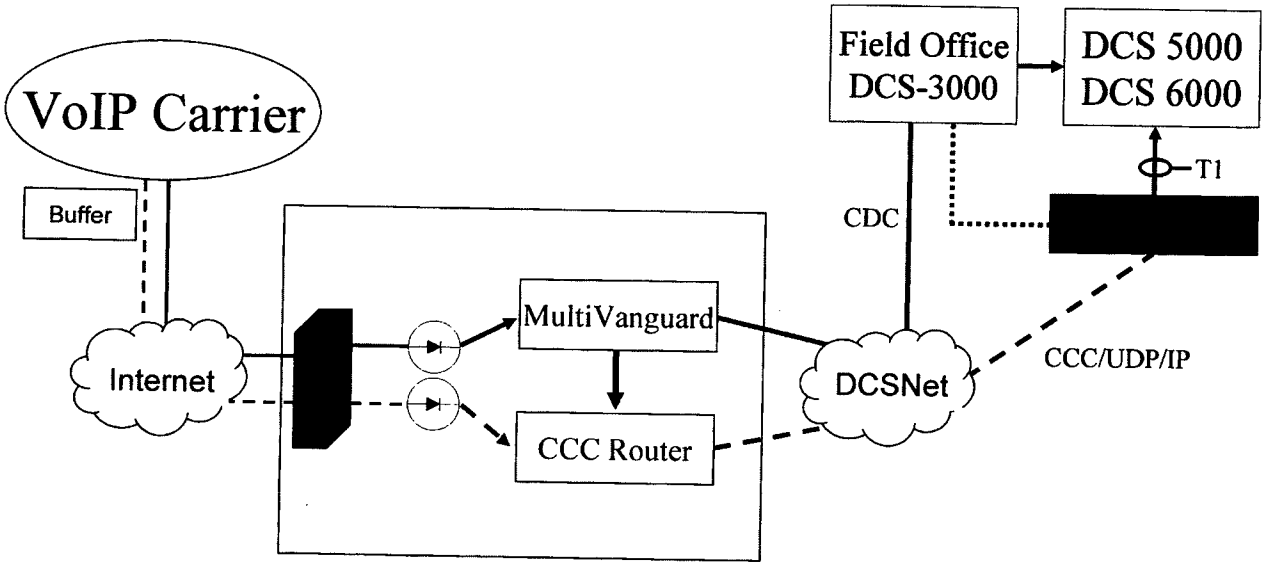
OTD Briefing on: Voice over IP (VoIP)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-02-2008 BY 60322/UCLRP/PJ/EHL

VoIP


VoIP Carrier
Buffer
Internet
MultiVanguard
CCC Router
Field Office
DCS-3000
DCS 5000
DCS 6000
T1
CDC
DCSNet
CCC/UDP/IP

Voice over IP (VoIP)

- What is it?
  - Technology used to transmit voice conversations over data networks
- Importance
  - Extremely cost effective for providers
  - Will eventually replace traditional PSTN telecommunications
- Types of VoIP
  - Carrier Grade – Quality ensured
  - Peer-to-Peer – No intermediary provider

Managed Carrier VoIP Experience

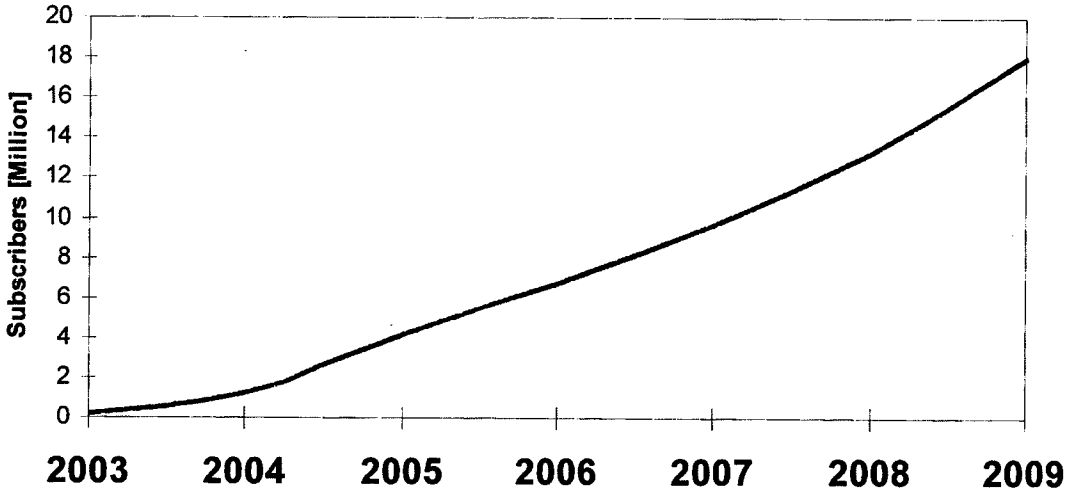
- **Some VoIP carriers have already embraced CALEA and have intercept solutions available**

