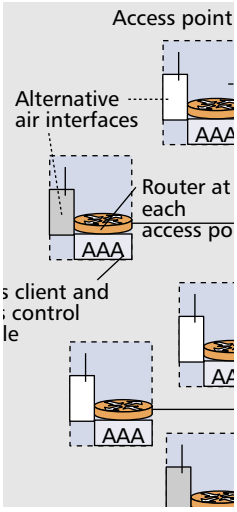
PUBLIC ACCESS MOBILITY LAN: EXTENDING THE WIRELESS INTERNET INTO THE LAN ENVIRONMENT

JUN LI, STEPHEN B. WEINSTEIN, JUNBIAO ZHANG, AND NAN TU
NEC USA INC.



Public wireless communications will increasingly extend into wireless LAN environments in order to meet the ubiquitous access, high data rate, and local services demands of future Internet appliances.

ABSTRACT

Public wireless communications will increasingly extend into wireless LAN environments in order to meet the ubiquitous access, high data rate, and local services demands of future Internet appliances. This article offers architectural guidelines for relatively large-scale IP-based WLAN environments configured to accept public access by mobile/portable appliances. By relying on IP-level service mechanisms at the access point, independent of the wireless medium access technology, the WLAN can simultaneously support different air interfaces, franchises for multiple service providers with effective authentication and billing, and a multisegment LAN environment including handoffs. QoS across the air interface is not addressed; this article rather concerns architecture of the wired LAN environment in which wireless access points are imbedded, and its capabilities for QoS and support of the business model.

INTRODUCTION

The rapid evolution of Internet services and wireless technologies have stimulated the development of both cellular mobile and wireless LAN (WLAN) access systems for the wireless Internet, providing users convenient Internet access and location-sensitive applications. Most existing WLAN access systems are either private, as in company or campus networks, or by subscription to the services of a WLAN operator. This article examines the functions and architecture of an Internet Protocol (IP)-based public access mobility LAN (PamLAN) that extends Internet access WLANs with capabilities for support of multiple air interfaces and multiple "virtual operators," local IP mobility, location-dependent services, and quality of service (QoS) traffic engineering. These capabilities will provide high-performance access capabilities for a wide range of future Internet appliances, from laptops and enhanced telephone handsets to Internet radios and digital cameras and camcorders.

The PamLAN is actually a wired local network supporting enhanced wireless access points. This article addresses only the service and QoS features of this supporting network, which is presumed to connect to a future differentiated services (DiffServ)-capable Internet, not the QoS challenges of the air interface. The IP and other new features of the access points can be implemented simply and at minimal cost as software running on standard personal computer processors. The concept of IP-capable access points is already established in references such as [1], although the virtual operator functional architecture has not, to our knowledge, been developed in previous publications to the extent described here. For example, the focus of [1] is primarily on the validity of a generic AAA framework, whereas in this article both framework correctness and implementation efficiency are evaluated in a public access wireless LAN context. Additionally, some of the issues not addressed in [1], such as mutual authentication between mobile stations and access points, are taken into consideration and resolved in our solution.

The PamLAN implements a business model serving three stakeholder categories:

- The network operator, such as an airport or hotel operator, who actually provisions and maintains the network.
- Third-party services providers such as Internet service providers (ISPs) and public communications carriers, who buy franchises from the PamLAN operator to offer data access services to their subscribers without having to invest in network facilities. These third-party service providers become "virtual operators" within the PamLAN.

Jun Li is now with Thomson Multimedia Inc.

Stephen B. Weinstein is retired from C&C Research Laboratories, NEC USA Inc.

Work described in this article was done while both authors were with C&C Research Laboratories, NEC USA Inc.

