

OVERVIEW

AT A GLANCE

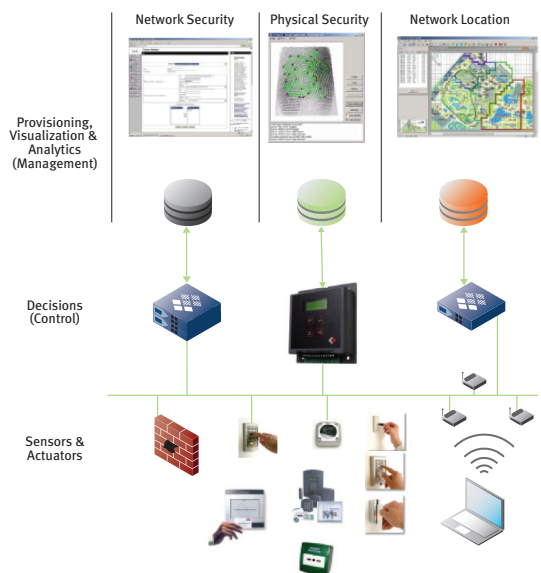
IF-MAP does for coordination & collaboration what IP has done for connectivity.

Effective use of information is essential if CIOs are to improve their organizations agility. The hospital administrator who knows patient status and location and can quickly locate equipment can dynamically reschedule services and reroute meals and medications to improve care, shorten stays and avoid errors and liability. The factory manager who can always locate critical parts and tools on the factory floor (or throughout the supply chain) can decrease cycle time, minimize inventory and eliminate lost hours and production delays.

Yet all too often, IT solutions fall short of their potential precisely because sharing essential information between business systems remains impossible or too complex and costly. Asset management systems can track people and devices, but rarely exchange that information with HR systems or enterprise applications. Network security systems don't share information with physical security systems. Manually stitching together these different applications is unfeasible as IT must incur high costs each time an application is changed, added or removed from the network. The time when corporate networks were fragmented by a jungle of networking protocols may be gone, but different applications and systems are as inaccessible to one another today as when they ran over SNA and IPX and AppleTalk.

The answer is a new technology standard called InterFace to Metadata Access Points—or "IF-MAP"—from the Trusted Computing Group (TCG) [<http://www.trustedcomputinggroup.org>]. IF-MAP standardizes the way devices and applications share information with one another. It does for coordination and collaboration what IP has done for connectivity. IF-MAP has been developed by senior engineers from a number of companies that are part of the TCG's Trusted Network Connect (TNC) subgroup, which includes HP, Juniper, McAfee, Microsoft, Symantec, and many other industry leaders.

A Network of Silos



Devices may share a common IP network, but still do not communicate with one another

The Third Generation of Network Computing

Today's IT networks are poised for the next generation in network computing. During the first generation, the IP stack won the protocol wars replacing SNA, AppleTalk, IPX and more as the standard for connecting all computers and computer-related peripherals and devices.

During the second generation of computing, IP emerged as the universal connection for anything—not just computers and computer peripherals. Our phones and cameras, sensors and actuators of all kinds—even parking meters—can share a common IP infrastructure, but continue to function independently of one another.