[redacted] b2 b7E

- **The solutions deployed by these carriers have forced FBI/OTD to develop a new access model:**
  - [redacted] **over the Internet** b2 b7E

VoIP

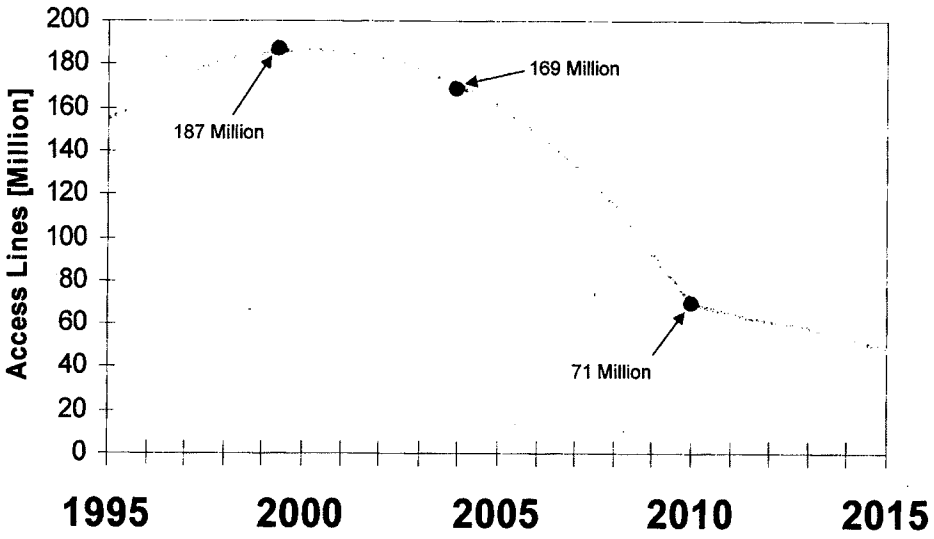
Managed U.S. Residential VoIP Subscribers



Source: Telecommunications Industry Association

VoIP

ILEC Narrowband Access Lines



Source: Technology Futures, Inc.

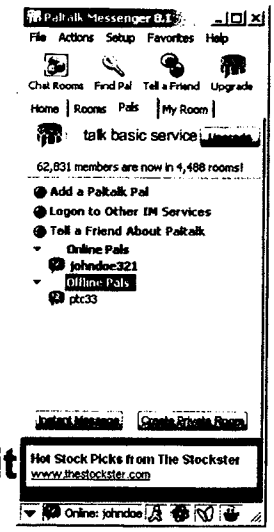
VoIP

Two Categories of VoIP

- **Managed**
  - **"Pay for" services**
    - **AT&T**
    - **Verizon**
    - **Vonage**
- **Unmanaged**
  - **"Peer-to-Peer" services**
    - **Skype**
    - **Paltalk**
    - **Google Talk**

