802.11r Holds Promise Of Secure Wi-Fi Mobility

Upcoming IEEE spec to reduce hand-off delay between access points

BY DAVE MOLTA

FOR WI-FI TO SERVE AS A FOUNDATION for mobile applications and voice, networks must provide secure mobility. And to achieve that, mobile devices need robust authentication and encryption, fast roaming and QoS (quality of service).

Enterprise IT pros should pay attention to the IEEE's 802.11r fast-roaming task group, whose standard is likely to make its way to market by late 2007 or early 2008, with broad adoption by enterprise solution providers in 2008.

The arrival of 11r is timely. Voice over Wi-Fi is expected to generate increased interest as more dual-mode Wi-Fi/cellular solutions are delivered this year. Many enterprises have moved from VPNs and captive portals to WLAN security architectures built around 802.11i/WPA2. Vendors have been offering proprietary secure-mobility solutions for years, and many of the underlying foundations for 802.11r have been tested on real networks.

Given the need to integrate with 802.11i security and 802.11e QoS standards, developing a workable standard for fast roaming is challenging. Not surprisingly, 11r defines a complex architecture, though one that is not expected to require forklift upgrades of existing hardware. But getting all the software right will be difficult.

SECURITY IS EASY, MOBILITY IS HARD

The expected deployment of time-sensitive applications like Vo-Fi on enterprise networks is driving 11r. Most Vo-Fi vendors have advocated virtual WLANs dedicated to voice, with WEP encryption often serving as the shaky foundation for privacy and a variety of techniques, largely proprietary, prioritizing voice traffic.

That's yesterday. Tomorrow's Vo-Fi installations will

THE LOWDOWN

THE PROMISE / The IEEE 802.11r standard will facilitate secure mobility by reducing hand-off delay in WLANs during transitions between access points. This protocol will let more stringent security mechanisms, such as 802.11i, be employed without service interruption, which is essential for real-time apps like Vo-Fi.

THE PLAYERS / 802.11r is being developed by a task group that includes participants from **Aruba Networks**, **Broadcom**, **Cisco Systems**, **Intel**, **Motorola**, **Nokia**, **SpectraLink** and **Texas Instruments**. Expect broad support from WLAN infrastructure and client vendors, with initial availability of infrastructure offerings by the end of 2007 or early 2008. The Wi-Fi Alliance will test interoperability of products implementing fast-roaming capability in its Enterprise Voice over WiFi certification.

THE PROSPECTS / Once 802.11r is implemented, secure mobility on Wi-Fi networks will be a reality. With new dual-mode phones and fixed-mobile convergence spurring enterprise interest in Vo-Fi, 11r will meet a significant need. Meantime, enterprises looking to deploy secure voice over WLAN networks must rely on inadequate security protocols and proprietary solutions.

TIMELINE // STEPS TOWARD FAST ROAMING

{11/2005} 802.11r Draft 1 is released for letter ballot.

{11/2006} The draft of the standard reaches Version 4.0.

{Late '07} Approval of 802.11r draft standard is expected.

{Late '07/ early '08} Initial client and infrastructure products compliant with draft 802.11r are expected.

{Early- to mid-'08} Final ratification of the 802.11r standard is expected.

{Early '08} The Wi-Fi Alliance will begin offering a certification focused on Enterprise Voice over Wi-Fi.

use advanced authentication and dynamic encryption-key techniques made possible by 802.11i and QoS capabilities defined by 802.11e. Unfortunately, upgrading to these standards while still providing fast roaming between APs may be tricky. Full authentication using 802.11i, for example, can create delays of several hundred milliseconds during roaming. The new Fast BSS Transition defined by 802.11r eliminates much of the handshaking overhead.

802.11r provides a no-compromise solution for secure wireless voice, providing fast-roaming transitions of about 50 ms while preserving a device's security and QoS context. It effectively "mobilizes" 802.11i's security services and 802.11e's QoS functions. The increasing number of enterprises that have begun or completed a migration to 802.11i and WPA2 will be poised to take advantage of 802.11r; those with legacy setups will have more to do.