1070-9916/02/$17.00 © 2002 IEEE

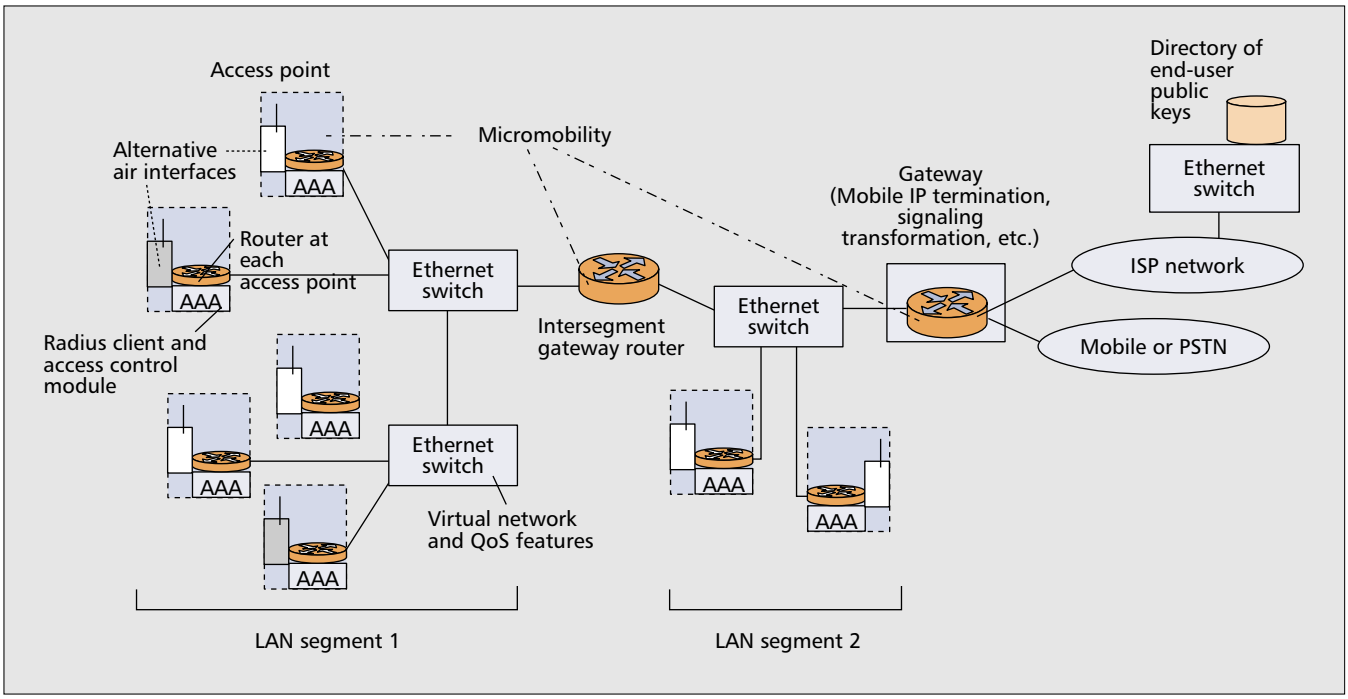


Figure 1. *Illustrative physical architecture of a PamLAN.*

- Individual end users, who obtain service based on their existing relationships with third-party service providers and see the charges appear on their regular statements from those providers. They enjoy access speeds far surpassing the relatively low-rate Internet access services of the digital cellular (2G) mobile telephony network and even envisioned third-generation (3G) mobile networks [2].

PamLANs as defined in this article may have multiple LAN segments and be installed in office buildings, airports, hotels, universities, shopping malls, and other campus-scale locations. They can be built on existing LAN infrastructure, simply adding wireless access points, avoiding costly new network deployments.

Public service operators are being attracted to this kind of private (enterprise LAN) networking, wired and wireless, in order to provide the capacity and performance expected by their customers. For a broad range of evolving Internet applications, including Internet audio and video multicasting and interactive multimedia applications, high speed and low delay are essential. The public cellular mobile network cannot fully meet this demand, even with the proposed enhancements of 3G mobile communication systems providing downstream burst rates up to 384 kb/s outdoors and 2 Mb/s rate indoors. Although these rates are a significant improvement over second-generation systems, and multiple-input multiple-output (MIMO) antenna technology may increase spectral efficiency significantly, there will still be limited bandwidth and high prices arising from the huge amounts paid by operators in spectrum auctions. This is an intrinsic problem because the 3G mobile system, like the 2G system, aims to provide continuous coverage in reserved spectrum. The capacity of the system is unlikely to be scalable to the investment cost.

WLAN technologies can and do provide Internet access at low cost and with high capacity. They use "free" spectrum (although, as described later, they may also implement cellular mobile microcells in reserved spectrum), are scalable, and can easily be integrated into the wired network. There is a potential problem with interference between WLANs in the unregulated spectrum, but this problem is likely to be overcome by enforcement of spectrum compatibility by the owners of properties such as airports and hotels where public access through WLANs will become serious business operations. The interference problem between IEEE 802.11 [3] and Bluetooth [4] systems, both of which may be supported by a property owner, is being addressed in IEEE 802.15 Task Group 2 (http://www.ieee802.org/15/pub/TG2.html).

The main disadvantages of present-day WLAN access services are the lack of public access (i.e., restriction to subscribers of the WLAN operator), being tied down to a single access point (discouraging applications such as listening to Internet radio while wandering through a shopping mall), and restriction to a single WLAN air interface, reducing the range of appliances, including those with cellular mobile air interfaces, it would be desirable to support.

The architecture described in this article addresses these limitations. It is a judicious combination of available technologies rather than a breakthrough in technological capabilities. The PamLAN is part of a general trend in mobility systems toward a distributed IP-based architecture, but it is our belief that the WLAN approach offers such compelling cost and performance advantages over cellular mobile systems that WLANs may become the preferred access mechanism for the majority of Internet appliance communication sessions.

PamLAN	Multiple virtual operators, each operating a VOLAN. AAA features.
VOLAN	Virtual operator LAN, extending VLAN capabilities across subnetworks for each virtual operator.
VLAN	Virtual LAN, implementing user group features such as broadcast containment within a physical LAN.

Table 1. *PamLAN/VOLAN/VLAN hierarchy.*

A Virtual Operator System

The PamLAN physical architecture (Fig. 1) relates not only to individual wireless LANs specifically associated with the cellular mobile infrastructure, but to any local communications infrastructure that connects to the Internet and wishes to support wireless access. A PamLAN could be a collection of LAN segments as illustrated in Fig. 1, or built into a metropolitan access network such as a cable data system. The virtual operators supported by a PamLAN could be any third-party service providers, including but not limited to cellular mobile operators.

Within a PamLAN, each virtual operator sees what it regards as a dedicated LAN, possibly across multiple network segments. This virtual operator LAN (VOLAN) is an independent logical LAN that conceptually belongs to a virtual operator and is managed based on the service level agreement (SLA) between the virtual operator and the PamLAN operator. It provides secure traffic separation and can be traffic engineered with QoS support. A virtual operator can, for example, provide different service qualities to users with different subscription status. The VOLAN is built from underlying medium-access-level virtual LAN [5] capabilities and inter-LAN-segment features, as described later. Table 1 illustrates the PamLAN/VOLAN/VLAN hierarchy.