Unmanaged Software VoIP Technologies

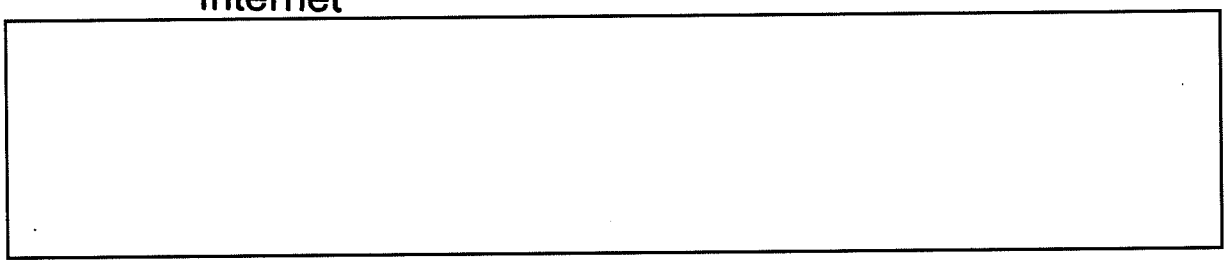
- **Computer Internet Applications**
  - Yahoo! Messenger, MSN Messenger, Paltalk, AOL Instant Messenger and Google Talk all utilize VoIP to allow computer-to-computer conversations



- **Utilizes free software installed on a computer and a microphone to transmit voice to another PC**

Encryption Example

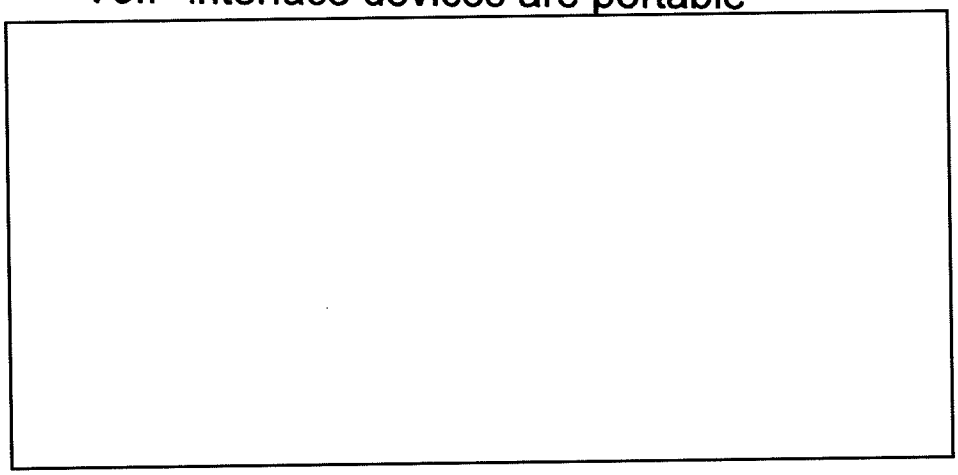
- A company wants inexpensive telephone service between offices in NY and LA
- They set up a secure VPN connecting the offices over the Internet