The IEEE's 802.11r standards initiative was established in 2004 to address 11i's limitations. The IEEE approved 11i while creating the 11r task group to address secure fast roaming. Many vendors—including Aruba, Broadcom, Cisco, Intel, Motorola, Nokia, SpectraLink and Texas Instruments—have been active in the 11r process.

The Wi-Fi Alliance is studying fast hand-off interoperability testing in its Enterprise Voice over Wi-Fi task group with a goal of releasing a certification plan in early 2008.

FAST HAND-OFF

The current 802.11i authentication process is notoriously slow. Although 11i included optional mechanisms such as pairwise master key caching and pre-authentication to minimize roaming times, these haven't been broadly implemented by vendors. In pure 11i, once a client has decided it needs to roam to a new AP, it must exchange association messages with the AP. After a user's login credentials have been authenticated, a master session key is derived. 802.11r ensures that the authentication processes and encryption keys are established before a roam takes place.

To speed up roaming, 802.11r introduces "fast hand-off." Authentication occurs only once, when a client enters the mobility domain. Subsequent roams within a mobility domain use cryptographic material derived from the initial authentication, decreasing roam times and reducing load on back-end authentication servers.

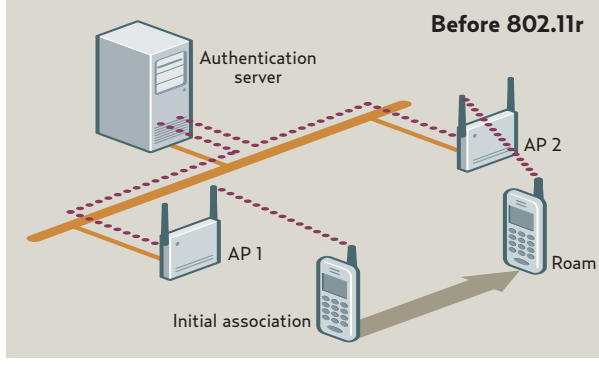
To securely cache and distribute encryption keys, 802.11r includes a new key-management hierarchy. In this multilevel setup, the highest-level key holder (a WLAN controller, for instance) has access to the original cryptographic material and is responsible for deriving keys for lower-level key holders (APs). 802.11r's key-derivation algorithms are based on a one-way hash function ensuring that a compromised lower-level key cannot be used to decipher the original master key.

802.11r also tackles QoS. Even if a Wi-Fi device establishes QoS-based resource reservation when it connects to the network, when transitioning to a new AP, QoS is not preserved automatically. An optional mechanism in 11r lets a client request QoS resources on a target AP before choosing to roam.

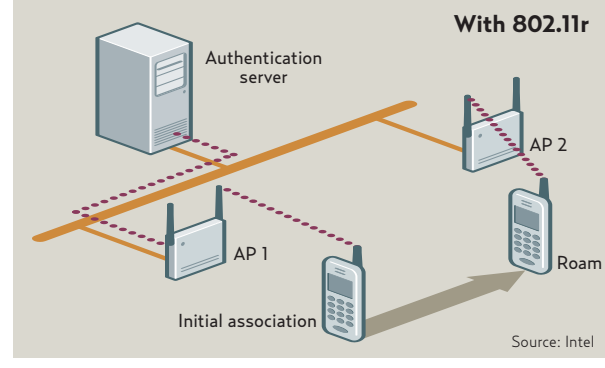
Most vendors we spoke to said they would support 11r. Aruba, Cisco and Meru have developed proprietary methods to deal with the shortcomings addressed by 11r. How fast they will migrate to a standards-based approach is uncertain, as is the pace at which client devices will be upgraded. To the degree that Cisco includes 11r support as part of its CCX certification program, the company will play a key role in promoting adoption of this standard. ■

DAVE MOLTA IS NWC'S EDITOR AT LARGE. HE IS ALSO ASSISTANT DEAN FOR TECHNOLOGY AT THE SCHOOL OF INFORMATION STUDIES AND DIRECTOR OF THE CENTER FOR EMERGING NETWORK TECHNOLOGIES AT SYRACUSE UNIVERSITY. WRITE TO HIM AT *DMOLTA@NWC.COM*. POST A COMMENT OR QUESTION ON THIS STORY AT *NWC.COM/GO/ASK.HTML*.