AAA features are a critical component. Among the different business models for a wireless access point, the PamLAN described here focuses on a semi-trusted access point that becomes a virtual extension of a service provider's network. "Semi-trusted" is defined as:

- Trusted to properly route the mobile user's traffic to the Internet.
- Partially trusted, as a franchised operation with a business relationship with a virtual operator, not to read, alter, or spoof mobile user traffic content. This level of trust is similar to what we assume about a local ISP and is adequate for most Web browsing. For transfer of sensitive data such as credit card information, end-to-end solutions such as secure socket layer (SSL) are recommended.
- Partially trusted to report correct accounting information to the virtual operators. The solution proposed here requires service measurement by both the access point and the mobile appliance, reported to the virtual operator and crosschecked for consistency. The mobile customer cannot be spoofed because of a mobile user/virtual operator authentication process to which the access point is transparent. These measures greatly reduce the possibility of fraud and dispute.

This business model requires authentication of the access point as a genuine franchised base station, as well as authentication and authorization of the visiting user. This is a more restrictive model than that of an entirely untrusted access point, but it facilitates implementation of IP-level AAA server/client functions at access points in order to support the virtual operator.

Structural Elements and Protocol Components

The architecture of Fig. 1 is a switched Ethernet LAN with various air interfaces at the access points, possibly including both WLAN (IEEE 802.11, HiperLAN 2, Bluetooth) and cellular mobile (GSM, IS-95, IS-136, 3G) base stations. The support of cellular mobile voice services on this IP-based infrastructure would require access point capabilities not addressed in this article, but General Packet Radio Service (GPRS) data services could be directly supported.

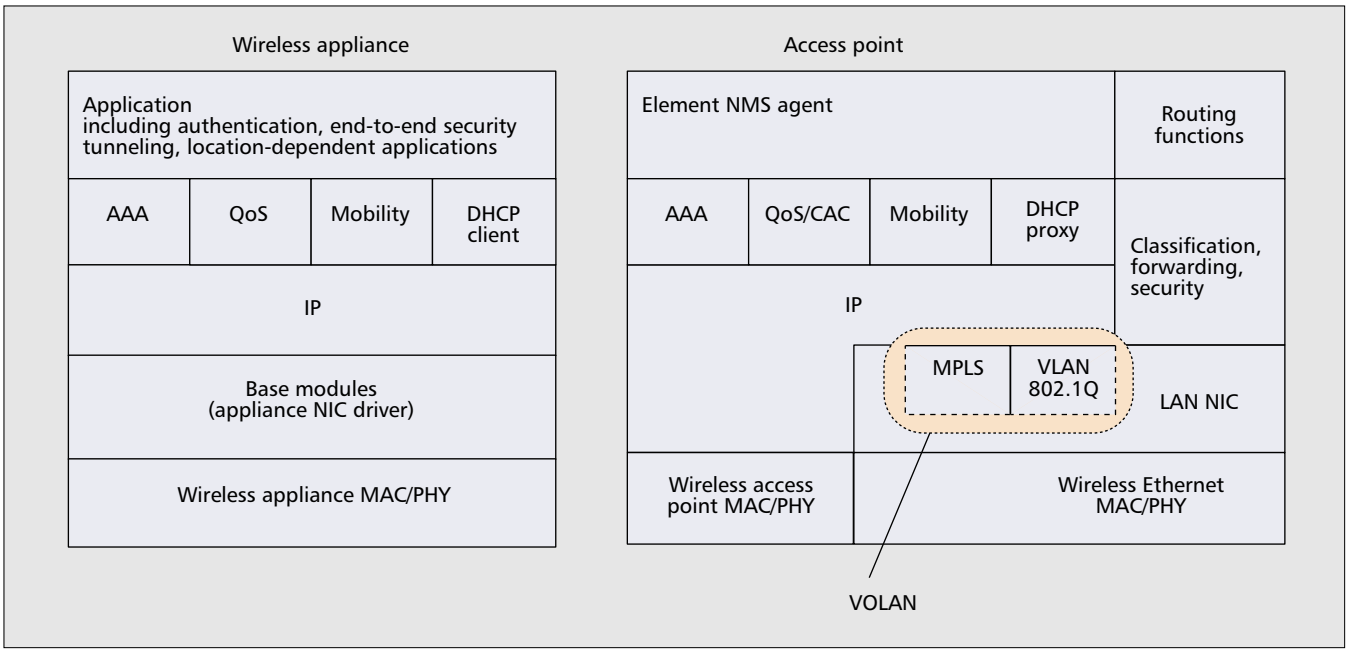
In contrast to an ordinary WLAN, in which the base station access point functions as a bridge, the access point in this network incorporates an IP access router, running proxy functions on behalf of mobile terminals. One of these proxy functions can be the base station controller for whatever air interface exists within a particular access point. This proxy controller communicates at the IP level with an IP gateway.

One or more IP gateways carry traffic toward the Internet or public networks, terminate mobile IP tunnels, and perform signaling transformations as needed. As an alternative to signaling transformations, encapsulated SS7 or ISDN control signals, as well as H.323, SIP, or other IP network-oriented signals can be transparently conveyed.

VOLAN technology is used to configure logical service networks across geographical LAN segments for different virtual operators. Within each virtual operator's VOLAN, QoS can be supported for DiffServ classes.

PamLAN utilizes standards-based virtual LAN and QoS features appearing in the Ethernet switch that is the core of each PamLAN segment. Although the Ethernet MAC protocol is still carrier sense multiple access with collision detection (CSMA/CD), a full duplex Ether switch operates with no contention, and new standards have been introduced to provide 802.1p packet prioritization and VLAN. We do not address air interface QoS issues in this article, but the IEEE 802.11e standards working group is investigating support of DiffServ and security. We assume that the Internet or other IP networking maintained by the ISP to which the PamLAN connects supports QoS features, probably in future traffic-engineered DiffServ networking, so the PamLANs QoS priorities can be mapped into core network QoS capabilities.

