AN OVERVIEW OF INTERNET PROTOCOL MULTIMEDIA SUBSYSTEMS (IMS) ARCHITECTURE

Jhansi Jujjuru*
Graduate Student, M.S. in Computer Science Program, Rivier College

Keywords: IMS Architecture, Application Servers in IMS, IMS Protocols

Abstract

Internet Protocol Multimedia Subsystems (IMS) is an internationally standardized Next Generation Networking (NGN) architecture for telecom operators in order to provide mobile and fixed multimedia services. It uses Voice-over-IP (VoIP) implementation based on a 3GPP-standardised implementation of Session Initiation Protocol (SIP), and runs over the standard Internet Protocol (IP). It also specifies interoperability and roaming, and provides bearer control, charging and security.

IMS is well integrated with existing voice and data networks, while adopting many of the key characteristics of the IT domain. This makes IMS a key enabler for fixed-mobile Convergence and value-based charging. IMS also supports existing Packet-Switched and Circuit–Switched phone systems.

1. Introduction

Recently, web based multimedia services have gained popularity and have proven themselves to be viable of communication. This has inspired the telecommunication service providers and network operators to reinvent themselves to try and provide value added IP centric services. There was a need for a system, which would allow new services to be introduced rapidly with reduced capital expense (CAPEX) and operational expense (OPEX) through increased efficiency in network utilization.

Various organizations and standardization agencies have been working together to establish such a system. Internet Protocol Multimedia Subsystem (IMS) is a result of these efforts. IMS is an application level system. It is being developed by 3GPP (3rd Generation Partnership Project) and 3GPP2 (3rd Generation Partnership Project 2) in collaboration with IETF (Internet Engineering Task Force), ITU-T (International Telecommunication Union–Telecommunication Standardization Sector), and ESTI (European Telecommunications Standards Institute) etc. Initially, the main aim of IMS was to bring together the internet and cellular world, but it has extended to include traditional wire line telecommunication systems as well. It utilizes existing internet protocols such as SIP (Session Initiation Protocol), AAA (Authentication, Authorization and Accounting protocol), and COPS (Common Open Policy Service) etc, and modifies them to meet the stringent requirements of reliable, real time communication systems. The advantages of IMS include easy service quality management (QoS), mobility management, service control and integration.

The aim of the report is to provide a brief overview of the IMS architecture. The essential requirement for IMS architecture to combine the worlds of internet and cellular technologies is initially discussed. Later the various nodes/servers that form the core network subsystem of IMS architecture is described in detail. The specific protocols involved in the communication between the nodes are briefly explained. A brief description of methods and systems for identification of users in the IMS environment is given.
2. IMS Architecture

2.1 General Description

The IP Multimedia Subsystem (IMS) is a standardized Next Generation Networking (NGN) architecture for telecom operators that want to provide mobile and fixed multimedia services. It uses Voice-over-IP (VoIP) implementation based on a 3GPP-standardised implementation of SIP (Session Initiation Protocol), and runs over the standard Internet Protocol (IP). Existing phone systems (both Packet-Switched and Circuit-Switched) are supported.

IMS is being developed and standardized for years now and the standardization process is not simple by any means. It involves a number of agencies and organizations. IMS architecture forms the basis for the development of NGN systems.

2.2 IP Multimedia Subsystem (IMS) Requirements

It is clear that there is shift from the traditional Circuit Switched (CS) to Packet Switched (PS) environment for the delivery of multimedia services. IMS was developed for this very purpose by the cellular industry. The objective was to bring the internet and the cellular worlds closer and to utilize the existing packet based services being provided on the internet, which would increase profits.

The IMS comprises a CORE Network (CN), which is a collection of signaling, and bearer related network elements. These CN elements operate collectively to provide multimedia services to the end user. The IP multimedia services are based on the IETF defined standards for session control and bearer control. The IMS terminal connects to CN via an IP-Connectivity Access Network (IP-CAN), which functions merely as a means to transport IP data. This allows IMS to achieve Access independence, as defined in 3GPP TS 22.228 V7.20 [1].

The ability for the subscribers to access their Multimedia services over any access network capable of providing IP-connectivity, e.g., via the following means:

- 3GPP (UTRAN, GERAN)
- Non-3GPP accesses with specified interworking (e.g. WLAN with 3GPP interworking)
- Other non-3GPP accesses that are not within the current scope of 3GPP (e.g. xDSL, PSTN, satellite, WLAN without 3GPP interworking). A few other important definitions are provided in Ref. [1] and are given below.

**IM CN subsystem:**
IP Multimedia CN subsystem comprises all CN elements for the provision of IP multimedia applications over IP multimedia sessions.

**IP multimedia application:**
An application that handles one or more media simultaneously such as speech, audio, video and data (e.g. chat text, shared white board) in a synchronized way from the user’s point of view. A multimedia application may involve multiple parties, multiple connections, and the addition or deletion of resources within a single IP multimedia session. A user may invoke concurrent IP multimedia applications in an IP multimedia sessions.
IP multimedia service:
An IP multimedia service is the user experience provided by one or more IP multimedia applications.