AUTHENTICATION BENEFITS



Under 802.11i, **each device must perform** a full 802.1X authentication with a back-end RADIUS-based authentication server to establish encryption keys when it roams between two APs.



In 802.11r, the initial association to the network still involves an exchange with the authentication server, but **roaming time is reduced** because encryption keys are distributed throughout the infrastructure before a roam occurs using 802.11r's three-tier key hierarchy.

Virtual Directories Take Hold

Open-source options lower the entry cost for small companies

BY MICHAEL CATON

DATA ONLY PROLIFERATES, NEVER CONSOLIDATES, so finding ways to access the increasing amount of customer, partner and employee data in databases and directories can be daunting. Virtual directories provide a way, regardless of where the data resides.

Until recently, this arena was dominated by commercial tools, but recent open-source innovations have shifted the landscape. Open-source groups MyVD Virtual Directory and Safehaus Software Foundation are offering options that may appeal to small companies.

The main advantages of a virtual directory compared with a metadirectory include faster deployment time, the ability to avoid synchronizing data from other sources and security efficiencies. Commercial virtual directories are less expensive over time than metadirectories or custom-built ones. Beyond that, open-source alternatives help smaller companies adopt the technology because they are less expensive than commercial products.

THE LOWDOWN

- **THE PROMISE** / Virtual directories let organizations gather information from many data sources and present that information from one interface, securely. They give companies access to existing information without having to re-create it or develop a new app. New open-source options could bring the cost of virtual directories within reach of small companies.
- **THE PLAYERS** / **Radiant Logic** was one of the first vendors with a virtual-directory product. **MaXware**, **Persistent Systems** and **Symlabs**, other early-to-market vendors, focus primarily on virtual directories and ID management. **BMC Software**, **CA** and **Novell** also play in this arena. **Microsoft** and **Oracle** have virtual-directory offerings as part of their directory- and ID-management products. Two open-source groups, **MyVD Virtual Directory** and **Safehaus Software Foundation**, are attempting to gain a foothold in the arena. Surprisingly, **IBM** doesn't have a true virtual directory, but it does have directory-synchronization products and partners with vendors such as **Radiant Logic** and **Symlabs**.
- **THE PROSPECT** / Virtual directories give companies effective ways to access data without undertaking a metadirectory or application-integration project that can lead to data synchronization and infrastructure problems. The market is expected to double in the next three years, to $1.8 billion.

One drawback of virtual directories is that they introduce a layer of middleware between the user and the authoritative system of record, which may translate into slower performance than users would experience with the authoritative system; this may be a problem only with apps that require a high service level, such as those for call centers. In addition, a virtual-directory application must be deployed with the same level of fault tolerance as the directory and database applications it will interact with.

USING THE DATA YOU HAVE

A virtual directory (and a metadirectory, for that matter) presumes two facts: The information users need exists in some enterprise application; and having users access that application directly is impractical, inefficient or inappropriate. In addition, companies may want to present data from multiple applications in a single view to give users all the information they need in one place. Without a virtual directory, companies would be faced with using a metadirectory to pull that information into an additional, more broadly accessible data store or with extending that information into an application to which users have been granted access—a customer-service program, for instance, through which users would see customer-contact information from a CRM application and shipping information from a logistics and supply-chain application all on a single screen.

With a metadirectory, IT admins must extend the metadirectory or application schema, then provide a mechanism that synchronizes data. The downsides of this approach include costly development, unreliable synchronization and information that is only as up-to-date as the last synchronization. In organizations subject to regulatory requirements, these changes also must be documented and justified for audit purposes.

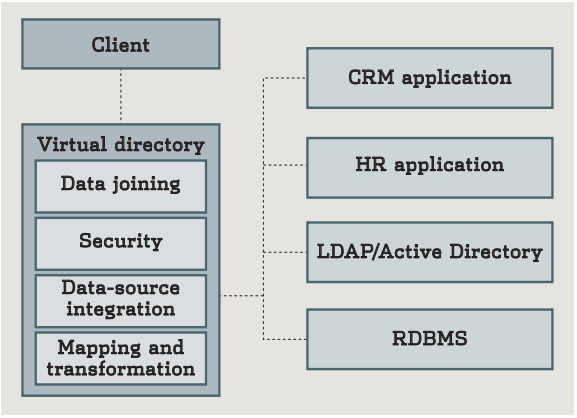
Virtual directories, in contrast, let users access data structures already in place, regardless of format, while maintaining the authoritative app's security structure. Rather than replicate existing data as a metadirectory would, a virtual directory acts as a proxy to the authoritative app, passing security credentials, accessing records and transforming data so that it can be displayed to users in the proper context.