Finally, IP local mobility protocols have been proposed, such as cellular IP and HAWAII [6, 7] for a wireless LAN environment, to improve the performance of mobile IP, particularly faster handoff, more direct traffic routings, and more distributed and scalable connection control. We



■ **Figure 2.** *Protocol stacks at a wireless appliance and an access point of a PamLAN.*

do not endorse a particular local mobility proposal, but note the general advantage of the gateway in Fig. 1 becoming a relatively fixed address for the visiting user, so only routers internal to the PamLAN have to be informed about path changes because of movement of the user from one local access point to another. Even this requirement is reduced through the use of multiprotocol label switching (MPLS) [8] paths, as described later. A mobile appliance obtains an IP address dynamically when it enters a PamLAN and can then freely roam across the geographical LAN segments in the PamLAN without new IP address assignment.

As a brief summary, the PamLAN architecture presented here makes possible:

- IP-level virtual networks representing virtual operator franchises, supported by IEEE 802.1Q VLAN, MPLS traffic engineering, and an AAA client at each access point
- Autonomous base stations that can, within the same network, support alternative air interfaces
- DiffServ QoS services facilitated by prioritizations in IEEE 802.1p and MPLS traffic engineering
- Micromobility to facilitate path redefinition (and hence minimize delay) for access-point-to-access-point handoffs
- Potential interoperability with 3G cellular mobile systems, not addressed in this article beyond the possibility of supporting cellular mobile base stations at access points

These are significant enhancements over available public access WLANs that are simply WLANs plus security servers.

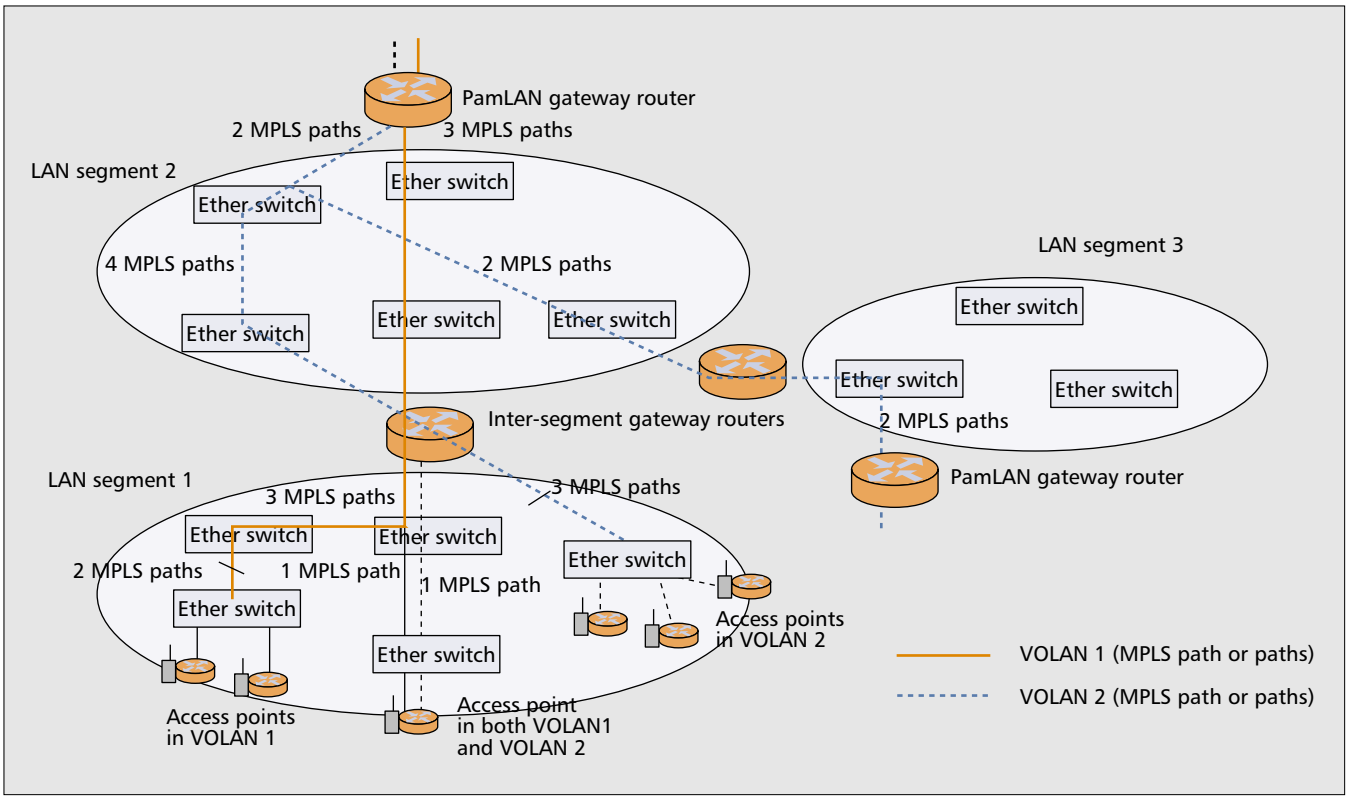
In order to provide the kind of public Internet access outlined above, the necessary protocol components must be in place in the PamLAN access network, the access points, and the visiting Internet appliances.

Figure 2 illustrates the protocol stacks in the wireless appliance and the access point. The access points host critical protocol components including DHCP proxy, agents for distributed AAA, packet filtering and classification, QoS control, and mobility management. Because the access point is router-based, these PamLAN functions can be implemented at layer 3 and above, requiring no wireless MAC protocol changes. The router approach also avoids changes to the protocol stacks in the mobile appliances, relying on existing protocol components (e.g., DHCP client, IPSec) or implemented in the application layer (e.g., authentication session). Note the combination of MPLS and VLAN in the access point, forming a VOLAN that supports the PamLAN QoS and mobility functions.