IP multimedia session:
An IP multimedia session is a set of multimedia senders and receivers and the data streams flowing from senders to receivers. IP multimedia sessions are supported by the IP multimedia CN Subsystem and are enabled by IP connectivity bearers (e.g., GPRS as a bearer). A user may invoke concurrent IP multimedia sessions.

2.2.1 Support to establish IP Multimedia Sessions
IMS can provide the users with a variety of services but the most basic and most important service is audio and video communication. The IMS architecture allows the users to invoke multimedia sessions in a controlled and a flexible manner. It allows for usage of a large variety of media types and ensures interpretability. The IP multimedia session is designed to support one or more multimedia applications. The IMS system also ensures that there is no compromise or reduction in privacy, security, or authentication as compared with traditional systems.

2.2.2 Support for QoS (Quality of Service) negotiation and assurance
One of the main problems with internet-based multimedia services is the lack of QoS. The IMS provides support for QoS negotiation for IP multimedia sessions, both at the time of establishment and during the session by the user and the operator. Same applies for individual media components. It also ensures end-to-end QoS for voice at least as good as that achieved by the circuit switched wireless systems (AMR based).

2.2.3 Support of interworking with the internet and CS domain
Support of interworking with the internet domain is most important and in a way obvious. The IMS users will be able to access information, services and applications available through the internet. Their connectivity will provide a tremendous increase in the number of potential sources and destinations for multimedia sessions. The IMS users will have the ability to establish IP multimedia session with non IMS users from the internet and the existing circuit switched systems including PSTN and cellular networks.

2.2.4 Support for roaming
Roaming has been a requirement of cellular systems for some time now; IMS will allow users to roam between different service provider’s networks. There are established procedures to transfer signaling, authentication, authorization, accounting, and other service related information between different IMS operations in a standardized and secure fashion.

2.2.5 Support for Service delivery control by the operator
The system requires strict control in terms of service delivery options. The operator will have control over all the services being offered to the users; these policies for control of user services have been classified into two categories:
1. General policies would be implemented throughout the network and would apply to all users; these restrictions might include control over the type of coded permitted for audio or video information. The purpose of such restrictions might be to monitor and control the bandwidth requirements in the network.

2. Individual policies on the other hand would apply to a particular user; they are configured specifically for each user depending on the subscription. The operator will have the ability to prevent an IP multimedia session for launching if the user is not authorized to use a type of media, for example video services.

2.2.6 Support for non standardized rapid service creation

The design of the IMS architecture has been influenced very strongly by this requirement. According to this requirement the IMS services do not need to be standardized. IMS would provide the necessary support for developing such services, or it would provide the necessary service enablers. This allows the service providers or application developers to economically and rapidly develop and deploy services, which would work equally well in different IMS networks. This is a radical change from the previous model of operation in the cellular field where almost all the applications were proprietary and did not always work in visiting networks (while roaming).

IMS has been able to successfully reduce the time and effort for developing a new service or application, by standardizing the service capabilities instead of the services.

2.3 Description of Core Network (CN) Subsystem Architecture: Nodes and their functions

Before describing the IMS architecture, it is important to remember that IMS does not standardize a network element, but the functionality provided by the element. The manufacturer is free to decide about the physical design of the functional unit; two or more may be combined if deemed necessary. On the same lines, IMS does not standardize services but the service enablers.

The core network elements or nodes are shown in Fig.1 below. These nodes communicate with each other using specific protocols; each of these interfaces is identified using a reference point label as shown in Fig.1. A detailed list of all the interfaces and their operation is available in 3GP TS 23.002 [2].

Also another important characteristic of the IMS architecture is that it exclusively uses IPv6; it requires network elements such as NAT-PT (Network Address Translation – Protocol Translation) and IMS-ALG (IMS Application Level Gateway) to interoperate with the traditional internet, which mostly uses IPv4). Presented below is a brief description of the nodes and their role in the IMS environment.

2.3.1 IMS Nodes: Databases

IMS utilizes one or more databases. The Home Subscriber Server (HSS) is used to store all the user related information, which is required to establish and handle multimedia sessions. The user information may include items such as the user profile (including the services the user subscribes to), location information, security information, the allotted SCSCF address, etc. all the information is stored in a standard format and decisions are made by the HSS about the user sessions based on these items or user information. There could be more than one HSS, if the number of users is too high or for redundancy. In this case a Subscriber Location Function (SLF) is used to locate the HSS where the user information is stored.
The SLF is a very simple database, which maps the user’s address with an HSS, where all the user information is stored. Both the HSS and SLF use DIAMETER protocol defined in RFC 3588[3]. The DIAMETER protocol is the base protocol, there are specific applications developed for IMS to make the necessary decisions in the matters of authentication, authorization and accounting for a particular user.
2.3.2 Serving Call Session Control Function (S-CSCF)

The S-CSCF is a SIP (Session Information Protocol) based server and is one of the three types of Call Session Control Functions (CSCF). The S-CSCF is considered as the central node in the signaling plane. It is basically a SIP server but performs session control as well. It also maintains a session state as required by the network operator. Within a network there could be a number of S-CSCF’s with different functionality and used for different purposes. The main functions of the S-CSCF as defined in 3GPP TS 23.228 [4] are described below.