Besides faster deployment and synchronization benefits, in comparison with metadirectories, virtual directories bring security efficiencies. They let companies work within the security parameters of existing directory and database apps rather than creating a new

security model. The virtual directory also can act as a proxy to other apps. It can act as an identity firewall without forcing a company to invest in a federated ID-management product. A virtual directory lets companies re-architect how users view ID information without changing underlying apps. Although initial costs for virtual-directory software are comparable to metadirectory and custom-built products—typically about $50,000—the lower management and maintenance overhead makes it a cheaper alternative.

A practical application of a virtual-directory application would be to consolidate user data for an employee directory in a corporate portal. Portal information could be pulled from the human resources management system, an e-mail server, a knowledge-management application and CRM system, for instance.

VIRTUAL DIRECTORIES: CONSOLIDATED ACCESS



The virtual directory gives end users a single view of directory data in a variety of enterprise applications. It handles connections to other applications, ensuring security levels are honored, and presents the requested information to the client.

DEVELOPER ROLL CALL

In June 2006, Safehaus Software Foundation launched Penrose 1.0, an open-source virtual-directory project. Penrose is a Java-based server that can run as a standalone application or as a back end for ApacheDS (Apache Directory Server) or OpenLDAP. Although Penrose doesn't directly integrate with specific database applications—it uses JDBC—it is an open-source product with a plug-in architecture, so companies should be able to build their own connectors or find third-party connectors.

MyVD Virtual Directory is a Java-based open-source project hosted on SourceForge. MyVD is still in development (the .80 version was introduced in February), but it will support custom connectors, called inserts, to manage integration with other applications that hold ID data.

It's not surprising that Microsoft and Novell provide virtual directories, but many of the early third-party metadirectory vendors that created directory-synchronization tools also offer virtual directories. MaXware, Persistent Systems, Radiant Logic and Symlabs were among the first with virtual-directory products. Another early developer, Octet String, was acquired by Oracle in 2005. Oracle is making the Octet String products part of its suite of ID-management apps. Although IBM offers the middleware, database and directory products that should let it play in this space, partners such as Radiant Logic and Symlabs help IBM deliver virtual directories.

Despite bigger players such as Oracle entering the fray, dedicated directory management vendors, including Radiant Logic and Symlabs, are the market leaders in terms of share and innovation.

ID management is a fundamental application of the technology, and vendors with ID-management systems, such as Microsoft, also offer products. This means that conventional systems-management vendors, such as BMC Software and CA, also offer virtual directories through an OEM agreement or partnership with a virtual-directory software vendor. ■

MICHAEL CATON IS A FREELANCE WRITER WITH 18 YEARS EXPERIENCE EVALUATING TECHNOLOGY PRODUCTS FOR TECHNOLOGY BUYERS AT LARGE ORGANIZATIONS. MOST RECENTLY HE HAS BEEN REVIEWING CRM AND MESSAGING AND COLLABORATION PRODUCTS. WRITE TO HIM AT *MCATON@NWC.COM*. POST A COMMENT OR QUESTION ON THIS STORY AT *NWC.COM/GO/ASK.HTML*.

TIMELINE // DIRECTORY EVOLUTION

{1993} Tim Howes and Steve Kille develop LDAP, established from X.500 telecommunication directory standard; Novell introduces X.500-compatible Novell Directory Services.

{1996} 40 software companies, including Netscape, endorse LDAP.

{Feb. 2000} Microsoft introduces Windows 2000 Server and Active Directory.

{2001} Radiant Logic introduces first virtual directory product; Symlabs founded.

{Nov. 2005} Oracle acquires virtual directory software developer Octet Systems.

{June 2006} Safehaus Software Foundation releases open-source virtual directory application, Penrose 1.0.