IMS AND THE IMPORTANCE OF ACCESS NETWORK MANAGEMENT

Rich Higgins
C-COR, Inc.

Abstract

IP Multimedia Subsystem (IMS) is positioned to become the primary next generation IP network services architecture for broadband service providers worldwide. IMS has the potential to increase revenue opportunities by allowing greater flexibility in both services and the types of devices that consumers will use to access these services. IMS also has the potential to lower service development costs and reduce time to market.

The need for access network management both to prevent theft/abuse and ensure a quality user experience grows as more services come to depend on this shared infrastructure.

This paper will examine some of the IMS architecture/service elements and the implications of IMS for the cable access network architecture with particular emphasis on the Policy Decision Function (PDF) and access network security.

INTRODUCTION

Background

IP Multimedia Subsystem is an architecture which defines a platform for the delivery of multimedia services via the IP protocol. It is largely derived from specifications developed by the 3rd Generation Partnership Project (3GPP) but incorporates many standards from the Internet Engineering Task Force (IETF). IMS was originally developed to provide mobile operators the ability to offer IP based services to subscribers via cellular networks.

A number of other standards bodies have adopted IMS as a basis for their ongoing work. The European Telecommunications Standards Institute (ESTI) Tispan project is extending IMS to include support for legacy telecom systems. ESTI has agreed that Tispan developed specifications will be submitted to the 3GPP body for approval and inclusion in future IMS releases. CableLabs, via PacketCable 2.0, is focused on extending release 6 to include support for cable HFC access networks. Other standards groups such as the International Telecommunications Union (ITU), the Alliance for Telecommunications Industry Solutions (ATIS), the Open Mobile Alliance (OMA), the GSM Association, and 3GPP2 are also following the progress of IMS closely and are expected to be heavily influenced by it. It is expected that IMS release 7 will include some of these extensions as well as important enhancements such as better end-to-end quality of service and policy control definitions.

The following section provides a very brief look at the IMS architecture for those who may be unfamiliar with the basic principles of operation.

IMS Overview

Traditional telecom operators have long sought a Service Delivery Platform (SDP) which would be based on a common infrastructure and would allow for the rapid and inexpensive development and deployment of new services. IMS incorporates many of the features desired of an SDP. In the IMS model both the Core (or control) layer and the Service (or application) layer are access agnostic and are accessible using standards based protocols.

Any access mechanism that is IMS compliant can make use of the complete suite of control functionality offered by the core as well as applications in the service layer. New services need be developed only once as they are independent of the access network. It no longer matters whether a subscriber is requesting service via a cable network or over a cell phone. All that matters is the availability of the necessary resources to provide the requested service.

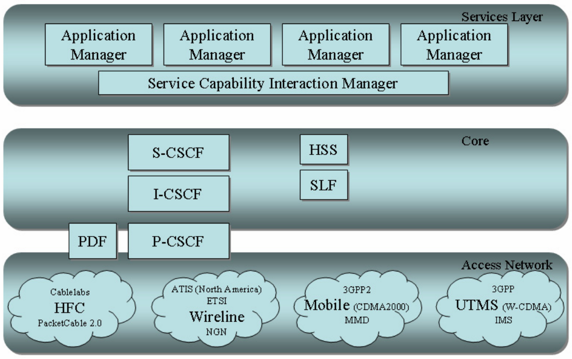

Figure 1. IMS Architecture

As shown in

Figure 1 immediately above the access network layer is the core or control layer. The core contains the Call Session Control Function (CSCF) as well as specific systems which support this general processing function. It is the Proxy CSCF (P-CSCF) which acts as the interface between the access network and the IMS core. All requests for services from any end user device (referred to in the IMS specifications as User Equipment or UE) regardless of access mechanism are initially handled by the P-CSCF.

The Interrogating CSCF (I-CSCF) provides an access point into a specific operator network. If the P-CSCF is located in the subscriber's home network then requests for services may (or may not) route directly to the Serving CSCF (S-CSCF) depending on the number and configuration of S-CSCF's in the network. If the P-CSCF, which is requesting services, is located in a network that is not the UE's home network the I-CSCF of the home network is contacted and will determine the appropriate S-CSCF to route the service request.

It is the S-CSCF that is responsible for actually servicing the request(s) of the subscriber that is associated with that server. The S-CSCF interacts directly with the Services Layer and the various Applications Managers. The S-CSCF also interacts with the Home Subscriber Server (HSS) which is a database of information about the subscriber. Specifically, the HSS maintains the mapping between the subscriber and the S-CSCF, subscriber service profile, and security (identity) information.

The Policy Decision Function (PDF) is responsible for authorizing quality of service for the media in accordance with the parameters of the service request and the operators established business rules. In a PacketCable 2.0 implementation it is likely that the PDF functions will be performed by the PCMM Policy Server.

The Subscriber Location Function (SLF) is also defined in the IMS specifications and serves to identify the HSS that contains information about a specific subscriber. Also identified by the IMS specs is a function referred to as the Service Capability Interaction Manager (SCIM). The SCIM was envisioned as a service broker between application mangers. As of release 6 this component was ill defined and there is considerable debate as to the necessity for a separate SCIM.