Registration related operations:
- It may perform the task of the Registrar as defined in RFC 3261 [5]. It accepts the registration requests from the users, verifies the request by downloading the authentication vectors from the HSS. DIAMETER protocol defined in RFC 3588 [3] is used for this purpose over the Cx interface.
- It downloads the user profile from the HSS, which contains the service profile or information about any application servers, which need to be included in the SIP procedures.
- The S-CSCF makes the information available to the location servers, thus linking a particular user to an S-CSCF for the duration of the registration.

Session related and session-unrelated flows:
- It controls the sessions for the registered users and might deny establishment of different sessions (IMS communication) on the basis of various conditions or clauses that bar such an activity for the particular user.
- The S-CSCF may behave as a proxy server as defined in RFC 3261 [5] or subsequent versions of the protocol. It may accept and service requests locally or forward them to the relevant node after translation and filtering the request.
- The S-CSCF has the ability to behave as a User Agent as defined in RFC 3261 [5]; it can terminate and generate SIP transactions independently.
- It can interact with different service platforms or application server over the ISC (IP Multimedia Subsystem Service Control) interface. This interface allows for the coordination and support of various services provided by the application servers.
- The S-CSCF provides the endpoints with different service related information such as notification, location of additional media resources, billing notification etc.
- The functionality can be classified into two types; services provided for the originating end point and for the destination end point. First we look at the services provided for the originating end point, which may include an originating user/User Equipment (UE) or an Application Server (AS).

Services provided for the originating end point:
- The S-CSCF obtains the address of the Interrogating CSCF (I-CSCF) of the destination user from the destination name. This is done in the case of the destination user being the customer of a different network. The S-CSCF forwards the request to the corresponding I-CSCF.
- If the destination user belongs to the same network S-CSCF forwards the SIP request or response to the allocated I-CSCF with in the network.
- The S-CSCF also forwards the SIP request/response to a SIP server that is not a part of the IMS (e.g., internet). This depends on the policies of the home network operator.
The S-CSCF forwards the SIP request or response to a Break out Gateway Control Function (BGCF) for routing calls or sessions to the PSTN of any other Circuit Switched Domain (e.g. traditional cellular providers).

If the incoming request is from an Application Server (AS), the S-CSCF will verify the request coming from the AS is an originating request and proceed accordingly. The S-CSCF will process and proceed even if the user on whose behalf the AS is acting is not registered and reflect in the charging information that AS initiated the session on behalf of the user.

Services for the destination endpoint (terminating user/UE):

- The S-CSCF will forward the SIO request or response to a specific Proxy CSCF (P-CSCF) as a part of the SIP terminating procedure to a home user within a home network or for a roaming user in a visited network.
- The S-CSCF will forward a SIP request or response to an I-CSCF as part of the SIP terminating procedure for a roaming user in a visited network, where the home network operator chooses to include the I-CSCF in the path.
- The S-CSCF will modify the SIP request as per directions for the HSS and the service control interactions, for routing the incoming session to the CS domain. This allows the user to receive the incoming session via the CS domain. It also forwards the SIP request or response to a BGCF for call routing to the PSTN or a CS domain.
- The SIP request might contain preferences for the characteristics of the destination endpoints; the S-CSCF performs preference and capability matching as specified in RFC 3312 [6].

Charging the resource utilization management monitoring:

- Like all the other nodes of IMS, the S-CSCF is a part of the complicated charging or accounting procedure. It generates Charging Data Records (CDR) for this purpose. The S-CSCF is always located in the home network, and there are usually a number of S-CSCFs in a network for the sake of scalability and redundancy. Each of them can serve a number of IMS terminals at the same time.

2.3.3 Proxy-Call Session Control Function (P-CSCF)

As shown in Fig.1, the P-CSCF is the first contact between the user and the IMS network in the signaling plane. All the signaling and control information passes through the P-CSCF before getting to the user. It acts an outbound/inbound SIP proxy server. The discovery of the address of the P-CSCF and its allotment to the user is performed during the process of IMS registration and this does not change of the duration of the registration. The various functions performed by the P-CSCF are described below:

- The P-CSCF establishes a security association between itself and the IMS terminal. The security association requirements and procedures are provided in 3GPP TS 33.203 [7]. The IPsec security associations provide integrity protection. The P-CSCF also authenticates the user and asserts the identity with rest of the nodes in the network, to avoid redundant authentication requirement.
- The P-CSCF forward the SIP register request from the UE to the appropriate I-CSCF determined from the home domain name provided by the user. This allows for the successful IMS registration of the user/UE.
The P-CSCF forwards the SIP request or response to and from the UE to the allotted SIP server, which could be an S-CSCF. The address of the S-CSCF would have been obtained by the P-CSCF as a result of the registration process.