Building a Virtual Operator LAN from VLAN and MPLS

The VOLAN is a resource-sharing and traffic engineering infrastructure, possibly extending across several LAN segments, permitting virtual operators to offer independent QoS services to their respective user groups, in accordance with their SLAs. These services must not interfere with those offered to existing local users in a preexisting LAN environment in which a PamLAN may be built. The VOLAN proposed here is, as noted above, a combination of the VLAN capabilities of commercial LAN switches and the use of MPLS paths across a multisegment LAN environment.

A VLAN is a logical grouping and broadcast containment mechanism in a switched LAN environment. Switches in the LAN enforce logical group membership by forwarding broadcast/multicast Ethernet frames to the port supporting devices belonging to the group. The IEEE VLAN standard, 802.1Q, specifies a 12-bit



■ Figure 3. *Two VOLANs operating in a three-segment PamLAN.*

VLAN ID within a 4-byte section in the IEEE Ethernet header. Switches implementing 802.1Q need only examine the VLAN ID in each Ethernet frame to determine group membership.

When a PamLAN is a single switched LAN, a VOLAN is simply implemented as a VLAN by tagging all traffic of the VOLAN (i.e., of visitors associated with a particular virtual operator) with the assigned VLAN ID. QoS provisioning can be implemented using an IEEE 802.1p header, a 3-bit section embedded in the IEEE 802.1Q header to differentiate eight frame priorities.

However, in a large PamLAN with multiple routers interconnecting subnetworks, VLAN alone is no longer adequate for VOLAN provisioning. In such an environment, a VOLAN can be implemented as a chain of VLANs connected by gateway routers. The VOLAN coherence is maintained by these routers, which map a virtual operator packet to a VLAN tag when forwarding the packet into a subnetwork. Since the gateway router works at layer 3, all VLAN information from the layer 2 header is lost when a packet crosses subnetworks. It is thus not possible for the router to maintain a VLAN mapping table between adjacent subnetworks. The routers must use layer 3 information such as source and destination IP addresses to determine VOLAN membership for a packet.

There are, however, problems with this approach. In particular, all the intermediate routers in the PamLAN have to keep all the IP addresses (at least the address prefixes) of the active mobile users in order to make VLAN mapping decisions. Furthermore, because of the hop-by-hop nature of IP routing, it is difficult to effectively manage and provide service provisioning for different VOLANs. For these reasons, we propose using MPLS together with VLAN for VOLAN provisioning.

MPLS provides a simple and efficient solution in which the access points and Internet gateways handle VOLAN provisioning while all the intermediate routers are shielded from the VOLAN details. Combining MPLS and VLAN provides an elegant VOLAN solution: Inside each LAN segment, VLAN is used to group traffic per virtual operator (VOLAN). In the whole PamLAN, MPLS is used to set up routing paths and provision each VOLAN. Figure 3 illustrates this architecture for a three-segment LAN with two VOLANs, in which VOLAN 1 has three MPLS paths from access point routers to PamLAN gateway routers, and VOLAN 2 has four MPLS paths.

The use of MPLS makes it possible to limit VOLAN management at the borders of the PamLAN. Only Internet gateways and access points need be aware of the existence of VOLANs. MPLS tunnels are built among them to direct mobile user traffic in a systematic way without routing function changes in the intermediate PamLAN routers. These routers examine only the MPLS label, which carries information regarding a VOLAN path between the source and the destination border router.

At an access point, each mobile user packet is mapped into a forwarding equivalence class (FEC) based on virtual operator membership and the desired QoS class. An MPLS label conveying the FEC information is inserted into the packet and is used by the label switched routers along the MPLS path to determine VLAN assignment as well as 802.1p priority within each

