

Interworking Architecture Between 3GPP and WLAN Systems

Kalle Ahmavaara, Henry Haverinen, and Roman Pichna, Nokia Corporation, Finland

ABSTRACT

The Third Generation Partnership Project has recently taken the initiative to develop a cellular-WLAN interworking architecture as an add-on to the 3GPP cellular system specifications. This article presents an overall view on an interworking architecture, which enables provisioning of public WLAN access service for the 3GPP system subscribers by mobile operators. The enabling functionalities include the reuse of 3GPP subscription, network selection, 3GPP system-based authentication, authorization and security key agreement using SIM/USIM card, user data routing and service access, as well as end user charging. The interworking functionalities are achieved without setting any 3GPP specific requirements for the actual WLAN access systems, but relying on the existing functionality available in a typical WLAN access network based on IEEE 802.11 standards.

INTRODUCTION

Mass market public wireless access has typically been provided by cellular systems owned by cellular operators. Currently, WLAN-based systems are emerging as a new means of public wireless access; therefore, interworking and integration solutions between the existing public wireless access systems, cellular networks, and the new potential access systems, WLANs, are being developed.

The Third Generation Partnership Project (3GPP) is a joint initiative of European, U.S., Japanese, and Korean telecommunications standardization organizations to produce global specifications for the Universal Mobile Telecommunication System (UMTS). 3GPP was initially formed to specify a common set of 3G cellular system specifications on behalf of these regional standardization bodies.

3GPP has recently also taken the initiative to develop a cellular-WLAN interworking architecture [1] as an add-on to the existing 3GPP cellular system specifications to be published with 3GPP Release 6 specifications. The main driver

is to enable 3GPP system operators to provide public WLAN access as an integral component of their total service offering to their cellular subscribers. 3GPP aims to create a complete set of specifications for interworking to facilitate the emergence of a competitive open multivendor business environment for driving public WLAN access toward a mass market business.

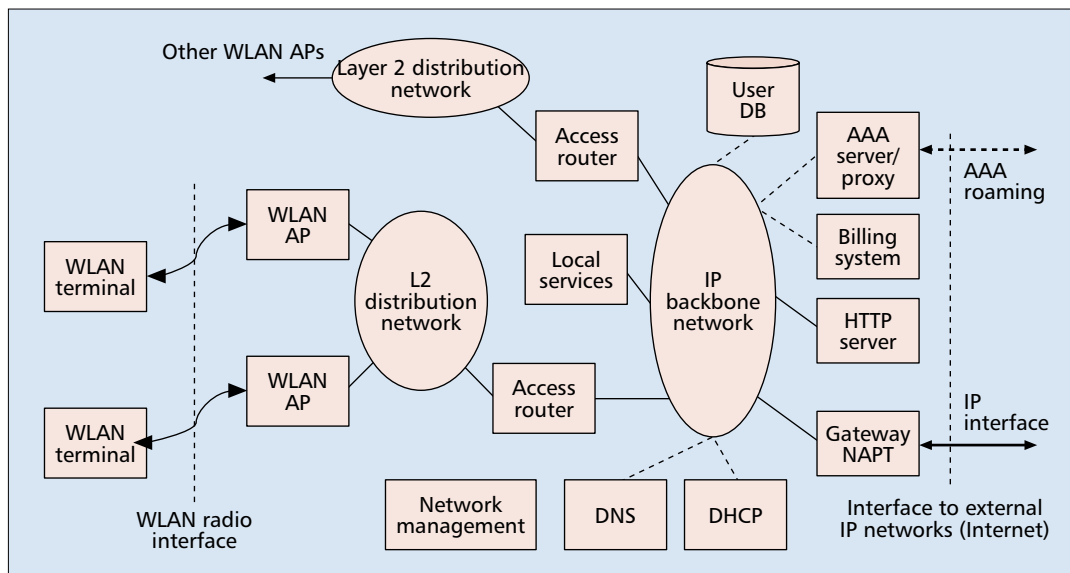
Definition of the interworking architecture in the 3GPP is currently ongoing, and the first version of the specifications is targeted to be finalized by the end of 2003. At the time of writing this article, major portions of the architecture work have already been done, but issues still remain unresolved. This article presents the authors' view of the 3GPP-WLAN interworking architecture likely to be standardized in 3GPP early in 2004, focusing on the portions that have already been agreed on. All the authors are active contributors and participants in 3GPP on WLAN interworking standardization.

The 3GPP standardization work is partly based on earlier mobile operator WLAN architecture development, in which the authors were also involved. One of the authors participated in the design of a pre-standard system, described in [2], before the 3GPP work was started. The pre-standard system resembles the 3GPP system in many respects.

This article presents the assumed de facto WLAN system architecture. We outline the usage of 3GPP subscription for WLAN access. We introduce the functionalities to realize 3GPP-based access control, such as network selection, and 3GPP system-based authentication and authorization. We present the user plane routing for accessing services and describe the effects online and offline charging have on the interworking architecture.

