SEAMLESS MOBILITY BETWEEN HOME NETWORKS AND CABLE SERVICES

Jay Strater and Gordon Beacham
Motorola

Abstract

Cable operators are now offering landline voice service in addition to video and high-speed data. However, cellular service is quickly becoming another important service for cable operators to offer to ensure that they stay in a competitive position with telephone companies.

This paper provides an overview of seamless mobile communications and its potential use by cable operators. It includes a description of seamless mobile applications and their value, network approaches for seamless mobility, and considerations for power management, Quality of Serivice (QoS), security, and Network Address Translation (NAT) traversal. The paper concludes with a discussion of other seamless mobility concepts revolving around the connected home.

INTRODUCTION

Through a careful development and standardization processes culminating in Data Over Cable Service Interface Specification (DOCSIS) in the late 1990's, cable operators have very successfully deployed high-speed data as a key element of the broadband service package. Cable operators are leaders in residential broadband, and are now leveraging this penetration to provide landline voice service using Voice-over-IP technology (VoIP) to POTS phones.

Landline voice service provides the "third leg" of cable's current "triple play", completing a service mix consisting of data, video, and voice. Nonetheless telephone companies are a competitive threat since teaming up with satellite-TV providers to offer their own voice, high-speed internet, and video service bundle. The three largest local telephone companies also own significant portions of the major wireless phone carriers, giving them a leg up on the cable providers by also offering cell phone service. Consequently, as enticing as landline voice service is, cellular service is quickly becoming another important service, a "quadruple play", for cable operators to offer to ensure that they stay in a competitive position.

Cable operators are interested in offering a mobile service with access to cellular and wireless local area network (WLAN) service using seamless mobility. In general terms seamless mobility is an approach that allows users to roam between application domains and communication networks without being aware of the underlying mechanisms that enable them to do so. This includes the scenario where a user moves between environments where different networking capabilities are present, but the network provides negotiation to allow for seamlessly transparent access. This differs from today's environment where handover between heterogeneous networks is not supported in most cases, and users are required to stop one communication service and initiate another between different networks.

Seamless mobile communications between cellular and WLAN environments refers to a service in which a user receives voice and data service on a dual-mode mobile handset when inside or outside a WLAN.[1] Service within a WLAN is provided via VoIP over unlicensed WLAN spectrum and DOCSIS in the case of a cable plant. Service outside the WLAN is provided via circuit switch cellular technology (GSM or CDMA) or VoIP over cellular or a 3G data network. Moreover, a voice call or data connection is seamlessly handed off between WLAN and cellular network as a user moves between them.

This paper provides an overview of seamless mobile communications and its potential use by cable operators. It includes a description of seamless mobile applications and their value, network approaches for seamless mobility, and considerations for power management, QoS, security, and NAT traversal. The paper concludes with a discussion of other seamless mobility concepts revolving around the connected home.

SEAMLESS MOBILE COMMUNICATIONS APPLICATIONS AND VALUE PROPOSITION

As described previously, we refer to seamless mobile communications as a service in which a user receives voice and data service on a dual-mode mobile handset with cellular and WLAN capability. Moreover, service in the WLAN is provided via VoIP over Wi-Fi and carried via DOCSIS in a cable plant. Service outside the WLAN is provided via cellular technology such as GSM or CDMA. A voice call or data connection is seamlessly handed off between WLAN and cellular networks as a user moves between them.

Seamless mobile communications may apply to residential or enterprise applications. Cable operators are focused on residential seamless communications initially but see value in an enterprise application longer term. A few differences exist between residential and enterprise applications. These include the number of access points, the call control technology and features, and the level of required security.

Residential applications typically require only one WLAN access point (AP) in a user's home whereas enterprise applications require multiple WLAN AP in a user's work location. Having multiple APs adds to the complexity of a seamless mobile communications solution by requiring micro-mobility management for call handover between APs in addition to macro-mobility handoff between WLAN and cellular service. In addition residential applications have phone service controlled from a central office (circuit or packet switched) and CLASS5 features offered, whereas enterprises typically have phone service controlled by a PBX (often an IP PBX using SIP or H.323 signaling protocols) along with enterprise features.

What are the benefits of seamless mobile communications? For residential users, the benefits may include:

- Reduced cellular bill resulting from off-loading the cellular air-interface when calls are made from the mobile handset in the home's WLAN[2]
- Improved in-home coverage and reliability which is often limited with cellular service
- Wireline audio quality because of a higher-rate codec thanks to WLAN and broadband connections

[1] A dual mode handset here refers to a mobile handset with functionality for cellular and WLAN operation.

[2] Cell phone contracts typically bill for a bulk number of minutes and residential VoIP service is typically an all-you-can-eat service. By switching your cell phone call to a Wi-Fi call, the minutes should now fall in the all-you-can-eat category.