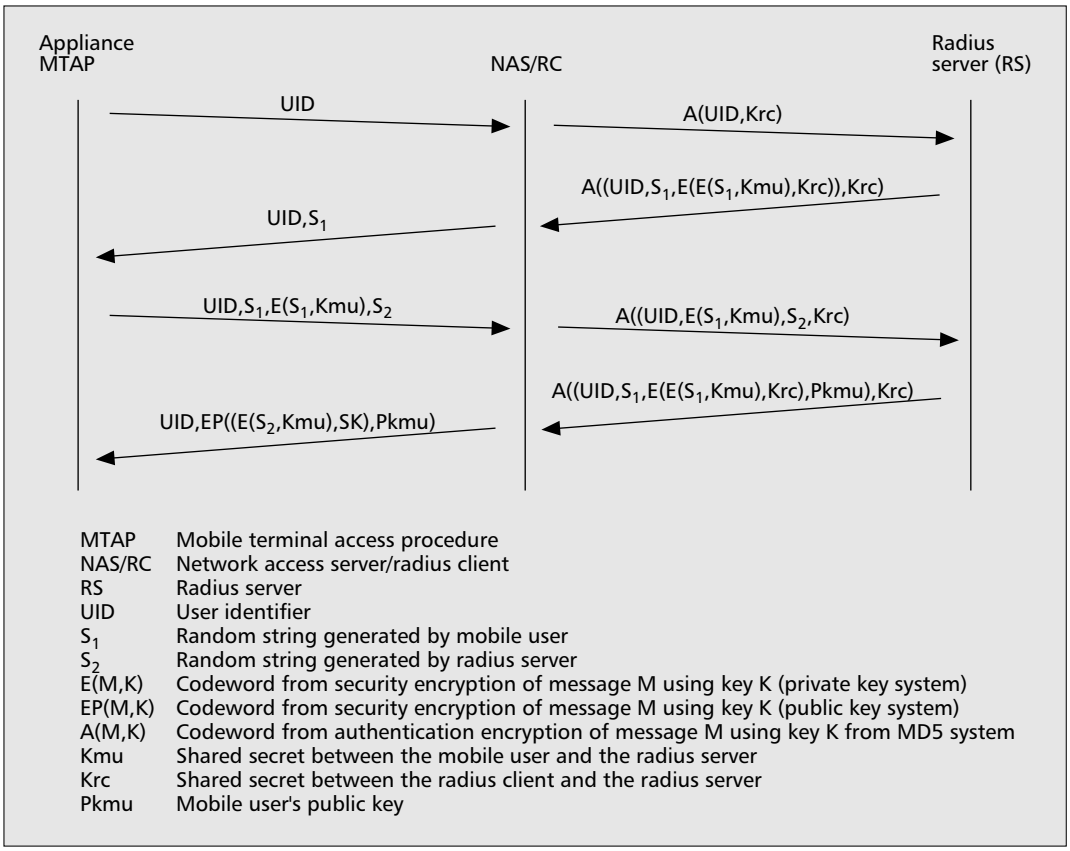


Figure 4. *A message exchange sequence during mutual authentication.*

When a mobile user attempts to access a PamLAN, the access point must make sure that the mobile user is authorized to access the PamLAN and can be properly charged for services rendered. Simultaneously, the mobile user must make sure that the PamLAN is (semi) trustworthy and is certified by his/her service provider.

VLAN. Traffic engineered paths can be set up among access points and Internet gateways according to the service contracts between the PamLAN and different virtual operators.

Virtual Operator AAA

When a mobile user attempts to access a PamLAN, the access point must make sure the mobile user is authorized to access the PamLAN and can be properly charged for services rendered. Simultaneously, the mobile user must make sure that the PamLAN is (semi) trustworthy and is certified by his/her service provider, who has a virtual operator franchise in the PamLAN. Finally, both the user and the PamLAN must make sure that the transmission between them is secure and that no one can fake the user's identity to gain unauthorized access. The PamLAN security framework addresses these concerns in four major components:

¶**Mutual authentication** between the mobile user and the virtual operator through Remote Authentication Dial-In User Service (RADIUS) with the access point serving as the RADIUS client. The access point is also certified by the virtual operator's RADIUS server, so the mobile user and the access point now enjoy a reasonable level of mutual trust.

¶**Public-key-based secure channel establishment** between the user and the access point. Each user has his/her public key in a directory maintained by the virtual operator. After user (and access point) authentication, the virtual operator sends this key to the access point. The access point then generates the session key, encrypts it using the user's public key, and sends it to the user.

¶**Per packet encryption** for authenticated sessions. Once the mobile user obtains the per session key, all user traffic is encrypted at the IP layer using IPSec [9], or at layer 2 using hardware encryption if the layer 2 protocol implementation (e.g., 802.11) at both the appliance and the access point supports per session keys.

¶A **filtering function** at the access point to control traffic from the mobile devices. The access point filters each packet and determines whether it should be let through (user traffic authenticated with the session key), sent to the authentication engine (login session traffic), or blocked (unauthorized traffic). This filtering function is a fundamental building block used for many other purposes such as VLAN assignment and QoS control.

Mutual Authentication Process

The proposed authentication scheme is similar to that in an IEEE 802.11 draft proposal submitted by Cisco, Microsoft, Intel, Symbol, and Informed Technology [10]. The major difference is that we use a pure IP-based solution, while the proposal in [10] makes use of the IEEE 802.1x port-based authentication scheme, which requires minor changes to both IEEE 802.11 and 802.1x standards.

The IP-based authentication architecture works across different radio technologies without the need to change layer 2 protocols, which are usually built into hardware and not easy to mod-

The service provider would be most assured of accurate accounting information if all user traffic were routed through its own location or that of some trusted entity in the Internet, but this is undesirable for efficiency and scalability reasons. Several locally operating mechanisms corresponding to different contractual and subscription agreements may be employed.

ify. It enables access points to interoperate with wireless interface cards from different vendors, which may have their own proprietary AAA schemes. All that is required for interoperability is to install the necessary application-level authentication software on the wireless appliance.

In the proposed framework, a mobile device associates with an access point through open authentication. The access point then assigns the mobile device a dynamic IP address via DHCP and also installs a filter for the assigned IP address. All IP traffic from this address is initially terminated by the access point filter and sent to the authentication engine. After the IP stack is properly set up at the mobile device, the mobile user initiates a login session with his/her service provider (virtual operator) through the access point. If the service provider has a partnership agreement with the PamLAN, the access point, serving as a RADIUS client, can initiate a RADIUS session with the virtual operator's RADIUS server. By employing a challenge/response scheme and using the access point as a relay agent, the mobile user and service provider's RADIUS server authenticate each other through RADIUS protocol message exchange.

Figure 4 illustrates one possible authentication sequence. The result of such mutual authentication is that the mobile user and access point may now trust each other with respect to the service provider agreement. With this assurance, the access point can then request the service provider to send the user's profile, including the user's public key and subscription status. The public key is used to securely inform the mobile user of the session key while all other parameters in the profile are used to enforce the virtual operator's access and QoS policies for the user traffic.