ASSUMED DE FACTO WLAN SYSTEM ARCHITECTURE

3GPP WLAN interworking architecture design work is focused on the interworking functionality between 3GPP and WLAN systems. To achieve



■ **Figure 1.** *A de facto WLAN system.*

In practice there are as many WLAN system architectures as there are available systems. Fortunately the basic functionalities are similar in all WLAN systems as they are based on the de facto standardization paradigm of the ISP industry.

a 3GPP-WLAN interworking architecture that can be widely adopted, it is imperative that the existing de facto WLAN access equipment can be used as such for 3GPP interworking. Requiring introduction of 3GPP-specific WLAN access equipment would slow down, if not disable, real deployment of 3GPP-WLAN interworking systems. Therefore, a fundamental assumption in 3GPP is that it is out of the 3GPP scope to standardize the WLAN access network architecture or the WLAN radio interface; thus, the WLAN access network box in the 3GPP-WLAN interworking specifications appears undefined. However, in order to develop the interworking architecture, it is important to understand how the assumed typical WLAN systems work.

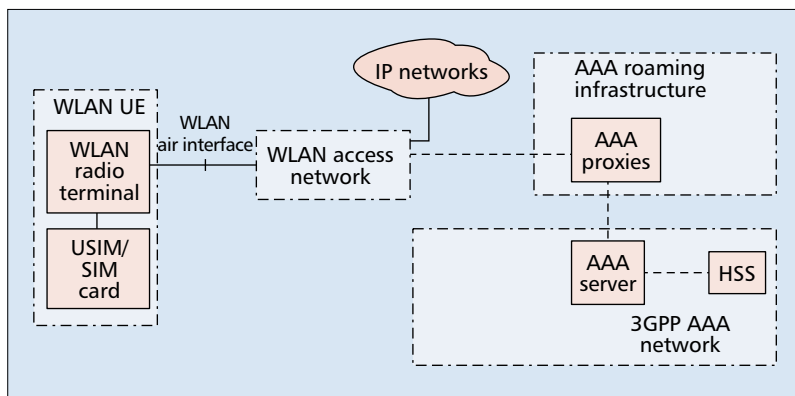
Unlike the 3GPP system architecture, there is no existing formal standard for a WLAN access network architecture nor for a typical public access WLAN system. In practice, there are as many WLAN system architectures as there are available systems. Fortunately, the basic functionalities are similar in all WLAN systems as they are based on the de facto standardization paradigm of the Internet service provider (ISP) industry.

The WLAN system shown in Fig. 1 enables IP connectivity between the WLAN terminal and IP networks over its WLAN interface. The core of the WLAN system is the IP backbone. Attached to it are servers offering services ranging from those that enable basic IP connectivity up to possibly application-level services. A Dynamic Host Configuration Protocol (DHCP) server is needed to facilitate configuration of the WLAN terminal's IP stack. A DNS server resolves Internet fully qualified domain name (FQDN) addresses into IP addresses. GW/NAPT is a gateway toward external IP networks such as the Internet. The GW usually also performs IP network address and port translation (NAPT) to enable the WLAN access network operator to use private-space IP addresses inside the WLAN system and enable access to services available in outside IP networks at the same time. A HTTP server may offer local application-level service

for accessing users. Its functionality can also be used to push landing Web pages to the WLAN terminals to enable username/password access control with standard Web browsers in terminals. Accounting data has to be processed to issue bills. This is done in the billing system server. The local services server is a general box covering services at IP level or above, such as mail servers and local Web content. Network management takes care of the management of all network elements at all layers. It is instrumental in network configuration and monitoring.

The WLAN terminal is typically a laptop computer or a PDA with a built-in WLAN module or a PCMCIA WLAN card. As for the WLAN standards used today, the 11 Mb/s WLAN IEEE802.11b [3] working in the 2.4 GHz industrial, scientific, and medical (ISM) band is the de facto standard. There are newer WLAN standards offering higher data rates up to 54 Mb/s that will very likely complement and possibly even replace IEEE802.11b, such as 5 GHz IEEE802.11a [4] or its 2.4 GHz version, IEEE802.11g [5]. From the WLAN system point of view, the consequences of these upgrades are limited mostly to the radio interface as higher layers remain untouched.

The WLAN access point (AP) is mostly just a layer 2 bridge between IEEE802.11 and Ethernet. The AP can also support IEEE802.11i [6]/802.1x [7] functionality, in which case it is also a RADIUS [8] client toward the fixed network and performs radio link encryption toward the WLAN terminal. APs are attached to the layer 2 distribution network such as a switched Ethernet subnet. An Ethernet subnet can be augmented with IEEE802.1Q [9] tag switching to support virtual LAN (VLAN). In some special cases, the L2 distribution network may also provide intra-subnet mobility for WLAN terminals. The layer 2 distribution network enables layer 2 connectivity toward the first IP routing device, the access router (AR). The functionality of the AR can be very rich, but its basic function is to route user IP packets.



■ **Figure 2.** *WLAN system architecture reusing the 3GPP subscription.*

Authentication and authorization is one basic prerequisite for providing IP connectivity and other services via a WLAN system. To realize these functions an authentication, authorization, and accounting (AAA) server and a user database are required.

An AAA server is typically a RADIUS server used for authentication, authorization, and accounting for subscribers of a WLAN system. The subscribers' user identities such as login names, shared secrets like passwords, and user profiles can be stored in the user database. The database is accessed from the AAA server over the IP backbone network using the Lightweight Directory Access Protocol (LDAP) as the de facto standard.