- Convenience of a single mobile number and voice mail service, whether inside or outside the home
- Mobile and landline voice service inter-working, e.g. allowing for a shared “family” number as well as “individual” mobile and landline numbers

Studies indicate that users will still want access to their existing landline telephone service in addition to a mobile handset. Consequently, residential applications should also allow for a mobile handset and landline phone to inter-work. In the example noted above a “family” number implies a user selected mix of mobile and landline phones, allowing for group ringing and possibly line-extension service. By contrast an “individual” number implies a unique number for mobile handsets and landlines. Having “family” and “individual” numbers requires that distinctive ringing be supported.

For enterprise users, the benefits of seamless mobile communications may include:

- Cost savings from eliminating use of cellular calls in the enterprise, assuming cellular service is available and otherwise utilized in the enterprise
- Operational cost benefits from carrying VoIP and data on a single network; although this may already be realized if an IP PBX service is in place
- Wireline audio quality because of a higher-rate codec thanks to WLAN and broadband connection
- Convenience and productivity benefit of using a single device for all communications, whether inside or outside the office, whether at or away from ones desk

In addition to the benefits outlined above, users may receive advanced services and, through use of a common handset, consistent services inside and outside the enterprise and home.

For wireless carriers, the benefit of seamless mobile communications may include:

- Cellular capacity relief by off-loading of air-interface when user is in a WLAN at home or in the office
- Ability to offer residential phone service, in the case of independent wireless carriers (those without a wireline carrier affiliation)
- Increased customer satisfaction from improved in-home coverage, a key user network quality metric
- Improved customer retention (reduced churn) through unique value added services

For cable operators, the benefit of seamless mobile communications may include:

- A “quadruple play” service offering of data, video, voice, and wireless as in the case of cable operators, allowing added service bundling
- Greater pricing flexibly resulting from increased service bundling and migration of customers to higher revenue / margin wireless offerings
- Increased leverage of existing broadband infrastructure
- Ability to offer superior QoS over cable infrastructure (via DOCSIS 1.1 or higher QoS)
- Increased customer retention through bundling and possible value added services, including interworking of mobile and landline phone services

The presumption is that by bundling services, a broadband carrier will present a customer with only one bill, and offer some service discounting compared with offering services individually.

Finally for vendors, the benefit of seamless mobile communications may include:

- Increased handset, modem, and access point /gateway sales
- Increased core network equipment sales
- New opportunities for integration and deployment services

In summary, seamless mobile communications appears to offer a win-win solution for all stake-holders. And as stated in the introduction, having a "quadruple play" is quickly becoming a service cable operators will need to stay competitive.

NETWORK APPROACHES FOR SEAMLESS MOBILE COMMUNICATIONS

An important aspect of any seamless mobility solution is providing an easy-to-use service that is transparent to the user. Ease of use and seamless service functionality can be achieved by including intelligence in the network or in end user devices. The most likely point for intelligence to be implemented is in the network with varying levels of support in the end user devices.

We know of three fundamentally different network approaches to providing mobile seamless communications. They include call forwarding, Unlicensed Mobile Access (UMA), and Third Generation Partnership Project (3GPP) IP Multimedia Subsystem (IMS) technologies.

Call Forwarding

In a call forwarding approach, a specialized mobility management element is integrated (logically or functionally) with a call management server (CMS) serving landline phones and mobile/dual-mode handsets in a WLAN. For residential applications the CMS would reside in a central office whereas for enterprise applications the CMS may reside in the enterprise as an IP PBX. In either case there is no need for changes at a cellular Mobile Switching Center (MSC).

A phone number is assigned at the CMS to each dual-mode handset as well as landline phones served by the CMS. Calls destined to a dual-mode handset's CMS number when the handset is inside a WLAN are served directly by the CMS. Calls destined to the dual-mode handset's CMS number when the handset is outside the WLAN (in the handset's cellular WAN) are forwarded by the CMS to the handset's cellular number. Seamless handover between (into or out of) WLAN and cellular WAN is provided for any calls to the dual-mode handset's CMS number, and any calls initiated by the dual-mode handset from inside the WLAN or to a phone controlled by the handset's CMS.

For single number reachability and seamless mobility to be supported as outlined above, all calls must pass through the CMS/mobility management element(s). Consequently the handset's CMS number must be the only number advertised to friends and colleagues.

The following figure illustrates an example of a call-forwarding network architecture. VoIP signaling and bearer transport protocols are shown, data is not.

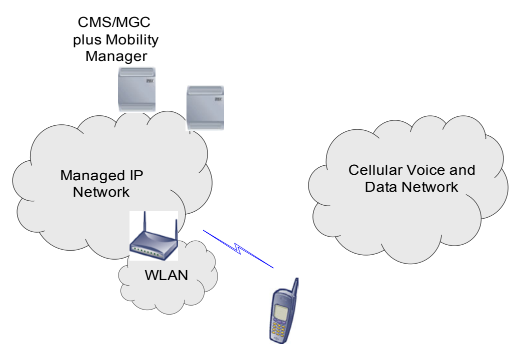

Figure 1. Example Network Architecture for Call-Forwarding Approach

The call-forwarding approach has the benefit of making maximum use of existing CMS and media gateway resources if present. As such new integration requirements with operator back-office systems may be minimized and use of common features for landline phones and mobile handsets may be maximized. The call forwarding approach has the disadvantage of imposing inefficient routes via dog-legged calls that must always be anchored at a CMS, even if the CMS is far from source and destination. This inefficiency may prove costly from a PSTN interconnect perspective and also from a transcoding, performance perpective, when transcoding is required.[3] Also support for seamless mobile handover from cellular WAN to WLAN is not possible when calls are initiated by a dual-mode handset in the cellular WAN to a phone outside the control of the dual-mode handset's CMS. Finally seamless mobility call forwarding approaches are not currently standardized, raising the concern over single supplier cost premiums and limited product availability.[4]