The P-CSCF performs SIP message compression/decompression for the purpose of reducing the size of the messages and thus reducing the transmission time and quicker session establishment.

The P-CSCF may also include a Policy Decision Function (PDF). It performs the task of authorizing the bearer resources and performing QoS management over the media plane. The PDF may or may not be included in the same physical unit.

Like the S-CSCF, P-CSCF also generates the CDR and forwards the information to the charging collection node. Details about this function of the P-CSCF are provided in 3GPP TS 23.207 [8].

An IMS network may have multiple P-CSCF for scalability and redundancy. The P-CSCF may be located in the home network or in a visited network.

### 2.3.4 Interrogating – Call Session Control Function (I-CSCF)

I-CSCF is SIP proxy server; it is placed at the edge of the administrative domain of an IMS network. It is a point of contact for a connection destined to the user who belongs to that network, or a roaming user currently located within the service area of that network operator. The address of the I-CSCF is listed in the DNS (Domain Name System) database and is made available when a SIP server follows the protocol for locating a SIP server for the next hop the protocol is provided in RFC 3263 [9]. The functions performed by the I-CSCF are described below:

- During the registration process the I-CSCF assigns a S-CSCF for a particular user. I-CSCF communicates with the HSS and SLF just like the S-CSCF over the Cx and Dx reference points. It uses the DIAMETER protocol. The user information is received by the I-CSCF and depending on the requirement; it assigns a S-CSCF to the user if one is not already allocated.
- I-CSCF routes a SIP request from another network to the S-CSCF after obtaining the address of the appropriate S-CSCF from the HSS.
- I-CSCF may encrypt certain parts of the SIP message, which may contain sensitive information about the home domain; this functionality is optional and is called THIG (Topology Hiding Inter-network Gateway).
- Like other CSCFs, the I-CSCF also generates CDRs to be transmitted to the charging collection node.

### 2.3.5 Application Servers

An application server provides value added services and can be located in the home network or any third party network. It is essentially a SIP server which hosts and executes various services. There are different modes of operation for an Application Server. It can be operated in SIP proxy mode, SIP User Agent mode (termination or origination), SIP Back – to Back User Agent (B2BUA) mode etc.

The S-CSCF interfaces with the AS through the ISC (IP Multimedia Service Control) interface. The ISC interface is based on SIP [5]. Fig.2 shows three different types of Application Servers, which are described below:
**SIP AS:** The SIP Application Server (SIP AS) is the native AS. It hosts and executes IP multimedia services based on SIP. All the new services that are going to be developed for the IMS architecture would be implemented using the SIP AS.

**OSA-SCS:** The Open Source Access-Service Capability Server (OSA-SCS) provides an interface to the OSA framework applications. An AS located at a third party location will not be able to securely connect with the IMS network, whereas OSA has the capability to establish a secure connection with the IMS network. The OSA-SCS inherits all the abilities of OSA and is used to provide secure connectivity for a remotely located AS to the IMS network. The OSA-SCS acts as a regular AS and interfaces with S-CSCF via SIP on one end and as an OSA AS using OSA Application Programming Interface (API) on the other end. The OSA API is described in 3GPP TS 29.198 [10].

**IM-SSF:** The IP multimedia service switching function is a specialized application server, which allow for integration and reuse of the traditional applications developed for the GSM architecture. CAMEL (Customized Applications for Mobile network Enhanced Logic) was the name of the services that were developed to provide multimedia or enhanced services for GSM handsets. The IM-SSF (IP Multimedia Service Switching Function) acts as an application server on one side interfacing with the S-CSCF using SIP, and on the other side it acts as a Service Switching Function (SCF) interfacing with the gsmSCF with a protocol based on CAP (CAMEL Application Part). The CAP protocol is defined in 3GPP TS 29.278 [11].

---

**Fig.2:** Types of Application Servers in IMS
The three AS mentioned above may perform different tasks but they behave exactly the same towards the IMS network.

The Application Servers present in the home network may optionally interface with the HSS. The SIP AS and the OSA-SCS interface with the HSS using DIAMETER protocol [3] and the interface is labeled ‘Sh’. The IM-SSF interfaces with the HSS using protocol based on MAP (Mobile Application Part) defined in 3GPP TS 29.002 [12].

2.3.6 Breakout Gateway Control Function (BGCF)

As shown in Fig.1, the BGCF provides connectivity to the Circuit Switched domain through the MGCF (Media Gateway Control Function), SGW (Signaling Gateway) and the MGW (Media Gateway). These three nodes put together are referred to as the PSTN/CS Gateway.