Note that the above sequence can be simplified into only one round trip message exchange, i.e. only the mobile challenges the Radius server. This is possible because all mobile packets will be subsequently authenticated based on the shared key. The Radius server thus need not authenticate the mobile user in the first step. This simplified authentication procedure is apparently faster, but is also subject to easier denial-of-service attacks (i.e., a malicious user may constantly challenge the Radius server). Even with the addition of some user credentials, replay attacks are still possible. These two mechanisms can be used according to the level of security requirement in an actual system.

Authorization Control

After successful authentication and per session key establishment, the mobile user can use the PamLAN to access the public Internet or local resources (e.g., printing services, temporary storage spaces, and caching services). The filtering function at the access point plays an important role in controlling user access and enforcing a rich set of access policies.

The most basic policy is the per-packet authentication/encryption policy that maps an authenticated mobile appliance IP address to the corresponding session key. This key is used to authenticate and/or decrypt the IP packets from the mobile device. Depending on the level of security the mobile user desires, user packets may simply be authenticated using IPSEC authentication header, which authenticates the packet by generating a codeword over the whole packet plus the session key and appending the result to the IPSEC header. Since only an authenticated mobile device shares a session key with the access point and can generate the correct authentication header, per-packet authentication can be performed securely.

This approach is sufficient to deter fake identity attack wherein an unauthorized user fakes someone else's IP address in the hope of gaining PamLAN access. However, it does not protect the security of the packet content. If the user is concerned about data being eavesdropped, the IPSEC encapsulated security payload (ESP) can be used to encrypt the IP payload. Alternatively, the user may use an end-to-end approach such as secure socket.

Other representative policies include giving access only to certain types of subscriptions with authorized service providers, giving free access together with advertisements, excluding access to particular Web sites as in parental control, and imposing a service provider's QoS limitations such as a limit on access rate.

Accounting

With the help of the traffic filtering function, per-user accounting information can be collected by the access points and sent to the RADIUS server of the virtual operator (service provider). Accounting information may be as simple as the duration of a session, or may contain a detailed list of requested services, visited sites, total duration, and QoS provided. The service provider would be most assured of accurate accounting information if all user traffic were routed through its own location or that of some trusted entity in the Internet, but this is undesirable for efficiency and scalability reasons. Several locally operating mechanisms corresponding to different contractual and subscription agreements may be employed.

Flat-fee-based: A PamLAN operator charges each virtual operator a flat fee to provide unlimited access to the mobile users belonging to the virtual operator, which in turn charges each mobile user a flat monthly fee. Accounting can be done loosely in this case, e.g. only the access points keep track of the user traffic profile and report to the virtual operator periodically.

Per session: The virtual operator is satisfied with proof of user login and signoff. It is simple and puts very little burden on the various parties, but does not take idle periods into account.

Usage-based: The user is only charged for the actual traffic his/her mobile appliance generates on a PamLAN. To avoid possible dispute, the virtual operator must have digitally signed (authenticated) evidence that the user and the access point measured the same traffic usage.

Mobility Management

Mobility management becomes a significant issue in large PamLANs with multiple subnetworks. Because PamLAN works as a layer 3

infrastructure, mobility requirements — dynamic path routing and fast AAA handoff in particular — must be supported at the IP layer.

Micromobility with Dynamic Path Routing

Micromobility refers to roaming within a PamLAN environment. It should not be necessary to follow the full mobile IP procedure of rerouting through the Internet to the user's home location when only a local movement is made. Cellular IP and an MPLS-based solution are viable candidates.

Cellular IP was designed for micromobility support in a LAN environment with multiple router-based access points and a single Internet gateway. When a mobile appliance moves and changes its associated access point, a routing update message is sent from the mobile appliance through the new access point toward the Internet gateway. Each router along the way, like the access point and the gateway, updates its routing table to reflect this change. These routing entries are refreshed periodically, so if there is a pause in regular packet transmission, the mobile device must periodically send location update packets (paging packets) to prevent the routing table entries from expiring. The whole process is a significant burden when a large number of mobile devices are being serviced by a PamLAN.

A preferable micromobility solution for a PamLAN relies on MPLS label switched paths (LSPs) between Internet gateways and access points to handle mobile traffic. Access points and Internet gateways serve as ingress or egress routers, depending on the direction of the mobile traffic. If LSPs are statically provisioned between access points and Internet gateways, there is no need to update any intermediate routers when mobile devices move. Only the old access point, the new access point, and the Internet gateway need be informed of the change to redirect mobile traffic through a different LSP. Apart from efficient micromobility support, this solution also, as described earlier, provides a way to provision virtual operator LANs.

Fast AAA Handoff

In a PamLAN environment, it is undesirable to make a mobile user repeat the authentication process each time he/she associates with a new access point, due to both inconvenience and traffic interruption. It is thus necessary that the AAA control state be smoothly transferred from the old access point to the new one. A fast and smooth handoff is possible provided the old access point trusts the new one, which is normal in a PamLAN. To ensure a fast handoff, the following actions must be taken:

- The new access point fetches the user profile from the old access point. Among other things, this profile contains the user's public key, the old session key he/she shares with the old access point, the mobile device's IP address, and all the access policies associated with the old session.
- The old access point signals to the RADIUS server the termination of the current accounting session.
- The new access point generates a new session key, encrypts this key and the user's old session key using the user's public key and sends the result to the user in a UDP packet. Upon receiving the packet, the user decrypts these keys and compares the old session key with the one he/she has. If the two match, the user uses the new session key to establish a secure connection with the access point.
- The filtering functions together with the access policies in the user profile are installed by the new access point, which initiates a new accounting session with the RADIUS server.

Initial Experimental Implementation

A laboratory implementation used a commercial 12-port Ether switch (including VLAN capabilities) and three personal computers, each running the Linux operating system, including software router functions. Two of the personal computers served as access points with 802.11b wireless LAN interfaces, and the third functioned as the gateway to the outside network.