Unlicensed Mobile Access

With UMA technology, GSM and GPRS signaling and RTP and IP data traffic are carried over an IPsec tunnel between a dual-mode handset and UMA network controller (UNC) when the handset is in a WLAN. The UNC emulates a GSM base station controller (BSC), providing a gateway between WLAN and cellular WAN signaling and traffic. GSM signaling is used to signal when a user moves between a UNC and a BSC for mobility management and handover purposes. The cellular number maintained at the cellular carrier's home location registrar (HLR) identifies the user.

[3] Transcoding between WLAN and PSTN can be avoided by utilizing G.711 while in the WLAN.

[4] Even if signaling from handset to mobility manager is SIP based, unique SIP extensions are likely required to support specific mobility and handoff signaling requirements. To date no call forwarding approaches we know of have been standardized. However Motorola, Avaya and Proxim have developed an enterprise solution that they are working to move into an industry standard.

The following figure illustrates an example UMA network architecture. VoIP signaling and bearer transport protocols are shown, data is not.

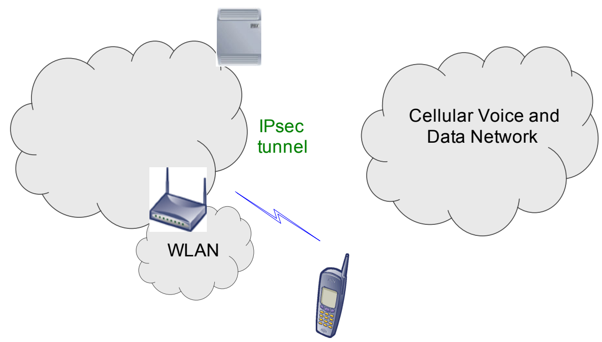

Figure 2. Example UMA Network Architecture

The UMA approach has the benefit of requiring little change to an existing GSM cellular infrastructure, only requiring the addition of a UNC. As such the approach offers a quick time-to-market solution for cellular operators. It also has specifications that are governed by a consortium of cellular operators and vendors. The UMA approach has the disadvantage of being limited to GSM systems. And because it utilizes existing GSM infrastructure it is limited in terms of offering new, advanced IP-based services (limited to what an existing MSC offer). Moreover a major investment in current-technology GSM infrastructure including MSCs would be required for those operators without GSM infrastructure (most MSOs) to deploy a UMA solution.[5]

IP Multimedia Subsystem

[5] Otherwise, an unorthodox business arrangement would be required in which a cellular operator Mobile Switching Center (MSC) allows access from a 3rd party operator's UNC. In any case, cable operators could still receive revenue from a UMA solution offered by cellular operators over a cable operator's infrastructure. In this case the cable operator could provide the cellular operator QoS on the DOCSIS network and charge for it accordingly. Of course cellular operators can also use the DOCSIS network without permission or knowledge of the cable operator and offer a best effort VoIP service.

With IMS technology, VoIP is provided via SIP signaling and RTP traffic between a dual-mode handset and call control elements in an IMS core network when the dual-mode handset is in a WLAN. The same applies if a dual-mode handset is in a 3G cellular network that supports VoIP over its data network. When a handset is in a circuit-switched cellular network, circuit-switched signaling and voice are converted to SIP signaling and RTP at an IMS signaling and media gateway respectively. To neighboring MSCs in a circuit-switched cellular WAN, the IMS core looks like another MSC. Yet all signaling within the IMS core network remains SIP based with WLAN and cellular call mobility controlled from the core.[6] In essence, the IMS core provides WLAN and cellular network-agnostic access control with centralized application services.

A cellular number is maintained at the home location registrar (HLR) associated with the IMS core network and identifies the user. However additional numbers at the IMS core could be used for identifying a dual-mode handset when in the WLAN. This allows flexibility to support "family" and "individual" phone numbers when the handset is in the WLAN.

Note that IMS, which is developed by the 3GPP forum, applies to GSM-based cellular network technologies. In contrast, CDMA-based cellular network techologies have an IP core solution like IMS as directed by 3GPP2 Multimedia Domain (MMD) forum. Therefore, we refer to IMS as a cellular core technology for supporting any cellular network technology. Note also that seamless handoff between cellular networks and/or WLAN has not been specified as yet. Its specification is anticipated as another SIP application serving an IMS serving call session control function (S-CSCF).

[6] 3GPP SIP header extensions are used in IMS SIP signaling.