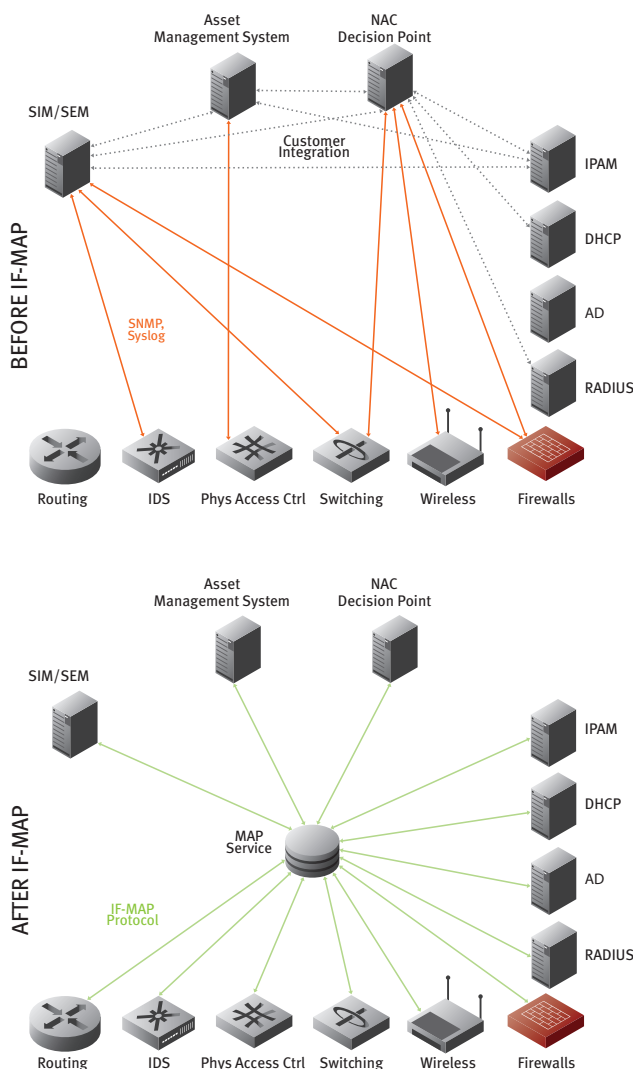
In the third generation of computing, we enable all connected systems to work together. Any system or application connected via the IP network will be able to easily share information with any other

OVERVIEW

application or system—security and business policies permitting. A new array of intelligent, automated systems will be created, with consequences as profound as the adoption of IP for connectivity.

IF-MAP is a key enabler behind this third-generation of computing. The technology allows systems and applications to easily share data of all types, in real time. More specifically, IF-MAP defines a protocol and associated database used by applications and systems to publish information, subscribe to changes in information of interest, and search for relevant data. It's analogous to Facebook for network devices and systems, and can be used entirely within a company as well as between and among different organizations.

The IF-MAP Network Transformation



Why a New Protocol?

The challenge of collecting and disseminating data in real time among many applications and systems carries with it a unique set of requirements. Meeting this challenge requires the ability to accommodate diverse data types, data relationships and many, many devices and entities:

- Unstructured Data** – There's no way to anticipate all of the different types of information that applications and systems may want to share on the network. There's network-related data, such as IP addresses and MAC addresses, and identity information, such as user names, roles and access rights. There's device information, such as the type of device, its manufacturer, and asset tag; physical data, such as location, temperature, and the state of the device (whether it's on or off, busy or free), etc. A data sharing system must be able to accommodate both pre-determined as well as user-defined data types without major effort.
- Unstructured Relationships** – Just as it's impossible to anticipate all of the kinds of data that will be shared, it's equally difficult to anticipate the relationships between those elements. A user can be associated with many devices, and a device can be associated with many users. The same is true for related pieces of data. Attempting to capture all the potentially useful relationships using pre-defined, static structures quickly becomes restrictive and renders the system unable to adapt to real customer needs. Instead, an effective design must support emergent relationships where associations between users, devices and the related data are learned from the network itself.

OVERVIEW

- **Scalability** – With the rapid increase in the number of devices and systems that are on networks, a coordination system needs to scale to many millions of devices and data elements, and must be able to handle real-time transactions among many thousands of systems.

No prior technology meets these requirements. Relational databases and directories, such as LDAP, require pre-defined data types, data structures and hierarchies. They were not designed to support unstructured data and unknown relationships.

Infrastructure monitoring and management protocols, such as SNMP and Syslog, do not have an associated database technology, so while they're effective for exporting information about the status and activities of different devices and systems, there's nothing in the SNMP or syslog protocols that correlate information from multiple systems and support collaboration. Similar to working with proprietary APIs, integration via SNMP and syslog typically requires a significant integration effort and is more effective for monitoring and management applications than for real-time collaboration and coordination.

A New Approach

By contrast, IF-MAP is built around a new, more flexible, and scalable design that reduces the complexity and cost of system integration, enabling new worlds of collaborative systems and applications.

IF-MAP uses a publish/subscribe/search paradigm, as exemplified by Web applications and services. There is no pre-defined global structure for an IF-MAP database; rather, the global database structure (schema) emerges as each application and system publishes information to the IF-MAP service. Another key operation supported by IF-MAP is subscription. Systems compatible with IF-MAP can subscribe to changes in data of interest—such as a new device coming onto the network, or a user changing role, or an item moving from one location to another—and receive updates automatically.