This testing platform was used to:

- Verify VLAN and Diffserv support of an Ether switch
- Integrate the cellular IP protocol implementation into a regular LAN environment
- Prepare for implementation of basic AAA functions

VLAN was realized through the configuration of VLAN-specific network interfaces in the Ether switch. Since in general more than one VLANs are active at an access point (and hence at an Ether switch port), multiple network interfaces were configured, each with its own VLAN-specific IP address. With the VLAN ID (12-bit tag) appearing in the Ethernet header, the switch was able to distinguish VLAN-specific traffic according to the tag. Two service classes were supported: strict priority and best effort. Testing under heavy network load remains to be done.

Cellular IP was ported to the Linux platform from the FreeBSD implementation developed at Columbia University. The protocol was originally designed for an ad hoc wireless network consisting of router-equipped nodes. The principle of cellular IP was adapted for the wired PamLAN IP network in which, unlike the situation in a wireless ad hoc network, handoff delay is mainly due to air interface reassociation. The routing path update from the new access point to the gateway is relatively negligible.

The IP-based AAA functions are being implemented on a mobile laptop computer, the Linux-based access points, and an experimental RADIUS server. A client access module on the mobile device, adapted from open-source software, is responsible for the user interface for the login process and for cooperating with the access point for the authentication process. On each access point, IP-address-based access control is achieved through the IP filtering function built into the Linux kernel. A RADIUS client adapted from the Livingston open source implementation (http://www.Livingston.com/forms/one-click-dload.cgi) is also installed to support authentication with the RADIUS server. IPSec is enabled in the system kernels on both the access points and mobile terminals. The RADIUS server is extended from the open

Micro mobility refers to roaming within a PamLAN environment. It should not be necessary to follow the full mobile IP procedure of rerouting through the Internet to the user's home location when only a local movement is made. Cellular IP and an MPLS-based solution are viable candidates.

The business model and distributed IP structure constitute a secure, economical and extensible architecture that will accommodate multiple services providers, multiple air interfaces, and a variety of services appropriate for coming generations of Internet appliances.

source implementation to support mutual authentication with mobile users.

Further experimentation would build VOLANs using MPLS paths between access points and the gateway, and test alternative IP micromobility protocols and QoS admission control.

CONCLUSIONS

The architecture described in this article can provide wireless access services, in large public spaces, to subscribers of ISP, cellular mobile, and other service providers. Although many details remain to be specified, the implementations are straightforward, and precursors already exist in rudimentary form in available programmable access point products. The business model and distributed IP structure constitute a secure, economical, and extensible architecture that will accommodate multiple service providers, multiple air interfaces, and a variety of services appropriate for coming generations of Internet appliances.

REFERENCES

[1] C. Perkins, "Mobile IP Joins Forces with AAA," *IEEE Per. Commun.*, Aug. 2000.

[2] C. Andersson, *GPRS and 3G Wireless Applications: Professional Developer's Guide*, Wiley, May, 2001.

[3] IEEE 802 std., "Information Technology — Telecommunication and Information Exchange between Systems — Local and Metropolitan Area Networks — Specific Requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications."

[4] Bluetooth Special Interest Group, "The Bluetooth Specification," http://www.bluetooth.com/developer/specification/core_10_b.pdf

[5] Cisco Systems, "Virtual LAN Communications," http://www.cisco.com/warp/public/cc/pd/wr2k/cpbn/tech/vlan_wp.pdf

[6] A. G. Valko, "Cellular IP: A New Approach to Internet Host Mobility," *ACM Comp. Commun. Rev.*, Jan. 1999.

[7] R. Ramjee *et al.*, "HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless Networks," *ICNP '99*.

[8] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," Internet RFC 3031, http://www.ietf.org/rfc/rfc3031.txt

[9] IP Security Protocol Charter, "IP Security Protocol," http://www.ietf.org/html.charters/ipsec-charter.html

[10] D. Halasz *et al.*, "A Joint Proposal for 802.11 Security," IEEE draft 802.11-00/382.

BIOGRAPHIES

JUN LI received his B.S. and M.S. degrees from Xidian University and Ph.D. degree from WINLAB, Rutgers University, respectively, all in electrical engineering. Since January 1986 he has worked for various R&D labs and industrial companies in China, Japan, and the United States. He is now with Corporate Research of Thomson Multimedia Inc., Princeton, New Jersey, working on wireless communication systems for high-value high-quality digital content delivery.

STEPHEN B. WEINSTEIN [F] served as President (1996–97) of the IEEE Communications Society. He received his B.S., M.S., and Ph.D. degrees in electrical engineering from MIT, the University of Michigan, and the University of California at Berkeley, respectively. He invented the echo cancellation technique used in telephone channel modems and was a pioneer in OFDM/DMT modulation. He is the author of several technical books on communication technologies and data networking. He is currently editor in chief of *Journal of Communications and Networks* (JCN).

JUNBIAO ZHANG (junzhang@ccrl.nj.nec.com) is currently with the Computer and Communications Laboratories of NEC USA as a research staff member. He obtained his Ph.D and M.S. degrees, both in computer science, from Rutgers University and his B.S. degree in computer science from the University of Science and Technology of China. His major research interests include 3G wireless/WLAN interworking, wireless security, mobile applications, and optical network control.

NAN TU is a research associate in the Computer and Communication Research Laboratories of NEC USA. He received his B.S. in computer science and mechanical engineering from Tsinghua University, China in 1996, and his M.S. in computer science from Rutgers University in 2001. His current research interests are high-speed networks, optical networks, and mobile networks.