The following figure illustrates an example IMS network architecture. VoIP signaling and bearer transport protocols are shown, data is not.[7]

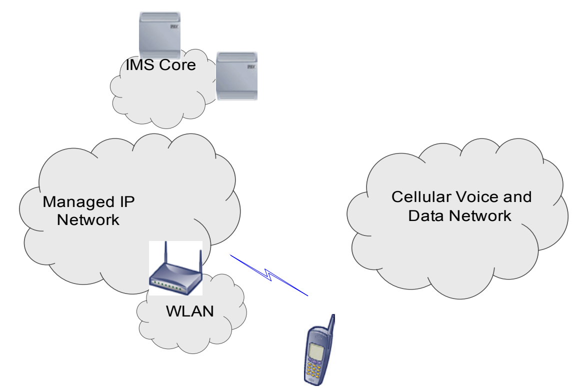

Figure 3. Example IMS Network Architecture

Compared to UMA, the IMS approach has the benefit of being RAN agnostic and facilitating rapid deployment of enhanced packet-switched services. It also has the benefit of allowing a cable operator the flexibility of controlling a dual-mode handset when on a WLAN connected to their broadband network. Compared to call forwarding, the IMS approach has the benefit of being governed by a set of standards (developed by 3GPP) and avoiding route, functionality and potential performance issues of the call forwarding approach. A limitation of IMS is that it does not make use of existing Call

[7] Of the IMS signaling elements: the HSS provides Home Subscriber Server with AAA and Databases. The Application Servers (AS) include a Session Initiation Protocol (SIP) AS, an Open Service Access (OSA) Service Capability Server (SCS) & OSA AS, and an AIN Interworking Server. The CSCF is the Call Session Control Function which has 3 flavors. Serving-CSCF provides session control for endpoint devices, Interogating-CSCF is an entry point to IMS from other networks, and Proxy-CSCF is an entry point to IMS for devices. The BGCF is the Breakout Gateway Control Function which selects networks to use for PSTN/PLMN interworking. The MGCF is the Media Gateway Control Function which controls the MGW. The MRFC is the Multimedia Resource Function Controller which controls MRFP (media server). And the PDF is the Policy Decision Function which authorizes QoS requests.

Management Servers (CMS) and media gateway resources for VoIP-based landline phone service. Dual-mode handset and landline inter-working is expected to be the subject for Phase 2 of the PacketCable 2.0 cellular integration initiative.

In summary, of the three alternatives discussed, IMS appears to offer the most promising solution to cable operators from a business, functional, cost, and performance perspective.

POWER MANAGEMENT, SECURITY, QOS, AND NAT TRAVERSAL CONSIDERATIONS

Aside from providing seamless roaming between WLAN and cellular WAN and enhanced services, seamless mobile communications solutions must address several critical factors in order to provide a viable service. These include handset power management, security, QoS, and NAT transversal for operation from a WLAN.

Power Management

Power management is required for a dual-mode handset in a WLAN to have active and idle talk time that is comparable to that in typical cellular service. Without power management active talk time may be reduced from hours to minutes and idle talk time may be reduced from tens of hours to single-digit hours.

Through the development of an enterprise seamless mobility solution, Motorola identified several factors as necessary for improving battery life in a dual-mode handset. These include choosing a low-power 802.11 chipset in the handset, running the handset with one radio at a time (cellular WAN or WLAN), providing fast switching technology to select WLAN/WAN, and implementing a new 802.11 power management approach for VoIP traffic. In the latter case, legacy 802.11 power management alone was found to be inadequate. To understand what new 802.11 power management approach was selected for VoIP traffic, it is first necessary to understand why legacy 802.11 power management was found inadequate.

In 802.11, legacy power management allows a station (dual-mode handset in our application) to receive data from an AP at infrequent intervals and only when data is available at the AP for delivery. AP data transfer may be scheduled to occur at Delivery Traffic Indication Message (DTIM) beacons, spaced say 300ms apart. Utilizing this timing, a station need only wake its processor infrequently to listen to selected AP beacons and poll the AP for its data if the AP indicates its data is available (via Traffic Indication Map).[8] However, VoIP traffic sent between station and AP during a VoIP call requires a short packet exchange intervals, say 20ms. Consequently, if legacy 802.11 power management were used it would need to have shortened beacon intervals of say 20ms to accommodate the VoIP traffic. In that case, processor sleep time would be very limited, particularly during idle call periods.

The new 802.11 power management approach is a method for allowing periodic frame exchange between a station and AP during a VoIP call while legacy power management is still utilized for data frame exchange. A station activates the new power management approach when it negotiates an admitted VoIP traffic stream (or any periodic frame transfer stream) with its AP. An AP then buffers frames from the VoIP traffic stream destined to the station and, when a station wakes up at a designated VoIP frame interval (presumably set to the VoIP packetization period), it sends a VoIP frame with an implicit "poll" request to its AP. The

[8] An AP responds to a poll with a buffered frame. The handset must poll for more buffered data if more exists. The AP will also send broadcast and multicast data right after DTIM beacons.

AP responds to a poll request with buffered VoIP stream frame(s).