These three operations—publish, search, and subscribe—are the simple yet powerful primitives for all IF-MAP transactions. This reflects what may be IF-MAP's greatest asset—its simplicity. Integrators working with IF-MAP have been able to deliver solutions using IF-MAP compatible systems in days rather than the weeks and months commonly required to integrate disparate systems.

Business and IT Impact

The Web Services model exemplified by SOA and related architectures has taken hold within IT organizations because it significantly reduces the time and cost required to develop, deploy and maintain applications. The resulting applications make organizations more efficient, more responsive and more compelling for their customers. The same is true for IF-MAP: A few of the initial use cases emerging from IF-MAP—barely the tip of the iceberg—include the following:

- **Application Security** – Some organizations have hundreds of applications that need to know if an employee or contractor’s status has changed and they’re no longer working for the company. Any delays in de-provisioning unauthorized users expose organizations to risk and liability. Having every application continuously poll the identity management system to look for changes is impractical. But by embedding an IF-MAP client stack in the HR system and in each application, a fairly simple task, applications can subscribe to changes in user status. They’re notified immediately by the IF-MAP service if the identity management system publishes a change in a user’s status from “employed” to “terminated”.
- **Cyber/Physical Security Convergence** – All organizations struggle with preventing external hackers from hijacking their WiFi networks. With easy access to information from a building’s physical access control system, a network security system can limit network access only to employees that are in the building or to registered building visitors.
- **Theft Prevention** – Hospitals and higher-education institutions grapple with stolen equipment all the time. With IF-MAP, a building security system can access information from facilities management and asset tracking systems, and sound an alarm or even lock the doors if expensive equipment starts moving to an exit.
- **Improved Customer Care** – Utilizing location information allows organizations to read-just their processes to provide better service and improve their bottom line. Hospitals can use IF-MAP to reduce the time needed to treat patients while improving customer care. By understanding a patient’s location, an IF-MAP-enabled care management system could identify if a patient is out of their room and waiting for a test at lunch time. The system can locate alternate equipment, or deliver their lunch while they wait—and also provide the patient’s temperature to the nursing station.

Not only does IF-MAP hold the key for revolutionizing the way businesses address strategic problems, the architecture will also change the way IT operates. Initially, IF-MAP was designed to support network access control (NAC) and to those ends it has extensive security features built in. But the applications of the IF-MAP architecture go far beyond network security:

- **Data Center Optimization** – Within the data center, IF-MAP allows organizations to integrate information from physical servers, power systems and data center air conditioning systems with virtual server management systems. This makes it possible to cut power costs by automatically finding available server capacity and moving work-loads to shut down unnecessary servers.

OVERVIEW

- **Automated Network Provisioning** – IF-MAP will allow IT to automate the process of virtual machine provisioning and deployment. Instead of the network services team having to coordinate with the server team to deploy or move a virtual machine (VM), all of the necessary policy and state information can be published in IF-MAP database. Automated provisioning of networks is not only more effective than today's manual processes, it is also a requirement to support dynamic environments such as private and public clouds.

IF-MAP Status

The initial version of the IF-MAP specification was released in May, 2008, and an update was released in May, 2009. Since then a number of companies, including vendors of network equipment, network security systems, wireless location systems, physical security systems and others have demonstrated and released IF-MAP compatible products. For such a young standard, the adoption rate has been impressive. Importantly, a number of large enterprises are deploying IF-MAP and are using it to improve existing processes and support new initiatives. And the standard continues to evolve as more use cases are added.

What Next?

In principle, IF-MAP doesn't make possible anything that can't be done already today with existing protocols and custom programming, just as network connectivity was possible before IP became the universal data communications protocol. By standardizing and simplifying information sharing, IF-MAP has the potential to transform not just IT, but also whole organizations and industries. This will not occur overnight, but early support from vendors and end users suggests that IF-MAP can deliver immediate benefits today and is a powerful architecture for the future.

For more information visit www.infoblox.com/solutions/overview-if-map.cfm