The BGCF is basically a SIP server, which has the additional capability of routing, and establishing sessions based on telephone numbers as user addresses. The BGCF is used exclusively for sessions initiated by an IMS user who needs to communicate with a user in PSTN or PLMN (Public Land Mobile Network) domain, both of which are in the Circuit Switched domain. The main functions performed by the BGCF are the following:

- It receives a request from the S-CSCF to select the appropriate PSTN/CS Domain break out point for a particular session.
- The BGCF selects the network in which the internetworking with the PSTN/CS Domain is to occur. If the interworking with PSTN/CS domain is to occur in the same domain, it selects the appropriate MGCF and forwards the SIP signaling to it.
- If the internetworking with the PSTN/CS domain is to be done at a different network, the BGCF forwards the SIP information to the BGCF of that network. If network hiding is required, the BGCF will forward the SIP signaling through the I-CSCF to the other BGCF.
- The BGCF also generates CDRs to forward to the charging collecting node.

2.3.7 Public Switched Telephone Network/Circuit Switched (PSTN/CS) Gateway

The PSTN/CS gateway comprises of three components as mentioned earlier. The functions performed by each of them are described below:

- **MGCF (Media Gateway Control Function):** The MGCF interfaces with the BGCF and receives the SIP signaling. Its function is to convert the SIP signaling to either ISUP (Signaling System 7) defined in ITU-T recommendation Q.761 [13] over IP or BICC (Bearer Independent Call Control) defined in ITU-T recommendation Q.1901 [14]. The converted signaling is forwarded to the Signaling Gateway (SGW). The MGCF also control the resources in the Media Gateway (MGW). The MGCF and the MGW communicate with the help of the H.248 protocol, specified in the ITU-T recommendation H.248 [15] (this protocol has been revised a number of times and annexes have been added to the main body).
- **SGW (Signaling Gateway):** The SGW provides the signaling interface with the circuit switched domain. Its main function is to perform lower level protocol conversion. It converts MTP (Message Transfer Part) defined in ITU-T recommendation Q. 701 [16] into SCTP (Stream Control Transmission Protocol) defined in RFC 2960 [17] over IP.
**GW (Media Gateway):** The GW connects the media plane of the PSTN or any other CS environment with the media plane of IMS. The MGW transcodes the IMS data transported over RTP (Real Time Protocol) defined in RFC 3550 [18] into PCM (Pulse Code Modulation) used in the PSTN environment. Also the MGW performs transcoding in situations where the IMS terminal does not support the codec being used by the CS side.

**2.3.8 Media Resource Function (MRF)**

The MRF handles all the media transportation and processing requirements. It is divided into two functional components as shown in Fig.1, the Media Resource Function Controller (MRFC) and Media Resource Function Processor (MRFP).

The MRFC interfaces with the S-CSCF over Mr Interface and uses SIP [5] for signaling purposes. The tasks performed by the MRFC are described below:

- It controls the media stream resources in the MRFP.
- The MRFC interprets the information forwarded by the S-CSCF and the Application servers and modifies the operation of the MRFP according to the directions.
- The MRFC generates CDRs like the other nodes in IMS to be forwarded to the charging collecting node.

The MRFP is controlled by the MRFC through the Mp interface, also called a reference point. The Mp reference point does not have a specific protocol specified for it yet and has an open architecture to allow extension work to be carried out. It completely supports the H.248 standard [15]. The tasks performed by the MRFP are described below:

- The MRFP controls the bearer plane on the Mb reference point. It provides the functionality of mixing various incoming media streams in case of a conference call.
- It acts as a source of media streams or plays streams as for multimedia announcements.
- The MRFC performs all other media processing functions such as transcoding, media analysis, etc.
- It also provides floor control or manages access rights in a conference environment.

**2.4 IMS Protocols**

IMS uses internet-based protocols for performing various tasks and operations. This includes establishment of sessions, control, Authentication, Authorization and Accounting operations (AAA) etc. The task of the standardization bodies is to choose the appropriate protocol for a specific functionality, this may sound simple but its not. There are times when the existing protocols are not suitable or sufficiently powerful to support the IMS requirements. In such situations the standardization bodies need to work together to modify the existing protocols or develop an entirely new one. We know that the protocols used in the IMS environment are derived from the internet and wireless domain (GSM/GPRS). Mentioned below is a brief description of the various protocols selected or developed to be used in different area of IMS.
2.4.1 Session Control in IMS

The protocol used for session initiation and control in IMS over IP networks is the Session Initiated Protocol (SIP) specified by the IETF in RFC 3261 [5]. SIP is a text-based protocol unlike other session protocols such as BICC and H.323. This makes it easier to debug, extend, and build services on it. One of big reasons for choosing SIP was the fact that it is based on many familiar and successful protocols such as SMTP (Simple Mail Transfer Protocol) and HTTP (Hypertext Transfer Protocol). Also SIP follows the familiar client-server model. SIP makes it very easy to develop new applications, which is one of the requirements of IMS.

2.4.2 Authentication Authorization and Accounting (AAA) in IMS

AAA operations play a very important role in any network, especially in the IMS environment. It is of great importance to have an efficient and highly reliable mechanism to perform the tasks to authentication a user’s identity, authorizing the user to access the appropriate resources and making sure the resources and services consumed are logged accurately and billed correctly. IMS uses the DIAMETER protocol to perform the AAA operations. It allows different nodes to access retrieve or modify user information from HSS or SLF. The DIAMETER protocol is used over different interfaces, such as Cx, Dx and Sh. It consists of a bases protocol and is used to develop various DIAMETER applications.