This new power management approach has been pushed into the 802.11e standard where it is referred to as Unscheduled Automatic Power Save Delivery (U-APSD). U-APSD may be enabled when the U-APSD station issues a bi-directional Traffic Specification (T-SPEC) to its AP at the start of a VoIP call[9]. The AP buffers frames matching the Access Category (AC) for the T-SPEC according to the method described previously. The following figure illustrates U-APSD from the perspective of AP and station (subscriber unit).

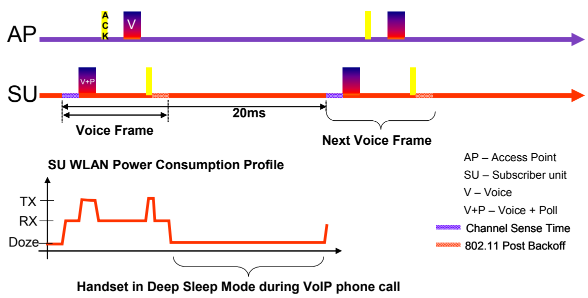

Figure 4. U-APSD Operation

<u>Security</u>

Security for a dual-mode handset operating from a WLAN is necessary to prevent user traffic (VoIP and data) from being denied, stolen, or eaves-dropped. The level of security offered should be commensurate with the level of threat and the impact of a successful security attack.

Security should be provided on the WLAN between handset and AP and end-to-end between handset and network infrastructure. For Wi-Fi access security, several standard approaches are possible. For residential applications, wireless protected access with pre-shared key (WPA-PSK) is a logical choice. WPA-PSK is based on the 802.11i draft 3 for authentication and encryption. Using WPA-PSK, mutual authentication, key verification and derivation between the station/handset and AP is established using an 802.1x handshake. This is illustrated in the following figure.

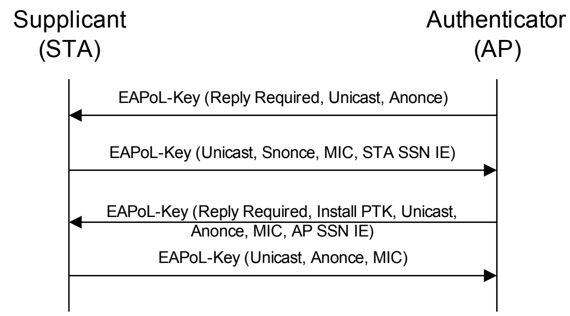

Figure 5. 802.11i WPA-PSK Example with Supplicant and Authenticator

After successful authentication, the Temporal Key Integrity Protocol (TKIP) encryption algorithm is used to encrypt session traffic. WPA2-PSK is another logical choice for residential applications. WPA2-PSK is an evolution of WPA-PSK, based on the final ratified 802.11i standard and includes use of the Advanced Encryption Standard (AES) encryption algorithm instead of TKIP.

For enterprise applications, WPA or WPA2 using an operator selected Extensible Authentication Protocol (EAP) method is appropriate. EAP methods may include mutual authentication schemes based on X.509 certificates (i.e., EAP-Transport Layer Security (TLS)), or other alternatives such as EAP-Tunnel TLS (TTLS), EAP-Subscriber Identity Module (SIM), etc. EAP message exchanges are illustrated in the following figure.

[9] 802.11e draft 12 also provides a mechanism for a station to enable U-APSD in its reassociation request frame, without submitting a T-SPEC.

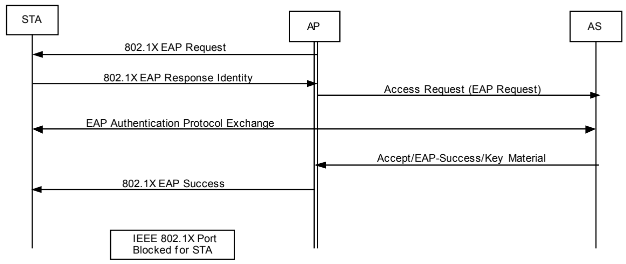

Figure 6. 802.11i Example with Supplicant, Authenticator, and Authentication Server

For end-to-end security, handset authentication and authorization is necessary to mitigate theft of service. In addition an IPsec tunnel may be utilized to protect VoIP, data, and signaling traffic. UMA and 3GPP IMS standards specify use of an IPsec tunnel and EAP authentication. In the case of UMA, an IPsec tunnel is established between a handset and UNC. The tunnel follows authentication between handset and UNC secure gateway and AAA server. Authentication is performed using EAP-SIM within IKEv2. IKEv2 is used to authenticate a UNC to a handset and EAP SIM is used to authenticate a handset to a network Authentication Authorization and Accounting (AAA) server, as relayed by the UNC's security gateway. UMA requires authentication and establishment of an IPsec tunnel with at least two UNCs as part of handset discovery and registration.[10]

In the case of IMS, an IPsec tunnel is established between a handset and Packet Data Gateway (PDG). As part of the tunnel establishment, the PDG contacts a 3GPP AAA Server in the Home Public Land Mobile Network (HPLMN) for authorization of the mobile.[11] IMS may require several IPsec tunnel attempts, starting with PDG associated with a handset's Visiting PLMN and progressing to PDG associated with its HPLMN.[12] Authentication between handset and AAA server uses either EAP-SIM or EAP-Authentication and Key Agreement (AKA).