Legacy authentication and authorization is done using Web browsers. When the user starts his/her Web browser, its first request is redirected into a WLAN system HTTP server and a landing Web page is displayed. The user is prompted to enter login name and password. The password can be static, limited time, or even generated ad hoc (using, e.g., SecureID technology). Similarly, users can be prompted to input their credit card number and pay for the connection without establishing a more lasting relationship with the WLAN system operator. With the advent of IEEE802.1x and IEEE802.11i standards, authentication is moving to a higher, more user-friendly, more secure level that will also be utilized for 3GPP-WLAN interworking, as described later in this article.

It is also possible to establish roaming relationships between WLAN systems. Roaming enables a user of a WLAN system to connect to another WLAN system. In this case, the AAA functions are still provided by the user's own WLAN system, while actual WLAN access is provided by the other WLAN system.

USAGE OF 3GPP SUBSCRIPTION FOR WLAN

3GPP system operators have a large established customer base. 3GPP system operators have elaborate customer care, charging, and billing systems, and a proven, robust, and scalable system for distributing and maintaining security modules and UICC smart cards containing Subscriber Identity Module (SIM)/Universal SIM

(USIM) applications. Most cellular operators already provide IP access and services over their packet-switched core network (PS CN) domain and wide-area cellular radio access networks. They use SIM/USIM for security control and maintain a user database, including security components and service profiles, in their home subscriber servers (HSS). HSSs together with the already distributed SIM/USIM smart cards and established global roaming agreements between 3GPP system operators form the largest operational security system in the world to date. On top of this, it is in the interest of cellular operators not to compromise their current security level by adding a new interworking domain. Given this requirement, the customer base, proven security track record, and developed tools for maintaining the system, it seems obvious that there are significant benefits in reusing the subscription system for interworking WLAN access.

To reuse 3GPP subscription, 3GPP interworking WLAN terminals will need access to UICC smart cards with SIM/USIM applications. A WLAN terminal equipped with a SIM/USIM smart card is called WLAN user equipment (WLAN UE) according to established 3GPP terminology. Given the need for dual-mode (WLAN-cellular) UEs, SIM/USIM will be available in those UEs anyway.

An outline of the architecture of interworking WLAN access reusing 3GPP USIM/SIM and HSS is shown in Fig. 2. From an AAA signaling point of view 3GPP-WLAN interworking is always a roaming case, where the subscription-related infrastructure is provided by the 3GPP system, and the accessed WLAN system provides actual WLAN access for the roaming user.

3GPP-BASED WLAN ACCESS AUTHENTICATION AND AUTHORIZATION

NETWORK SELECTION

GSM and UMTS specifications include provisions for selecting the visited network when the user is roaming outside the coverage area of the home operator network. The UE discovers the available networks, or more specifically the public land mobile network identifiers (PLMN IDs) of the networks based on broadcast transmissions from local networks. In manual network selection the user selects the network from a list of available networks. In automatic selection the UE selects the network on behalf of the user, optionally making use of a list of preferred PLMN IDs stored in the SIM/USIM.

Network selection becomes a more complicated issue in 3GPP-WLAN interworking. Although a mobile operator may provide a WLAN access network, the access network may also be operated by an organization other than a mobile operator, such as a premises owner or a wireless ISP. The WLAN operator may have agreements with one or more local GSM or UMTS operators, which in turn may have roaming agreements with the user's home operator. It is also possible to have direct agreements

between wireless ISPs and the home operator. Hence, in addition to the choice of radio network there may be several viable roaming routes to the home from a given WLAN access network.

At the time of writing, 3GPP has agreed to support visited network selection for WLAN interworking so that users will be able to select the visited PLMN (VPLMN) when several roaming routes are available. The technical solution is expected to be based on the Network Access Identifier (NAI), which is the username format used on WLANs. The NAI consists of a username portion, followed by the @ character and a realm portion, similar to email addresses. After associating with the WLAN access point, the UE indicates its home network in its NAI realm portion. If the WLAN access network cannot route the request to the home network, the UE is provided with a list of supported VPLMNs in that particular WLAN access network. UE selects the preferred VPLMN, reformats its NAI to contain also the VPLMN ID, and starts authentication again with its “new” ID. The WLAN access network then has the information on how to route the request.