2.4.3 Quality of Service in IMS

Generally, there are two models to provide QoS on the packet switched IP domain specifically the internet. They are the Integrated Service model and the Differentiated Service (DiffServ) model that are described below:

- **Integrated Service model** is defined in RFC 1633 [19]; it provides end-to-end QoS. The endpoints request a certain QoS and the network grants it. The protocol used by the Integrated Services architecture is RSVP (Resource reservation Protocol) it is specified in RFC 2205 [20] and has been updated by RFC 2750 [21] and RFC 3936 [22]. Integrated Service works well in small networks does not scale well as the routers have to store state information about every flow and perform lookup before routing any packet.

- **The DiffServ architecture** is specified in RFC 2475 [23] and RFC 3260 [24]. The DiffServ servers need to maintain minimum state information about the flow and enables a quicker treatment for the packets flowing through them. In this architecture the router is aware of the treatment that needs to be given to each packet; the treatment is referred to as the Per Hop Behavior (PHB). Each PHB is identified by 8-bit codes called Differentiated Service Code Points (DSCP). The packets in their IP headers carry the DSCP information. In IPv4 it is placed in the ‘Type of Service’ field and in IPv6 it is placed in the ‘Traffic Class’ field. IMS allows many different end-to-end QoS models.

2.4.4 Security in IMS

Security generally deals with integrity, confidentiality, and availability. There are various means to achieve the security requirements in the SIP environment. In IMS security can be divided in two different areas, Access security and Network security that are described below:
• Assess security deals with authentication and authorization processes and establishment of the IP security authorization (architecture defined in RFC 2401 [15]); these procedures are performed during the REGISTER transaction. All the procedures for security access are provided in 3GPP TS 33.203 [7]. In the 3GPP networks the user identity is stored on a smart card inserted in the IMS terminal; this card is usually known as UICC (Universal Integrated Circuit Card).

• Network security deals with protecting the traffic between two nodes. The nodes may or may not belong to the network. There may be different levels of requirements from the network security mechanism in place. If two different security domains are involved, the traffic travels through two Security Gateways (SEG). In this case the traffic is protected using IPsec ESP (Encapsulated Security Payload) specified in RFC 2406 [25] and runs in tuned mode. The security associations are established and maintained using IKE (Internet Key Exchange) specified in RFC 2409 [26]. All the network security requirements are mentioned in 3GPP TS 33.210 [27]. Recently newer versions of the internet security protocols have been introduced (December 2005) but they are not being used in the latest IMS release (Release 7).

2.4.5 Policy Control in IMS

Policy control deals with the media-level access control; the decisions made by the policy control mechanisms authorizes a user to use the media plane and assigns the QoS to be provided for that user session. The routers present in the network enforce the media-level policy, but these routers do not have the ability to make decisions about users, as they do not have access to the user information stored in the HSS.

A SIP server performs the task of obtaining the user information and making these decisions in this case. The SIP server informs the routers to allow or deny a certain user with the requested media resources. The node, which makes the decision, in this case, the SIP Server is called the Policy Decision Point (PDP) and the router is called the Policy Enforcement Point (PEP).

The protocol used between the PDP and PEP is called Common Open Policy Service (COPS) protocol; it is defined in RFC 2748 [28] and has been updated by RFC 4261 [29], which provides a higher level of security at the transport level. COPS generally support two models for policy control, the outsourcing model and the configuration model (also called provisioning).

In the outsourcing model the PEP contacts the PDP for every decision, whereas in the configuration model the PEP stores the policy from the PDP locally and uses it to make decisions. IMS uses a combination of the two models; it’s called COPS-PR. It’s a mixture of the two models as it uses the same message format and the Policy Information Bases (PIB) as used by the provisioning model and the policy decision are transferred in real time like in the outsourcing model. In IMS there are two types of limitations on the session that can be established. They are user-specific limitations and general network related policies:

• The user-specific limitations include restrictions on a particular user, in terms of resources that are allowed. An example would be an audio only subscription, so the user will not be allowed to establish video sessions.

• The general network policies would apply to all the users of that network. This might include restriction on the code’s that can be used.
The P-CSCF deals only with the enforcement of the general network policies, whereas the S-CSCF handles both user-specific policies and the network policies. Both these PDPs use the same mechanism to monitor the sessions. They access the SDP (Session description protocol) body to identify the type of session and media requested during SIP procedures.

2.4.6 Media Transport in IMS

There are a large number of codecs available to encode audio, video, and data. Ideally there should have been a common set of codecs, which would allow all kinds of terminals belonging to different networks to be able to communicate with each other without the need for any transcoders. But unfortunately 3GPP and 3GPP2 were not able to agree on a common codec and require transcoders to communicate between their IMS (MIMO in case of 3GPP2) terminals.