Note that enterprise solutions may also utilize separate VPN security for remote data access.

QoS

QoS for VoIP calls from a dual-mode handset when operating in a WLAN should be comparable to landline-like voice service to differentiate service from competitive VoIP service providers. QoS should be provided over the WLAN between handset and AP, and end-to-end between handset and network infrastructure.

The 802.11e standard provides QoS methods for a Wi-Fi network. It includes specifications for prioritized and parameterized QoS in two basic access approaches: Enhanced Distributed Channel Access (EDCA) service and Hybrid Coordination Function Controlled Channel Access (HCCA). EDCA is a prioritized CSMA/CA access mechanism offering four differentiated service Access Categories (AC). EDCA also offers a level of parameterized

[10] UMA clients are provisioned with or derive the FQDN for their provisioning UNC and UNC SGW. After resolving these addresses, a UMA client sets up a secure tunnel with the provisioning UNC to discover the FQDN or IP address of its default UNC and UNC Security Gateway (SGW). The UMA client then sets up a secure tunnel to its default UNC and attempts to register. The UMA client's default UNC may deflect the UMA client to an alternate serving UNC. In this case the UNC client will establish a secure tunnel this UNC and register.

[11] The service authorization decision is made by the 3GPP AAA Server based on subscription information retrieved from the IMS HSS/HLR.

[12] A handset will initially construct an FQDN based on its Visitor Public Land Mobile Network (VPLMN) and use it to discover (via DNS) a set of visited-network PDG IP addresses to attempt IPsec tunnel establishment with. Should these addresses not be reachable or the AAA server reject access to them, the handset will then construct a new FQDN based on its HPLMN and attempt IPsec tunnel establishment with a home-network PDG.

QoS for time sensitive traffic flows such as VoIP. A T-SPEC with AP admission control is used to establish a traffic stream. HCCA is a more complex approach involving a mix of contention and contention free periods (CFP). It provides T-SPEC parameterized QoS for time sensitive traffic using scheduled transmission opportunities in the CFP.

Several subsets of the 802.11e standard were identified by the Wi-Fi Alliance in order to expedite interoperability testing for WLAN QoS. Wireless Multimedia Extension (WME) features and more recently the Wireless Multi Media (WMM) features were chosen based on the EDCA. Compliance to these tests is mandatory for many solutions, making EDCA commonly utilized. With EDCA, VoIP calls are typically assigned a T-SPEC with QoS parameters that limit delay and jitter and with AC value set to VO, the highest level.

For end-to-end QoS, IP differentiated services per RFC2474 (DiffServ) should be considered. DiffServ sets packet priority via a Differentiated Services Code Point (DSCP) field of an IP header. For upstream traffic from dual-mode handsets in a Wi-Fi network a DSCP assignment could be used to classify a VoIP packet onto an 802.11e VoIP T-SPEC with AC_VO, established at the start of the call. It could also be used to classify a VoIP packet onto a DOCSIS Unsolicited Grant Service (UGS) service flow in the case of cable modem service, also established at the start of the call. In this case, PacketCable Multi-Media (PCMM) is needed for establishing a UGS service flow for the upstream VoIP call.[13]

In the case of downstream end-to-end traffic a reverse process would apply. A DSCP assignment at the other end of the VoIP call (terminating handset, MTA, or media gateway) could be used to classify a VoIP packet such that it receives proper DOCSIS downstream service flow assignment at the CMTS and 802.11e T-SPEC at a Wi-Fi AP. Downstream service flows would also have been established at the start of a VoIP call.[14]

The 802.1d or 802.1p user priority should also be assigned for priority queuing at an Ethernet switch. The following table provides a listing of typical assignments for 802.1d, 802.11e AC, and RFC2474 DSCP.

Table 1. Typical Relationships for QoS Assignments

8021D User Priority	80211e Access Category	RFC2474 DSCP Bits	Recommended Traffic Category
1, 2	AC_BK	001xxx or 010xxx	Background
0, 3	AC_BE	000xxx or 011xxx	Best Effort
4, 5	AC_VI	100xxx or 101xxx	Video
6, 7	AC_VO	110xxx or 111xxx	Voice

Note that there are various techniques that can be used for associating signaling and media to an 802.11e AC. In one case a station/handset could have a default AC method for signaling and media. In another case, a station could use UPnP to discover a UPnP capable AP's QoS capabilities and adjust its signaling and media ACs accordingly.

NAT Traversal

Dual-mode handset traffic (voice or data) should be allowed to pass through any residential gateway for a seamless solution to be widely deployed. This includes gateways with network address and port translation (NAPT).

[13] PCMM QoS is initiated by an Application Manager which, for a seamless mobility solution, would need to be affiliated with an IP PBX or CMS in a call forwarding solution, the UNC in a UMA solution, or an S-CSCF in an IMS solution.

[14] In the case of a DOCSIS downstream, the service flow would need a minimum reserved rate to be assigned via PCMM.

