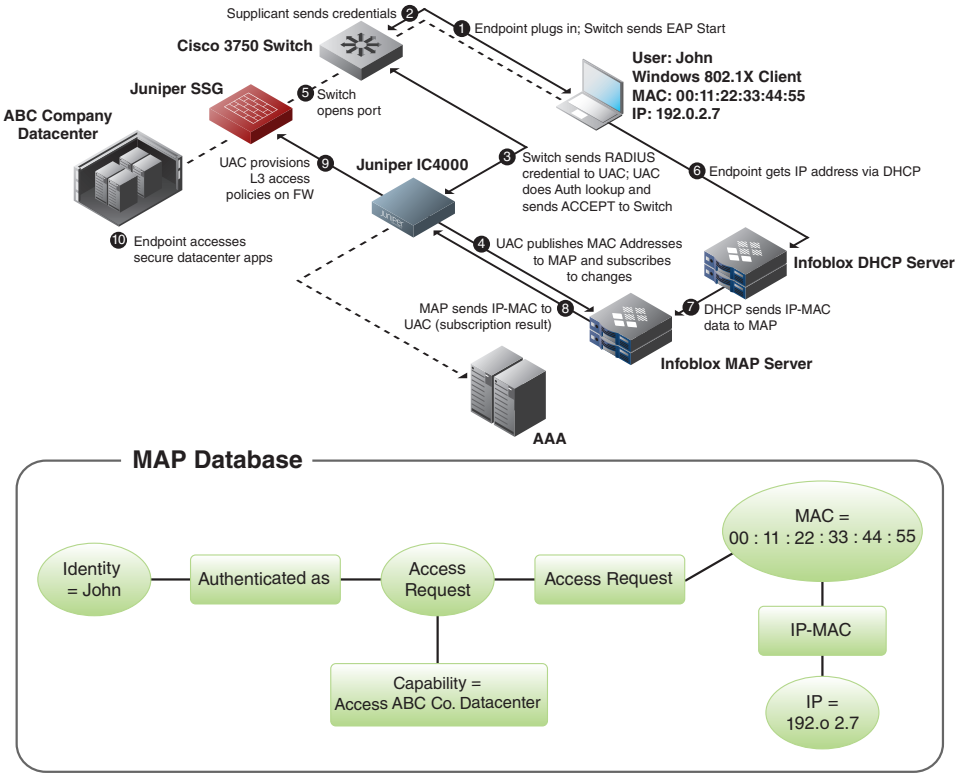


Figure 2: IF-Map enables the Juniper IC and the Infoblox DHCP server to update one another without direct integration between the two systems.

Physical Access Control/Logical Access Control Convergence (PAC/LAC)

The scenario above can be taken a step further with the addition of an IF-MAP compatible physical access control (PAC) system, such as the one available from Hirsch Electronics. The Hirsch system can publish metadata to the IF-MAP server that associates a user's location with their identity based on the last door that they badged through. With this additional information, a policy server can dynamically enforce a policy that requires a user to be in the room with their PC in order to get or maintain access to the network. By subscribing to changes in user location, the policy server can receive instant updates when a user changes location, and cut off access to the network or specific applications if a user leaves their PC unattended.

Reporting for Compliance

Many IT organizations today are faced with escalating requirements for compliance reporting—specifically, for documenting that the various elements in their infrastructure are at required patch levels and are configured consistent with company standards. There are few (if any) systems on the market today that can meet this requirement across multiple vendors' products. IF-MAP provides a powerful basis for storing "gold standard" configurations, for comparing the actual state of device configurations against the gold standard, and for providing the data needed to document compliance.

Virtualization, Cloud Computing and IT Automation

Compared with their physical counterparts, configuring virtual servers is highly automated. Virtual management tools, such VSphere™ from VMware, automate the process of provisioning a virtual machine (VM) image, and can easily move an image from one physical server to another—so-called VMotion. If VM images are confined to the same VLAN, it's generally possible to move them without making any significant network changes. But if a VM needs to be moved across VLAN boundaries, it generally requires reconfiguration of network and security systems, including routers, firewalls, load balancers, DNS and other network elements. Today, these changes are typically implemented manually and limit the ability to gain the benefits of virtualization that accrue with the ability to dynamically move workloads—including disaster recovery, capacity bursting, and least-cost computing.

IF-MAP provides an ideal integration point for coordinating the many diverse elements of an IT infrastructure. A MAP can be used to maintain a real-time model of the state of all of the elements in a network, including both endpoints and infrastructure. The existence of an accurate model of a network is an essential element of any system that can fully automate network provisioning and enable large-scale VMotion. By contrast, existing CMDBs are ill suited to capture the dynamic relationships in virtualization environments due to their relatively static and complex schemas.