3GPP and 3GPP2 individually do specify the codecs, which will be supported by all their terminals. 3GPP terminals support AMR speech codec and the H.263 video code; details are provided in 3GPP TS 26.235 [30]. It also supports AMR-WB (AMR-Wide Band) for terminals providing wide band services and for real time text ITU-T recommended codec T.140 [31] is used.

In IMS unreliable media transport is provided by using Real Time Protocol (RTP) defined in RFV 3550 [25] over UDP (User Datagram Protocol). UDP is the unreliable transport protocol defined in RFC 0768 [32]. RTP is used in conjunction with RTCP (RTP Control Protocol), which allows quality of service information and allow for inter media synchronization. This is essential in case of an unreliable media transport as packets might arrive in random order and a few might even be lost or dropped. RTP provides mechanisms to overcome such problems. An alternative for providing unreliable transport is DCCP (Datagram Congestion Control Protocol). It’s a new protocol being developed by IETF, and it may be used in the future but is not mature enough to be implemented on a large scale.

For reliable transport of media there are two protocols that are most popular: TCP (Transmission Control Protocol) and SCTP (Stream Control Transmission Protocol). In case of IMS, TCP would be the natural choice for reliable media transport because of its proven track record and global acceptance.

2.5 Addressing and User Identification in IMS

Addressing and routing operation performed in the IMS environment are based on IPv6 architecture. The mechanism, which deals with these operations to provide access to IMS services and general IP address management are provided in 3GPP TS 23.221 [33]. In this section we will briefly describe the methods and systems for identification of users in the IMS environment. The need to identify a user distinctively is universal requirement for any network; the same is true in IMS. There are various identities associated with every user in the IMS architecture. The following sections identify and define the purpose of these identities.

2.5.1 Private user Identity

Each user is assigned a Private User Identity by the service provider. The purpose of the Private User Identity is for Authentication, Authorization, Accounting (AAA), and registration purposes and not for the routing or establishment sessions. The Private User Identities take the form of a Network Access Identifier (NAI) as defined RFC 4282 [34].
The format of a NAI is ‘username@operator.com’. The contents of the NAI for the private identity may include the IMSI (International Mobile Subscriber Identifier) in the case of GSM/GPRS/UMTS systems.

The purpose and utility of Private User Identified are described below:

- Private User Identity is to be included in all the registration requests passed from the user Equipment (UE) to the home network.
- The Private User Identity shall be securely stored on the ISIM (IMS SIM), and the user will not have the ability to modify it.
- The Private User Identity identifies the subscription and not the user; it is a globally unique identity defined by the home network operator.
- The Private User Identity is allocated to the user permanently for the domain of the subscription; it’s not a dynamic identity.

The Private User Identity is used to identify the user information for a particular subscriber at the HSS; also it may be present in the charging records depending on the operator policies. The private User Identity is authenticated only during registration of the user. The HSS stores the Private User Identity is also required by the S-CSCF upon registration and registration.

2.5.2 Public User Identities

Public User Identities unlike Private User Identities are used to identify the user, for requesting communications with other users, etc. The Public User Identities are assigned by the operator and each user will be usually assigned two or more Public User Identities. The Public User Identities will be either a SIP or URI (Uniform Resource Identifier), as defined in RFC 3261 [5] and RFC 3986 [1], or a TEL URI defined in the RFC 3966 [35].

A few functions, users and characteristics of the Public User Identities are described below:

- The public User Identities are used as contact information of a user and can be distributed to others, on a business card for example.
- Both numbering and internet names can be used for this purpose. The Public User Identity using a SIP URI will generally have the format of “sip:first.last@operator.com” and the one using a TEL URL will have the format, which includes a “+” sign followed by the complete number, an example is “tel:+1-292-234-2343”.
- The ISIM (IMS SIM) can store one or more Public User Identities, securely and the user will not have the ability to modify it.
- The option for multiple Public User Identities is to facilitate the distinction between identities for different purposes, for example one might be personal use, which is known by family and friends and another for work related contacts.
- IMS has a system that allows Public User Identities to be registered implicitly or explicitly. This procedure allows for a number of identities to be registered using just one register request, thus saving time and bandwidth. Also all the Public User Identities can be registered independently as well.
- The network does not authenticate public User Identities during registration, and they can be used to identify the user information stored in the HSS.
2.5.3 Relationship between Public and Private User Identities and Service Profiles

The IMS operator assigns the various Public User Identities to the user. These Public User Identities are linked to one or more Private User Identities. All the information about the user along with other service related information is stored in the HSS in the form of service profiles. The structure and functionality of a user service profile as stored on the HSS is provided in 3GPP TS 29.228 [36]. The service profile includes a list of Public User Identities and a number of initial filter criteria. These initial filter conditions provide basic information about the user/operator preferences and usually lead to the invocation of one or more Application Servers. Figure 3 (below) shows the relationship between the Public and Private User Identities along with the service profiles.

![Relationship between Public and Private User Identities](image)

**Fig.3: Relationship between Public and Private User Identities**

The scope of a Service Profile defined and maintained in the HSS is limited to the IMS environment. A Service Profile is downloaded by the S-CSCF from the HSS during registration, and only one service is associated with a Public User Identity.