Two issues concern setting up and passing VoIP traffic through a NAPTing gateway. The first issue is that protocols that embed local IP or port information in signaling messages (i.e., SDP in SIP) will not be reachable through a NAPTing gateway without a solution that provides the device behind the gateway (dual-mode handset) with information about its NATed IP address and port or without a network server that provides address translation from local to routable addresses.[15] Simple Traversal of UDP through NAT (STUN) or Traversal Using Relay NAT (TURN) are two approaches that provide a client device behind the gateway with information about its NATed IP address and port.

There are four types of NAT implementations: full cone, restricted cone, port restricted cone, and symmetric as defined in [9]. STUN is a solution for full cone, restricted cone, or port restricted cone NAT implementations. However, in the case of a symmetric NAT implementation, STUN is not an effective solution because it will not work with connection oriented media using RTP. This is because a symmetric NAT will have different NAT mappings for each destination IP address and port. The symmetric NAT requires a VoIP client to send and receive RTP packets to and from the same IP address and port. For symmetric NAT implementations, TURN is a possible solution. TURN involves using an RTP relay server between communicating VoIP clients.

Unfortunately, the TURN solution has some disadvantages. It is processing intensive on the RTP relay server, raising issues of scalability, and it introduces undesirable delay into the communication path. In addition, both the STUN and TURN solutions require application layer support on the handset and the STUN/TURN server(s) in the service provider network must be on the public Internet, making them susceptible to threats such as denial of service attacks.

The second issue with pasing VoIP traffic through a NAPTing gateway is that if IPsec tunneling is utilized, NAPTing will not be possible without the handset providing UDP Encapsulated IPsec/ESP Tunnel Mode. This is because IPsec tunneling without UDP encapsulation only presents an unencrypted IP header field, providing no UDP field for port address translation. UDP Encapsulated IPsec/ESP Tunnel Mode provides an outer IP and UDP field for NAPTing as shown in the following figure.

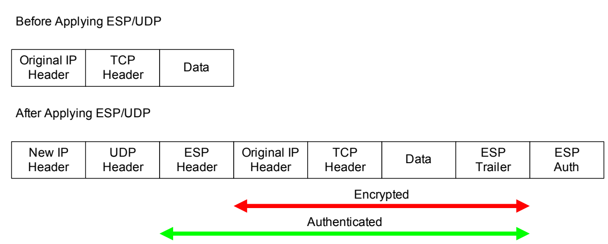

Figure 7. UDP Encapsulated IPSEC/ESP Tunnel Mode

When a NAPTing residential gateway receives a UDP Encapsulated IPsec/ESP tunneled packet (e.g. an RTP VoIP packet from a dual-mode handset when in a WLAN), it conducts the following operation:

1) replaces the Source IP Address in the outer IP packet header with the WAN IP address of the AP
2) replaces the Source Port in the outer UDP packet header with the UDP port selected by NAPT
3) recomputes the IP packet Header Checksum in the outer IP packet header[16]

[15] A gateway ALG may also be used but it is limited to scenarios in which signaling is not encrypted, a scenario that can not be relied on. An ALG can not be utilized with IPsec since there is no SIP port number in the IP payload for the ALG to key off. In addition, the inner IP header and contents are all encrypted and cannot be parsed or changed by the ALG.

[16] The Header Checksum provides a verification that the information used in processing an internet datagram

UMA and IMS require use of UDP Encapsulated IPsec/ESP Tunnel Mode for IPsec tunneled VoIP from a WLAN.

OTHER SEAMLESS MOBILITY CONCEPTS

As mentioned previously, seamless mobility in general terms is an approach that allows users to roam between application domains and communication networks without being aware of the underlying mechanisms that enable them to do so. This may include providing seamless mobility for voice and data communication from a multi-mode handset. It may also mean receiving access to a "family" number from any phone in the house or getting access to caller ID, call logs, and or billing information from a TV. In the most general sense, seamless mobility is more than seamless handover from a single device but having access to a common application or user experience from different devices at different locations. Furthermore, seamless mobility need not only apply to communications but may apply to other applications and experiences such as home monitoring and control, purchased content management, and personal content management.

In the case of home monitoring and control, seamless mobility is a means for allowing users access to their home monitoring and control system while on their home network, via a Web portal from anywhere on the Internet, from their cell phone, from their home TV/STB, and even from an automobile assistance service. The following figure illustrates these concepts.

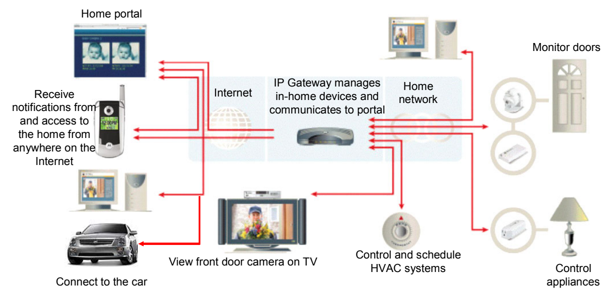

Figure 8. Home Monitoring and Control Seamless Mobility Scenario

In this example an IP gateway device in the home may be used to provide an "always on" portal between in-home devices and communications access. Home monitoring devices may have wired or wireless connections to the gateway. These devices may use non-IP protocols, in which case they are proxied on to the home network through a protocol translator to make them look like they have native IP. What is key to the concepts in this and other seamless mobility solutions is that a user's seamless mobile experience is consistent (same "look and feel") across the different access platforms, even with varying levels of features being accessible at different platforms.