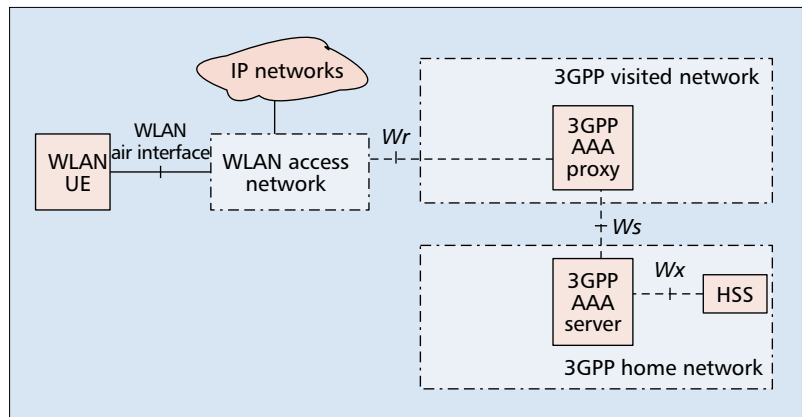
AUTHENTICATION AND KEY AGREEMENT IN IEEE 802.11

New WLAN standards are being developed to improve the level of security in the WLAN air interface. For IEEE 802.11, the extensions for enhanced security will be called IEEE 802.11i [6]. The standard will specify a scalable authentication, access control, and key agreement framework based on the IEEE 802.1x standard. Authentication and key agreement functions can be implemented with a centralized authentication server using RADIUS and the Extensible Authentication Protocol (EAP) [10]. The security keys distributed using EAP and RADIUS are used for new packet security methods that replace the infamous Wired Equivalency Privacy (WEP) algorithm.

RADIUS is an authentication, authorization, and accounting (AAA) protocol that is widely used in Internet access networks. For user authentication, RADIUS can function as an EAP transport. In the WLAN case, the access point operates as a RADIUS client, and the AAA server contains a RADIUS server implementation. RADIUS traffic may also traverse via a multitude of RADIUS proxy servers, for example, to implement roaming broker functions.

RADIUS has several limitations in the areas of security, robustness, roaming support, and server-initiated operations. DIAMETER, the successor AAA protocol to RADIUS, is currently being specified in the IETF to overcome these limitations. As DIAMETER will implement all the functionality specified in RADIUS plus more, DIAMETER can alternatively be used for AAA purposes in IEEE 802.11i once the DIAMETER standard is finalized.

EAP itself does not specify the actual authentication and key agreement protocol, but it provides a “wrapper” or framework for any multi-round-trip authentication protocol to be



■ Figure 3. 3GPP-WLAN interworking authentication and roaming architecture.

transported. A separate EAP method specification for each authentication method is required. Because EAP is an end-to-end protocol, the access point or other intermediate elements do not need to know the details of each authentication and key agreement protocol; it is sufficient that the AAA server and UE implement the same EAP method.

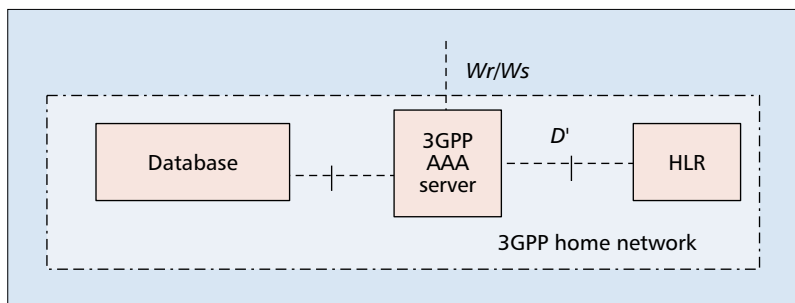
AUTHENTICATION AND AUTHORIZATION IN 3GPP-WLAN INTERWORKING

Mobile networks of the GSM family make use of smart cards to implement subscriber authentication for network access control. Smart cards are also used to agree on security keys for encryption and integrity protection over the wireless link. In GSM and GPRS, the SIM card includes a challenge/response algorithm for authentication and key agreement. In UMTS networks, an enhanced version of these techniques is used, and the authentication and key agreement functions require a new type of smart card containing the USIM application.

As the basic approach in specifying 3GPP-WLAN interworking is to pose as few new requirements on the WLAN access network as possible, the interworking standard refers to IEEE 802.11i to implement the authentication, access control, and key agreement functions. In order to be able to reuse the USIM/SIM-based authentication algorithms, two new EAP methods, EAP SIM and EAP AKA, have been specified for 3GPP-WLAN interworking.

EAP SIM [11] specifies an authentication and key agreement protocol based on the GSM SIM algorithms. Although it is based on the GSM authentication protocol, it includes several important enhancements to extend the GSM mechanisms with mutual authentication and longer session key derivation. EAP SIM also includes mechanisms for identity hiding using temporary identifiers, or pseudonyms, and a fast reauthentication procedure.

EAP AKA [12] encapsulates the UMTS Authentication and Key Agreement (AKA) within EAP. Because UMTS AKA natively supports mutual authentication and strong key derivation, EAP AKA is a more or less faithful encapsulation of the UMTS mechanisms into



■ **Figure 4.** 3GPP home network architecture when a legacy HLR is reused.

EAP. EAP AKA includes the same identity hiding and fast reauthentication functions as EAP SIM.

Figure 3 illustrates the 3GPP-WLAN interworking system elements and reference points involved in authentication and roaming. The WLAN access network is connected to the 3GPP AAA proxy via the Wr reference point. The 3GPP AAA proxy forwards authentication signaling between the WLAN access network and the 3GPP AAA server. Where no visited PLMN IDs are involved, the Wr reference point connects the WLAN access network directly to the 3GPP AAA server. The Wr reference point is used for authentication and key agreement signaling, and the protocols in this reference point will essentially be EAP over DIAMETER or RADIUS. In the roaming case, the reference point between the 3GPP AAA proxy and 3GPP AAA server is Ws .