As shown in Fig.3, a Public User Identity can be associated with only one Service Profile, but a Service Profile may be attached with one or more Public User Identities.

2.5.4 Public Service Identities

Public Service Identities (PSI) are used to define services that are hosted by different Application Servers (AS). The PSIs do not identify users, but they may identify groups. As example would be an application server hosting a chat group; it can be identified using a PSI. This PSI can be used to establish sessions and enable communication among the various subscribers of the service. A PSI can use the format of a SIP URI or a TEL URL as defined in the 13.5 of 3GPP TS 23.003 [37].

IMS allows for users to create, manage and use Public User Identities, running on an Application Server (AS). The creation of PSI can be done both statically and dynamically.

The Public Service Identities do not have an associated Private User Identity, as in the case of a Public User Identity. This is so because a PSI does not require authentication.
3. Conclusions

This report provided a brief overview of the IMS architecture. The requirements needed to bring the internet and a cellular world together is discussed. The core network subsystem architecture is described in detail that comprises of various nodes that communicate with each other using specific protocols. A brief description of methods and systems for identification of users in the IMS environment is given.

It was important to understand the process of IMS standardization to appreciate the scope of the system and its operation. The main purpose of developing this system is to be able to provide advanced, value added, IP based multimedia service, which are converged in nature or span multiple system. A few applications and services that have been developed include presence related services, instant messaging; push to talk services, etc. The services, which can be developed on the IMS platform, are limited only by the creativity of the application developers and requirements of the customer.

At present a lot of attention is being paid to providing bundled up services in the home environment. Services providers have been successful in providing traditional telephony, high speed internet and cable services in a single package. But there is very little integration among these services. IMS can provide a way to integrate them as well as extend the possibility of various other services to be added to increased automation in the home environment.

References


AN OVERVIEW OF INTERNET PROTOCOL MULTIMEDIA SUBSYSTEMS (IMS) ARCHITECTURE


Glossary

3GPP: 3rd Generation Partnership Project
3GPP2: 3rd Generation Partnership Project 2
AAA: Authentication Authorization and Accounting protocol
AMR: Adaptive Multi Rate
AMRWB: AMR-Wide Band
API: Application Programming Interface
AS: Application Server
B2BUA: SIP Back-to-Back User Agent
BGGF: Breakout Gateway Control Function
BICC: Bearer Independent Call Control
CAMEL: Customized Applications for Mobile network Enhanced Logic
CAP: Camel Application Part
CAPEX: Capital Expense
CDR: Charging Data Records
COPS: Common Open Policy Service
CS: Circuit Switched
DCCP: Datagram Congestion Control Protocol
DNS: Domain Name Service
DSCP: Differentiated Service Code Points
ESP: Encapsulated Service Payload
ESTI: European Telecommunications Standards Institute
GPRS: General Packet Radio Service
GSM: Global System for Mobile communications
HSS: Home Subscriber Server
HTTP: Hypertext Transfer Protocol
I-CSCF: Interrogating CSCF
IETF: Internet Engineering Task Force
IKE: Internet Key Exchange
IMS-ALG: IMS Application Level Gateway
IMSI: International Mobile Subscriber Identifier
IM-SSF: IP Multimedia Service Switching Function
IP: Internet Protocol
ISC: IP Multimedia Subsystem Service Control
ITU-T: International Telecommunication Union – Telecommunication Standardization Sector
MGCF: Media Gateway Control Function
MGW: Media Gateway
MIMO: Multiple-Input Multiple-Output
MRFC: Media Resource Function Controller
MRFP: Media Resource Function Processor
MTP: Message Transfer Part
NAI: Network Access Identifier
NAT-PT: Network Address Translation – Protocol Translation
NGN: Next Generation Network
Jhansi Jujjuru

OPEX: Operational expense
OSA-SCS: Open Source Access-Service Capability Server
PCM: Pulse Code Modulation
P-CSCF: Proxy CSCF
PDP: Packet Data Protocol
PDP: Policy Decision Point
PEP: Policy Enforcement Point
PHB: Per Hop Behavior
PIB: Policy Information Bases
PLMN: Public Land Mobile Network
PS: Packet Switched
PSTN: Public Switched Telephone Network
RSVP: Resource reSerVation Protocol
RTP: Real Time Protocol
S-CSCF: Serving Call Session Control Function
SCTP: Stream Control Transmission Protocol
SDP: Session Description Protocol
SEG: Security Gateways
SGW: Signaling Gateway
SIP: Session Initiation Protocol
SLF: subscriber Location Protocol
SMTP: Simple Mail Transfer Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
UE: User Equipment
UICC: Universal Integrated Circuit Card
UMTS: Universal Mobile Telecommunication System
URI: Uniform Resource Identifier

* JHANSI JUJJURU has come to the United States from Andhra Pradesh, India. She received her Bachelor of Technology degree in Computer Science in 2005. She is currently pursuing Master of Science degree in Computer Science at Rivier College.