In the case of purchased content management, seamless mobility implies a means of allowing users to purchase music and video content from home and cell phone, to store and manage content, to play content from a home stereo, TV, and cell phone, and to transfer content to CD, portable audio and video player, and automobile. The following figure illustrates these concepts.

has been transmitted correctly. The data may contain errors. If the header checksum fails, the internet datagram is discarded at once by the entity which detects the error.

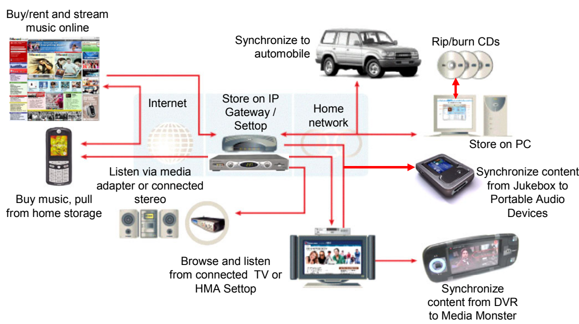

Figure 9. Purchased Content Management Seamless Mobility Scenario

In this example an IP gateway or Digital Video Recorder (DVR) Set Top Box (STB) device in the home may provide "always on" content and storage management. A partnership may be established with online content providers for seamless content purchases. Networked playback devices may be standalone or integrated. Portable audio and video players should be home network docked. Access from a gateway to automobile will need to occur via a wireless home networking connection. Digital rights management (DRM) licensing requirements may limit which devices and which network types that purchased content may have access to.

In the case of personal content management, seamless mobility implies a means of allowing users to store and manage family digital photos or video from camera, camcorder, and cell phone, to display content on TV, digital frames, or cell phone, and to order prints for digital photos over the internet. The following figure illustrates these concepts.

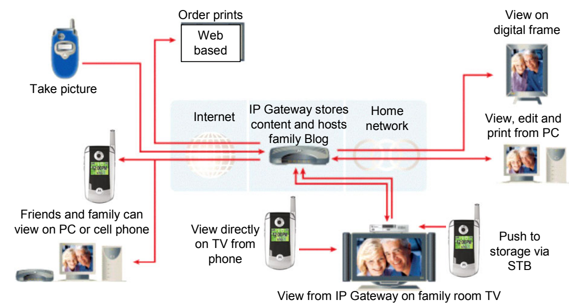

Figure 10. Personal Content Management Seamless Mobility Scenario

In this example an IP gateway device in the home may provide "always on" content and storage management as well as a family Blog. Accessory devices may be utilized for viewing photos. A partnership may also be established with online printing services for seamless print ordering.

SUMMARY AND CONCLUSIONS

Seamless mobile communications is an approach that allows users to roam between application domains and communication networks without being aware of the underlying technology or mechanisms that facilitate transparent mobility. It promises to provide value to residential and enterprise users, operators, and vendors.

Three different approaches to achieving seamless mobile communications were presented: Call Forwarding, UMA, and IMS. An IMS solution appears to be the superior choice for Cable operators.

Any seamless mobile communication solution must also account for power management, QoS, security and NAT traversal to be a complete service offering. For a dual-mode handset solution to provide acceptable battery life, additional power management techniques based on U-APSD are essential for a dual-mode handset service offering to be competitive with user expectations of cellular standby/talk times. In addition, proper handling of QoS on the WLAN and end-to-end is important in order to provide high quality audio and differentiate service offerings between competitive VoIP service providers. Security of the WLAN and end-to-end is should be provided and WPA2-PSK and WPA2 are good solutions for residential and enterprise WLAN applications respectively. NAT traversal is also an important consideration due to the variety of NAT implementations and detection capabilities of network equipment deployed in residential and enterprise environments.

Finally, seamless mobility need not only apply to communications but may apply to other applications and experiences such as home monitoring and control, purchased content management, and personal content management.

REFERENCES

1. UMA Architecture (Stage 2) R1.0.2 (2004-11-03), Technical Specification.
2. 3GPP Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) interworking; System description TS 23.234 V6.2.0 (2004-09).
3. IEEE Wireless LAN Edition, Standards Information Network IEEE Press compilation based on
4. IEEE Std 802.11TM-1999 (R2003) and its amendments.
5. IEEE Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements, Std 802.11i-2004.
6. IEEE Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment : Medium Access Control (MAC) Enhancements for Quality of Service (QoS) P802.11e/D12.0, November 2004.
7. IETF RFC 2474, Definition of the Differentiated Services Field (DS Field).
8. IETF RFC 3948, UDP Encapsulation of IPsec ESP Packets.
9. IETF RFC 3489, Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs).
10. IETF Internet Draft, Traversal Using Relay NAT (TURN). Work in progress.