The 3GPP AAA server includes the EAP server functionality. It implements the network side peer for EAP SIM and EAP AKA. The 3GPP AAA server also verifies if the subscriber is authorized to use WLAN. The authorization information and authentication vectors needed in the authentication protocols are stored (or generated) by the HSS. The 3GPP AAA server retrieves this information from the HSS exchange over the Wx reference point, which is basically a reference point for database access.

REUSING 3GPP LEGACY HOME LOCATION REGISTERS

Prestandard 3GPP-WLAN systems are expected to be deployed before the 3GPP specifications are fully completed, and thus before 3GPP-WLAN interworking-compatible HSS implementations are available. Since the authentication protocols used in WLAN interworking are reused from GSM and UMTS standards, the existing home location registers (HLR) can be used for generating authentication vectors in the absence of a new 3GPP-WLAN interworking-compatible HSS. Figure 4 illustrates the home network authentication architecture when a legacy HLR is used instead of a 3GPP-WLAN interworking-compatible HSS. The D' reference point between the 3GPP AAA server and the HLR represents a subset of the operations used in the D reference point locating between a visitor location register (VLR) and the HLR in the existing 3GPP CN specifications. In this case the 3GPP AAA server uses the same Mobile Appli-

cation Part (MAP) messages to retrieve authentication vectors from the HLR as a VLR uses, according to those CN specifications.

The D reference point also includes authorization operations. A VLR can retrieve a subscription profile for circuit-switched services to detect which circuit-switched services the subscriber is authorized to use. Some of the existing bits are currently unused, so it may be possible to redefine the meaning of the unused part of the subscription profile to indicate the existence of a WLAN subscription. In practice, the redefinition needs to be operator-specific. Alternatively, to the subscription profiles stored in the HLR, the 3GPP AAA server can use a separate database for storing WLAN subscription information.

USER DATA ROUTING AND ACCESS TO SERVICES

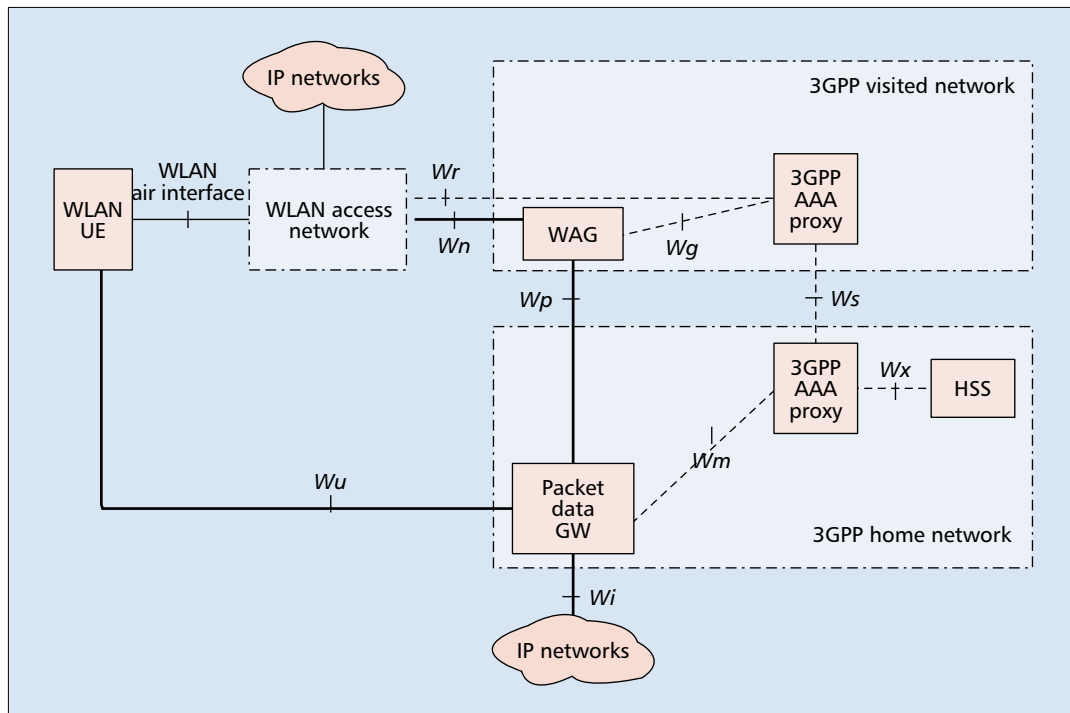
Once the user has been successfully authenticated and authorized for network access, the WLAN access network grants the UE access to an IP network. In the simplest case, the IP network is the public Internet, and the user data is directly routed from the WLAN access network to the Internet. Optionally, an aggregate site-to-site tunnel can be set up between a WLAN access network and a 3GPP network to divert the complete user plane through the operator network. The home or visited operator may also want to provide services that are accessible only in a private IP network, not over the public Internet. Examples of such services include the Multimedia Messaging Service (MMS), Wireless Application Protocol (WAP), and 3GPP IP Multimedia Subsystem (IMS). The home operator may also wish that all user data were routed via the home network to collect independent charging information and apply any operator policies.