The Open Cloud Consortium, (www.opencloudconsortium.org), an independent member-driven organization that supports the development of standards for cloud computing and frameworks for interoperating between clouds, has started work on modeling clouds using IF-MAP. They've established an Intercloud Testbed that will provide metadata services to support cloud interoperability. Figure 3 below shows some initial ideas for modeling clouds using IF-MAP.

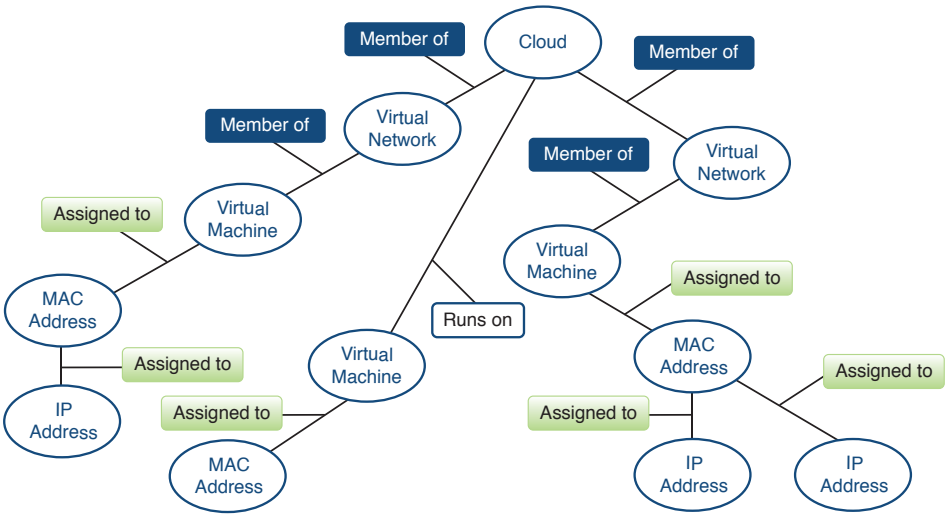


Figure 3: IF-MAP can be used to model cloud computing environments and facilitate dynamic movement of workloads between clouds.

Supply Chain Management

The availability of low cost GPS and WiFi-based network location technology is making it easy and inexpensive to add location context to applications. Existing wireless access points are already capable of providing a network location engine with the information necessary to triangulate the position of anything with a WiFi (802.11) radio, be it a laptop, a PDA or an asset tag. Manufacturers are installing 802.11-based asset tags on high value parts and tools so that they can track and find them in the factory, and are looking to establish cloud-based IF-MAP services that can enable the tracking of asset from part supplier to factory to warehouse, and out to the end customer. Hospitals have started to install 802.11-based tags on critical (and expensive) equipment, such as portable x-ray machines and pumps, and even on patients and physicians, so that they can be easily located—and detected if they leave the facility without authorization. Using IF-MAP, the location data can be made available easily to network security and physical security systems so that their policy decisions can be enriched with location data.

Smart Grid

Achieving the Smart Grid ideal of a smarter, more efficient and less costly electrical energy infrastructure requires the ability to rapidly gather and analyze enormous amounts of data and coordinate many independent systems—including electrical generation plants, transmission systems, distribution systems, metering systems, and energy consuming devices. This information must also interact in real-time with network security, physical security and other systems to ensure the integrity of the grid. IF-MAP is ideally suited as a technology for aggregating, correlating and distributing information to and from all of the touch-points necessary to operate a Smart Grid.

Transition and Adoption

As with any new protocol, mass adoption of IF-MAP will not occur overnight. Even for organizations intent on automation, it's expected that IF-MAP will co-exist with other management protocols and approaches for many years to come. In fact, the IF-MAP specification is designed with such a transition in mind on two levels.

The very nature of IF-MAP allows for vendor adoption through the self-definition of relevant metadata. Companies and organizations can begin devising their IF-MAP implementations today, creating IF-MAP extensions that are specific to their product and industry. This allows them to gradually experiment and introduce IF-MAP into their product set while continuing with their existing management frameworks.

Although not specified as part of the standard, IF-MAP servers will likely add schema import and validation to their feature sets. This will allow the IF-MAP server to import the vendor- or organization-specific XML schema and use it to parse and validate input of incoming requests.

At the same time, IF-MAP gateways will allow organizations to gradually transition to the new protocol. Much as the early multi-protocol routers converted between legacy protocols before IP became dominant, the open nature of IF-MAP makes it possible for any organization to convert between SNMP, syslog, Netflow, and others to IF-MAP, and vice versa. Given the inherent differences between the protocols and their intended use cases, however, the number of instances where SNMP and IF-MAP will compete are expected to be the exception rather than the rule. While IF-MAP could in theory replace SNMP for element management over time, the real value of IF-MAP lies in its ability to do those things that SNMP and other protocols don't do: Specifically, to aggregate, correlate and distribute data from multiple sources dynamically and to provide immediate for support for any new metadata.