Increased Revenue Opportunities

The disassociation of access, control, and services creates new service opportunities which would be difficult, at best, to host in a traditional "vertical" service environment. Because the control and services layers operate in the same way regardless of access network, development of services which span access devices will be simplified. New services could include multi-mode IP phones that operate wirelessly via Bluetooth or WiFi connected to an HFC network while in range of a home networking device but which switch seamlessly to a cellular network when the handset leaves the home.

IMS also incorporates the concept of "presence" in which the network itself contains intelligence about the subscriber's location and access device capabilities. It is possible to envision future service in which a voice only call may be initiated via a relatively low bit rate cellular connection while the user is driving to work but switches automatically to a video conference as the user enters their office environment.

The IMS infrastructure will allow subscribers to access content regardless of their broadband access network (HFC, DSL, WiFi, WiMAX, 3G, etc.). This unfettered service access will lead to service roaming beyond simple voice. Subscribers no longer need be tied to their desk, or their television, or their telephone in order to access the services or content that they desire.

Reduced Development Costs

In proprietary service environments providers have had to resort to developing their own applications from scratch. At best, they could rely on a few select vendors to develop services which frequently required long, expensive, and sometimes arduous integration periods.

In an IMS environment interfaces and the underlying protocols are well known and very actively used by the development community. Development environments and simulation tools exist that allow applications to be developed independent of the provider or network. It is reasonable to expect that application development will move more toward an "Internet like" model where new services are rapidly created and deployed.

Reduced Time to Market

Because application development is no longer necessarily confined to a specific platform the number of potential developers increases dramatically. Competition for new applications will not be confined to large vendors only but will be open to startups and even individuals. This model begins to more closely resemble the Internet model of application development and deployment.

If, indeed, application development becomes more "Internet like" it is reasonable to assume that the speed with which the applications are developed and deployed in an IMS environment will be similar. Groups are already working on standardizing interfaces to the IMS services layer to ease development of IMS applications. The Java Community Process describes their JSR 281 standard as follows, *"This JSR is intended to enable application programmers to easily write applications that can integrate with the IP Multimedia Subsystem (IMS). The specification will expose IMS functionality through high-level*

APIs in an integrated and consistent way. The API hides IMS implementation details to the maximum extent. The API abstracts the underlying technology and at the same time provides the developers with maximum flexibility. This approach secures conformance to IMS related standards and at the same time gives developers possibility to focus on the functionality of the services and not on the IMS technology implementation details. In this way IMS domain will be revealed to the broad J2ME developer community and will encourage faster adoption of the IMS services provided by the wireless networks." [1]

ACCESS NETWORK SECURITY

Opening the network to a multiplicity of access devices and (potentially) external service provider networks raises concerns particularly regarding user authentication.

Security threats to the network generally fall into one of three categories:

- Theft of service
- Denial or disruption of service
- Information theft (subscriber or provider)

IMS security standards are extensive and designed to deal effectively with each of these threats. A complete discussion of IMS security is well beyond the scope of this paper.[2] Instead, this discussion will focus only on the access portion of the IMS network and the security enhancements required for cable.

Authentication

In keeping with its wireless roots, release 6 of the IMS standards authentication of the user equipment (UE) is handled by an application running on a Universal Integrated Circuit Card (UICC). Authentication between the UE and the P-CSCF in handled via a challenge response mechanism known as Authentication and Key Agreement (AKA) specifically UMTS AKA. Similarly, authentication between the UE and the core network is handled via ISM AKA.[3]

During initial registration the UE sends a SIP Register message to the P-CSCF. The P-CSCF forwards the Register message to the appropriate S-CSCF (with the assistance of an I-CSCF as required) which contacts the HSS to obtain the user information necessary to complete the authentication. Using the information obtained from the HSS the S-CSCF responds to the UE (via the P-CSCF) with a challenge. If the UE responds correctly the UE will have successfully authenticated and a security association will have been established between the UE and P-CSCF. Additional message traffic including requests for service will now be allowed.

As mentioned above, the HSS contains profile information which includes both the subscriber's private and public identities. The private identity along with a long term shared secret is used to authenticate the user to the network. It is the responsibility of the HSS to maintain the shared secret key information necessary to secure communications between the UE, the P-CSCF, and the S-CSCF.

In a cable environment some devices may use a UICC based application for authentication (e.g. a GMS phone requesting access via a cellular network) while others may not (e.g. streaming audio or video to a PC). Extensions to define authentication mechanisms that provide support for non-

UICC devices will likely be addressed by PacketCable 2.0.

IMS makes use of the concept of private and public identities. The private identity is typically assigned by the home network at the beginning of the subscription process. It is permanent and persists for the entire duration of the user's subscription with the service provider. The public identity is used by the subscriber to request services and/or communication with other users. There is typically only one private identity associated with a UE although there may be many public identities.