The technical architecture regarding user data routing has not been agreed on in 3GPP at the time of writing. However, the requirements to remotely connect to private IP networks and to route traffic via a certain point in the network imply the need to tunnel data packets. In tunneling, a tunnel endpoint encapsulates a data packet within a new packet destined to the other endpoint of the tunnel. The other endpoint then decapsulates the packet and delivers the inner packet to the indicated original destination.

The IP network selection is based on a parameter called a WLAN access point name (W-APN), which is similar to the APN parameter used in GPRS. The UE indicates the desired IP network with a W-APN. The network authorizes the request, or verifies that the user has the right to use the W-APN, and the network may also influence the eventual choice of IP network in a user-specific manner. After the IP network has been selected using the W-APN, appropriate tunnels are established to route the user data to the selected IP network.

Even though the details of the technical solution are still open, it has been agreed that the tunnel will be terminated in the home operator network by a network element called the packet data gateway (PDG). The PDG terminates the tunnel and acts as a gateway to the selected

The 3GPP-WLAN interworking system is intended for provisioning chargeable public WLAN services for mobile operator subscribers. For the 3GPP system subscriber, two different charging methods are in general possible; post-paid and prepaid.



■ Figure 5. User data routing according to one of the current alternatives.

remote IP network, so it can be considered analogous to the gateway GPRS support node (GGSN) used in GPRS packet networks. The W_i reference point that resides between the PDG and the remote network is similar to the G_i reference point used between the GGSN and remote IP networks in GPRS. These reference points are simply the connection points between the 3GPP IP connectivity system and external IP networks. Depending on the architectural decisions, a network element in the visited network, the WLAN access gateway (WAG), may also be required to implement tunneling. The WAG and PDG, and the associated reference points used in user data routing according to one of the present alternatives are illustrated in Fig. 5. The reference points W_n , W_p , W_u , and W_i are used to convey the user data plane, and the W_g and W_m reference points are used for control.

3GPP-BASED CHARGING FOR WLAN

PRINCIPLES

The 3GPP-WLAN interworking system is intended for provisioning chargeable public WLAN services for mobile operator subscribers. For the 3GPP system subscriber, two different charging methods are generally possible: postpaid and prepaid. These two mechanisms shall also be available for a 3GPP system subscriber using a 3GPP-WLAN interworking system.

As described earlier, the 3GPP-WLAN interworking system can be used to directly access the Internet from the WLAN access network or to access the specific services provided by the home network via the PDG. Charging for both use cases needs to be supported by the 3GPP-WLAN interworking system. From the sub-

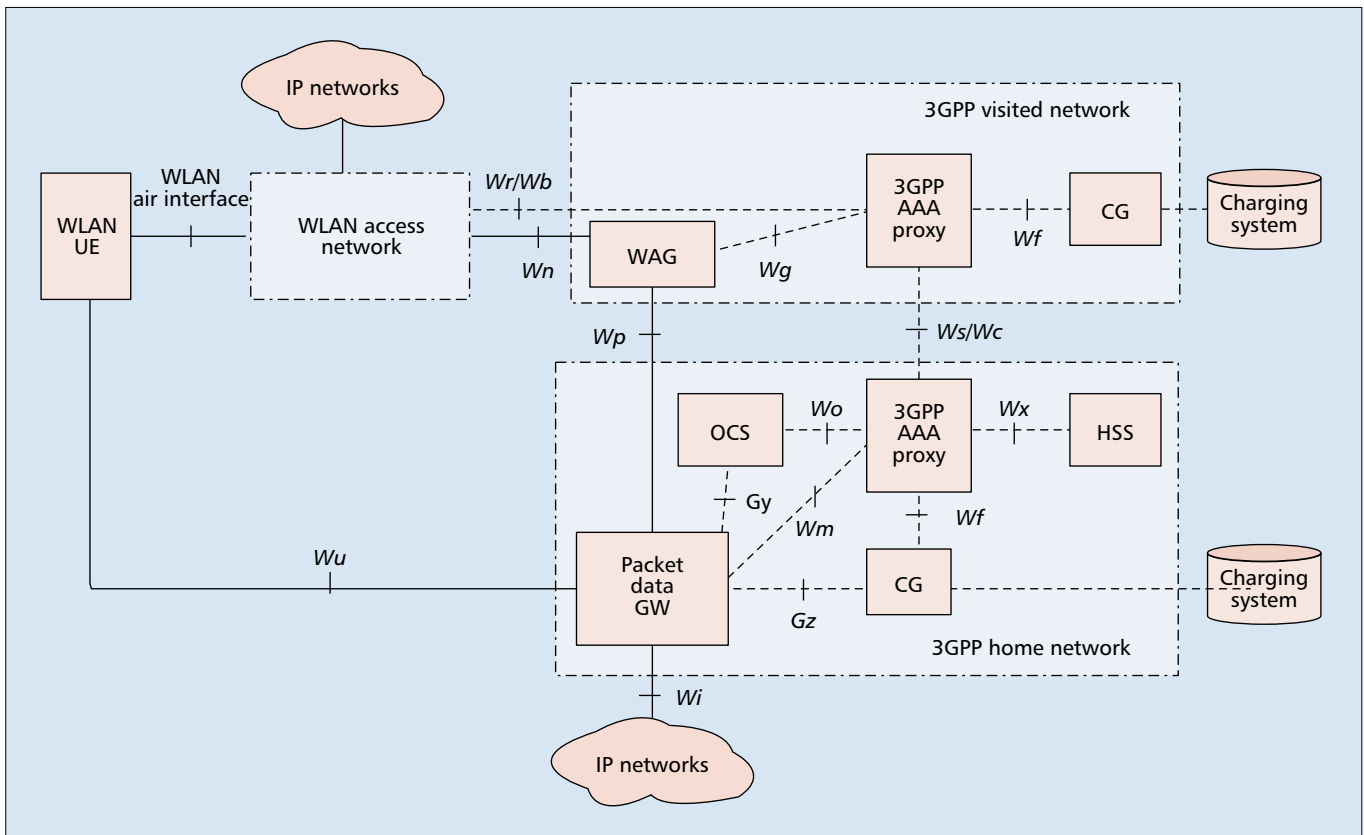
scriber point of view it is important that they clearly understand what they are charged for and how much. For example, if a user is using a service (e.g., sends one multimedia message), he/she should be charged a known service-specific fee for that service independent of the utilized access technology or the number of retransmissions that occurred within the access system when transporting the corresponding data.