Any system that implements an IF-MAP client can have access to all of the data it needs to make better decisions by communicating with an IF-MAP server. Integration of the IF-MAP client stack into a product is relatively simple. IF-MAP client stacks are available for several programming languages, and some vendors have demonstrated IF-MAP client integrations in a matter of days.

Join the Age of Orchestration

The introduction of automation has become necessary for organizations as they move to ITIL best practices and machine-to-machine coordination. But automating individual teams is only the first part of the problem. As networks expand, inter-team and inter-department coordination becomes a necessity if organizations are to achieve the ideals of ITIL.

IF-MAP is the only standards-based approach to solving those problems. The IF-MAP architecture gives any team the vehicle to share essential information with any other team. The protocol's extensible architecture accommodates a limitless range of industries and business problems. Its ability to aggregate and associate relevant information makes IF-MAP unique from any other management framework created. With built-in security, IF-MAP is well suited to applications that require very high security.

As with any standard, the value grows exponentially with the number of vendors that support it. Several visionary vendors are already fielding IF-MAP compatible products because doing so differentiates their products and provides competitive advantage. Over time, the mere inclusion of an IF-MAP interface on a product should not be a differentiator, any more than supporting an SNMP interface is a differentiator. Rather, inclusion of IF-MAP can differentiate products by enabling them to take more intelligent actions based on data from a wide variety of sources and domains. When this happens, users will benefit from smarter systems that are much easier to assemble and maintain than those built using today's labor-intensive and brittle integration approaches—and vendors will see expanded markets for their products. In the meantime, there are several actions that end users can take to accelerate IF-MAP adoption:

1. Identify infrastructure and applications in your environment that could be improved by using IF-MAP technology, such as network access control, IT automation, PAC/LAC integration, cloud computing, and compliance reporting.
2. Identify the products that need to support IF-MAP to enable your key application(s).
3. Contact vendors that are supporting IF-MAP.
4. Ask your other vendors when they will include IF-MAP support in their products.
5. Include support for IF-MAP as a requirement in RFIs and RFPs.
6. Join the Trusted Computing Group (www.trustedcomputinggroup.org)

IF-MAP has the potential to do for coordination what IP did for connectivity. The possibilities are limited only by our imagination. End users and vendors who adopt and implement this new technology stand to reap significant rewards.

For More Information

Visit http://www.infoblox.com/solutions/overview-if-map.cfm, or send email to info@infoblox.com.

TNC, IF-MAP, the IETF and Other Standards Bodies

IF-MAP is a component of the TNC architecture that provides a standardized infrastructure for sharing information. The TNC architecture is built around three entities—an access requestor (AR), a policy enforcement point (PEP), and a policy decision point (PDP). An AR is any endpoint, such as a laptop, initiating a connection. The 802.1x environment would call the AR a supplicant. Client hardware and any software supporting authentication and assessing endpoint security are included in the AR. A PEP is any device or system, such as a switch or firewall, performing an enforcement action, such as blocking network access. The PEP also controls the level of access granted to the endpoint. The PDP is typically a policy server or management system where IT defines and distributes the policies implemented by the PEPs. The PDP also communicates with the authentication server and to pass verification information to ARs.

IF-MAP's MAP Server and MAP clients extend the TNC architecture for communication with other systems. The MAP Server, or simply MAP, stores state information about devices, users, and traffic flows in a network. MAP Clients are the network systems or applications that publish information to a MAP Server, search the information in a MAP Server, and subscribe to notifications from a MAP Server when information stored in the server changes.

IF-MAP is an open standard that can be adopted by communities of related vendors, service providers and end users in applications beyond network security. IF-MAP can thus be used by other standards bodies in much the same way as it's used by TNC: Specifically, as a component that extends the standards to enable easy integration with previously unrelated systems.

The IETF and the TCG have been working together to gain universal agreement on NAC protocols. Towards that end, the IETF has adopted two of the TNC protocols (IF-TNCCS and IF-M, used between the Access Requestor and Policy Decision Point) as IETF RFCs—respectively called PB-TNC and PA-TNC. Additional TNC protocols will also be introduced as IETF RFCs, including IF-MAP.

About Infoblox

Infoblox (NYSE:BLOX) helps customers control their networks. Infoblox solutions help businesses automate complex network control functions to reduce costs and increase security and uptime. Our technology enables automatic discovery, real-time configuration and change management and compliance for network infrastructure, as well as critical network control functions such as DNS, DHCP and IP Address Management (IPAM) for applications and endpoint devices. Infoblox solutions help over 6,500 enterprises and service providers in 25 countries control their networks.

CORPORATE HEADQUARTERS:

+1.408.986.4000

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32.3.259.04.30

info-emea@infoblox.com

APAC HEADQUARTERS:

+852.3793.3428

sales-apac@infoblox.com