The one-to-one relationship of private identity and UE can be problematic. It is certainly possible to envision a single user owning multiple UE's with different capabilities (e.g. cell phone with multimedia capabilities and a PC). Difficulties also arise in the instance where a single UE requires multiple security credentials for accessing services via different access mechanisms. As in the earlier example it is certainly within the realm of possibility that an operator will wish to offer a service that allows customers to move seamlessly between a cellular network and a wireless (e.g. WiFi) network in a home environment. In this case the UE would require simultaneous security associations with both the P-CSCF that resides in the cellular operator's home network and the P-CSCF that resides in the MSO network.

POLICY DECISION FUNCTION (PDF)

Quality of Service (QoS)

In the IMS specification QoS within the core and services layers are handled with traditional IP bandwidth reservation or packet tagging methods.[4] Bandwidth reservation is accomplished via the Resource reSerVation Protocol (RSVP)[5] Integrated Services (IntServ)[6]. Packet tagging is accomplished via Differentiated Services (Diffserv)[7] or Multi-Protocol Label Switching (MPLS)[8].

In the HFC portion of the access network QoS will likely be provided as specified by PacketCable Multi-media (PCMM) with some modifications. In PCMM the application requesting service communicates directly with the Application Manager (AM). It is the AM that communicates with the Policy Server (PS). The PS, in turn, communicates with the policy enforcement point (PEP) which, in the HFC, network is the CMTS.

In an IMS implementation the application requiring QoS would first communicate that request to the P-CSCF. The P-CSCF would then forward the request to the AM which would determine the resources required for that service request. The AM would then generate a PacketCable Multimedia request which is forwarded to the PS. The PS will verify that the resource requests are within acceptable limits as set by the operator.[9] The PS will then act as a proxy with respect to the application manager and the PEP by forwarding policy requests and returning responses.

The ability of the access network to support a dynamic level of QoS is especially important in an IMS network. One of the most interesting features of the Session Initiation Protocol (SIP), which is the backbone of the IMS signaling network, is the ability to dynamically add and/or modify service flows. From a services perspective this means that the operator can offer a greater range of services than are possible today. For example, most early implementations of VoIP support some sort of multi-party calling (typically 3-way calling). Currently, 3-way calling functionality is an application that must be written for specific vendor hardware. In a SIP environment, additional call legs can be added to a media stream simply by making additional requests for resources. Also, there is no particular reason why a subscriber should be limited to only 3-way calling (except as dictated by business rules). With SIP a caller could conference 4, 5, or more other callers just as easily.[10] Similarly, a user may initiate a session as voice only and switch at some point to voice with video or vice versa.

SERVICE MONITORING

Another area of growing importance in the delivery of IP services via the IMS network is the ability of the operator to translate measured network performance into an understanding of service performance. Many content owners are now including some reference to service monitoring in their contractual agreements. Content providers want to be able to ensure not only that content was played out to a subscriber as specified but also that the quality of the user experience was acceptable. In an IP environment effective service monitoring will require changes to the network and changes to the monitoring process.

Release 6 of the IMS specifications includes support for Real-Time Transport Control Protocol (RTCP)[11] as the mechanism for monitoring audio service quality in the access network. RTCP provides feedback about specific session performance including measurements of packet loss, inter-arrival jitter, and delay or latency. These parameters can be translated directly to audio quality for example when judging the quality of a VoIP call. Additional audio monitoring information is available via the RTCP Extended Reports (RTCP-XR)[12] standard.

There are as yet no specified standards for monitoring video quality.

CONCLUSION

IMS is potentially very important to the cable industry. Depending on implementation details it may provide a powerful new means for rapid deployment of new services. It is also likely to be the mechanism by which the primary competitor (telco's) will deploy new services including IPTV.

Although there seems to be general agreement on the high level standards there is some disagreement on implementation details. One vendor may emphasize a specific component while another describes additional components or lacks some entirely. It is vital that the industry remain focused on creating cable specific standards to allow truly uniform multi-vendor compatibility if IMS is to reach it's full potential.

REFERENCES

1. Java Specification Requests (2005) JSR 281: "IMS Services API"

2. 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security"

3. 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-Based services"

4. 3GPP TS 23.207: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; End-to-end Quality of Service (QoS) concept and architecture (Release 6)"

5. IETF RFC 2205 (1997), "Resource ReSerVation Protocol (RSVP)"

6. IETF RFC 2210 (1997), "The Use of RSVP with IETF Integrated Services"

7. IETF RFC 2474 (1998), "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers"

8. IETF RFC 2702 (1999), "Requirements for Traffic Engineering Over MPLS"

9. PKT-TR-MM-ARCH-V02-051221, "PacketCable™ Technical Report Multimedia Architecture Framework"

10. IETF RFC 4353 (2006), "A Framework for Conferencing with the Session Initiation Protocol (SIP)"

11. IETF RFC 3550 (2003), "RTP: A Transport Protocol for Real-Time Applications"

12. IETF RFC 3611(2003), "RTP Control Protocol Extended Reports (RTCP XR)"