When accessing the Internet directly from the WLAN access network, the consumed resource from the 3GPP-WLAN interworking system is the WLAN access itself. That Internet access via WLAN can in this case be considered the service for which the user should be charged. If, alternatively, user data flow through WAG, it is possible to collect aggregate charging information for clearing purposes between 3GPP and WLAN operators.

POSTPAID AND PREPAID CHARGING

In postpaid charging a user has a service and billing contract with the operator, and the operator collects charging information of the postpaid subscriber's system usage. At certain intervals (e.g., monthly) the operator bills the user for the usage according to the collected charging information. The charging information collection happens via so-called charging gateways (CGs). Each operator collects information about all chargeable events in their network to their own CG. Typically, a CG consolidates this information and passes it further to the operator's billing system for further processing.

In prepaid charging the user gets a cellular subscription associated with a certain amount of credit the user needs to purchase from the operator prior to being able to access the system. In addition to buying the credit, there is no need for a specific contract with the operator, unless



■ **Figure 6.** Charging infrastructure and reference points in the 3GPP-WLAN interworking architecture.

required by national regulations. When the user uses the services, the operator online checks the resulting charging information and deducts a corresponding amount from the available credit of the user. When the credit runs out, the user is prevented from utilizing the system. In a 3GPP-WLAN interworking system this type of prepaid credit control is handled by the online charging system (OCS), which, according to other 3GPP specifications, is also responsible for prepaid charging of IMS related chargeable events. This OCS is aware of the credit accounts of individual subscribers and deducts credit from their accounts based on dynamic credit reservation signaling from the 3GPP system network nodes responsible for accumulating charging information.

CHARGING FOR WLAN ACCESS

The WLAN charging architecture is shown in Fig. 6. Consumption of the WLAN access resource occurs in the WLAN access network. Charging information about WLAN access therefore needs to be collected at the WLAN access network and forwarded to the 3GPP visited and home networks.

As described earlier, the home network 3GPP AAA server authorizes each user's access to a WLAN. Before authorizing a prepaid user to access the WLAN for direct Internet access, the 3GPP AAA server has to make a credit reservation from the user's prepaid account in the OCS over the W_o reference point. The 3GPP AAA server asks for credit for a certain amount of WLAN access resource consumption. If credit is available, the OCS acknowledges this request

and deducts the corresponding amount of credit from the user's account.

After authorization to access the WLAN access network is completed, a user-specific accounting session is established between the WLAN access network and the 3GPP home network. This accounting session is established with standard AAA accounting signaling, and the reference point for this signaling is W_b . At the establishment of the accounting session the 3GPP AAA server indicates to the WLAN a suitable set of accounting criteria, such as the accounting unit (e.g., amount of transferred kilobits) and reporting threshold to be utilized. After accounting session establishment the WLAN collects accounting information and reports it to the 3GPP AAA server over the W_b reference point as instructed.

The 3GPP AAA server collects and consolidates accounting information and forwards it as WLAN access call detail records (WLAN CDRs) toward the CG over the W_f reference point. In the billing system this information is then used for clearing the charges between the home network operator, visited network operator, and WLAN access network provider as well as for creation of bills for postpaid users.

For prepaid users the 3GPP AAA server monitors the received accounting information from the WLAN access network. When the downloaded credit is to be exhausted a new credit request from OCS is triggered, to cover the forthcoming accounting reports from the WLAN access network. At the termination of the WLAN connection the 3GPP AAA server returns any unused credit back to the OCS.

HOME NETWORK IP-FLOW-BASED CHARGING

As described earlier, all the specific remote services are accessed via the PDG within the home network. All associated IP flows traverse through the PDG; thus, more accurate and service-specific charging information can be collected at the PDG. The resource consumption by each IP flow can be monitored and collected internally at the PDG. For charging of these traversing IP flows, the PDG is also connected to the OCS by the *Gy* reference point and to the CG by the *Gz* reference point. At establishment of a certain IP flow via the PDG, the PDG needs to request credit for IP flow charging from the OCS over the *Gy* reference point in a similar way as the 3GPP AAA server does over the *Wo* reference point for WLAN access charging.

The PDG also monitors the established IP flows and collects IP flow resource consumption charging information for those flows. For prepaid subscribers the PDG must ensure that the accumulated charging information does not exceed the downloaded credit from the OCS. After information consolidation the PDG reports IP flow charging information to the CG in a form of IP flow CDRs over *Gz*. In the billing system this information is then used for clearance of the billing between the home network operator, visited network operator, and WLAN provider as well as for creation of bills for post-paid users.

CONCLUSIONS

This article has described the functionalities relevant to a 3GPP-WLAN interworking system, which enables provisioning of public WLAN access service for 3GPP system subscribers by mobile operators. The described enabling functionalities are reuse of 3GPP subscription, network selection, 3GPP-system-based authentication, authorization, and security key agreement using SIM/USIM card, user data routing and service access, as well as end user charging. All these 3GPP-WLAN interworking functionalities are assumed to be achieved without setting any 3GPP-specific requirements on the actual WLAN access systems, but relying on the existing functionality available in a typical WLAN access network based on IEEE 802.11 standards.

The 3GPP specifications for enabling 3GPP-WLAN interworking functionality described in this article should be finalized by the end of 2003. After initial deployment the 3GPP-WLAN interworking system can be enhanced by new functionalities such as more advanced service support, say, to enable efficient support of real-time peer-to-peer IP-based communication, location services, and policy control functions via WLAN access. Another dimension in evolving the 3GPP-WLAN interworking system is to introduce technologies for dynamic switching between different types of WLAN or cellular IP connections without interruption to the consumed services (e.g., based on Mobile IP). The long-term evolution of the 3GPP-WLAN interworking system should lead toward a system

that provides reliable and secure access to a common set of IP-based services over a multitude of access technologies with all the complexity of the underlying technologies hidden from the user.

REFERENCES

- [1] 3GPP, "Group Services and System Aspects; 3GPP Systems to Wireless Local Area Network (WLAN) Interworking; System Description (Release 6)," TS 23.234. v. 1.10.0, May 2003.
- [2] H. Haverinen *et al.*, "Cellular Access Control and Charging for Mobile Operator Wireless Local Area Networks," *IEEE Wireless Commun.*, vol. 9, no. 6, Dec. 2002, pp. 52–60.
- [3] IEEE Std. 802.11b-1999, "Local and Metropolitan Area Networks — Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band," Sept. 1999.
- [4] IEEE Std. 802.11a-1999, "Local and Metropolitan Area Networks — Specific Requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band," Sept. 1999.
- [5] IEEE Std. 802.11g-2003, Local and Metropolitan Area Networks — Specific Requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band," 2003.
- [6] IEEE Std. 802.11i/D4.0, "Draft Amendment to Standard for Telecommunications and Information Exchange Between Systems — LAN/MAN Specific Requirements — Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements," May 2003.
- [7] IEEE Std. 802.1X-2001, "IEEE Standard for Local and Metropolitan Area Networks — Port-Based Network Access Control," June 2001.
- [8] C. Rigney *et al.*, "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, June 2000.
- [9] IEEE Std. 802.1Q-1998, "IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks," Dec. 1998.
- [10] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," IETF RFC 2284, Mar. 1998.
- [11] H. Haverinen and J. Salowey, Eds., "EAP SIM Authentication," IETF draft-haverinen-pppext-eap-sim-10.txt, Feb. 2003, work in progress.
- [12] J. Arkko and H. Haverinen, "EAP AKA Authentication," IETF draft-arkko-pppext-eap-aka-09.txt, Feb. 2003, work in progress.

BIOGRAPHIES

KALLE AHMAVAARA (kalle.ahmavaara@iki.fi) received a Master's degree in applied physics and mathematics from Helsinki University of Technology, Finland, in 1996. From then until June 2003 he was employed by Nokia Corporation in international R&D positions in several countries including Finland, Japan, and Spain. He has authored various journal and conference papers as well as several international patent applications. His professional interests are in the areas of evolving communication system architectures and protocols, and recently he has been concentrating on multi-access communication system technology convergence and beyond 3G system studies.

HENRY HAVERINEN (henry.haverinen@nokia.com) is a senior specialist at Nokia Mobile Phones, investigating mobile wireless networking, network security, and the interworking of WLAN and cellular technologies. He has published a number of papers in the areas of WLANs, mobile networking, and network security. He is a Ph.D. student at Tampere University of Technology, where he received an M.Sc. in 1998.

ROMAN PICHNA (roman.pichna@nokia.com) received an Ing. degree in radio electronics from Slovak Technical University, Bratislava, Slovakia, in 1987, and a Ph.D. degree in electrical and computer engineering from the University of Victoria, British Columbia, Canada, in 1996. He is currently with Nokia Networks, Espoo, Finland. His professional interests are in the areas of WLAN and network system architecture. He has authored several journal and conference papers and contributed to three books.

The long-term evolution of the 3GPP-WLAN interworking system should lead us toward a system that provides reliable and secure access to a common set of IP-based services over a multitude of access technologies with all the complexity of the underlying technologies hidden from the user.