b2
b7E

Mobility of VoIP devices

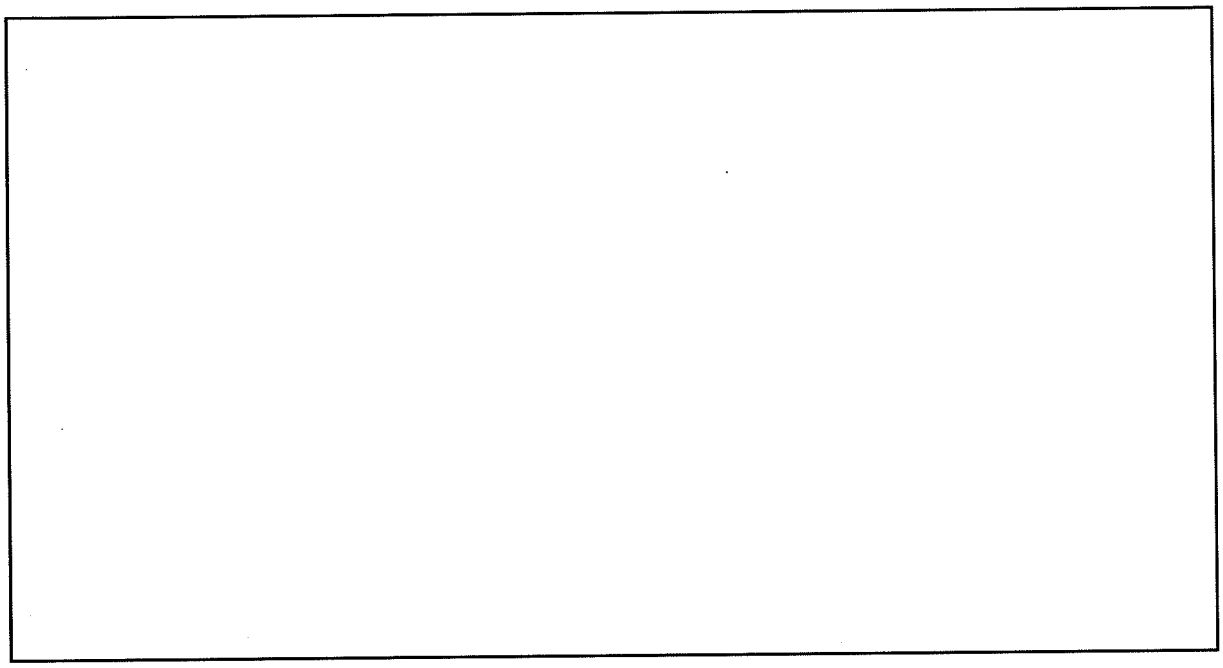
- VoIP interface devices are portable



b2
b7E

Technical Challenges

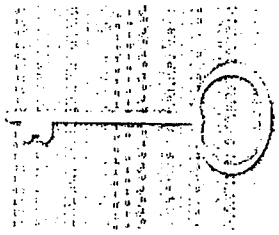
Mobility Example



b2
b7E

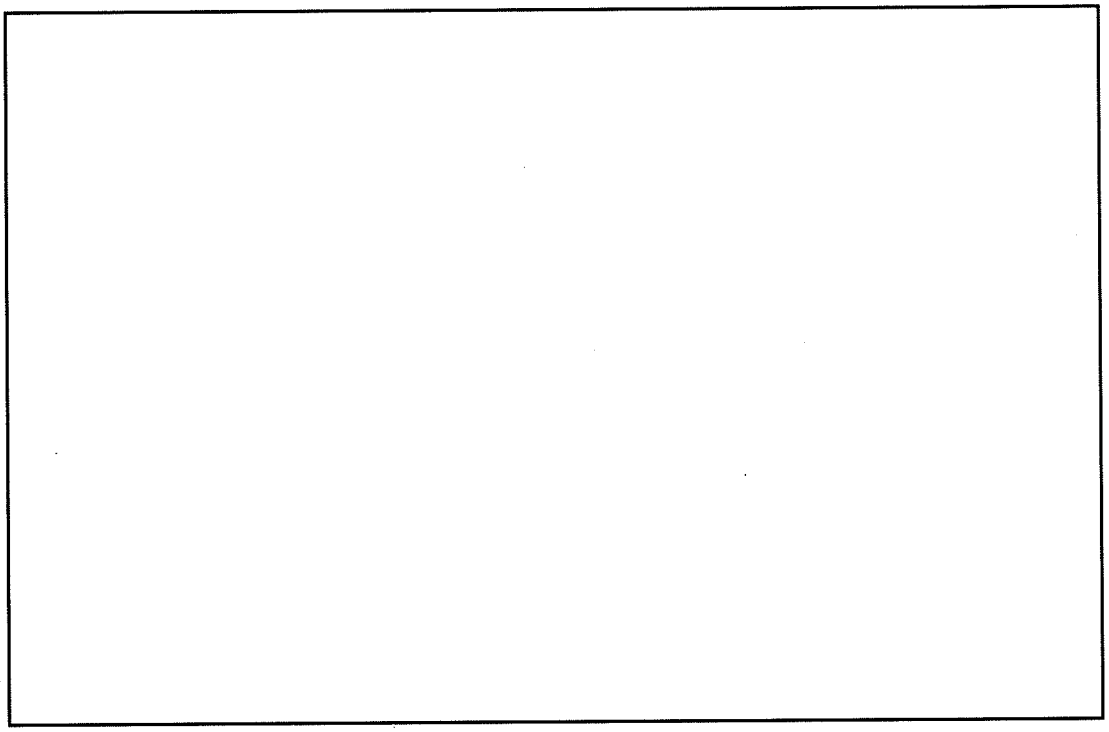
Technical Challenges

Encryption



- VPN connection between offices creates a secure private telephone system
- VoIP command messages can be easily encrypted
- Skype, Gizmo and other VoIP service providers offer secure encrypted voice service for a global market

VoIP Challenges



b2
b7E

VOICE OVER IP

b2
b7E

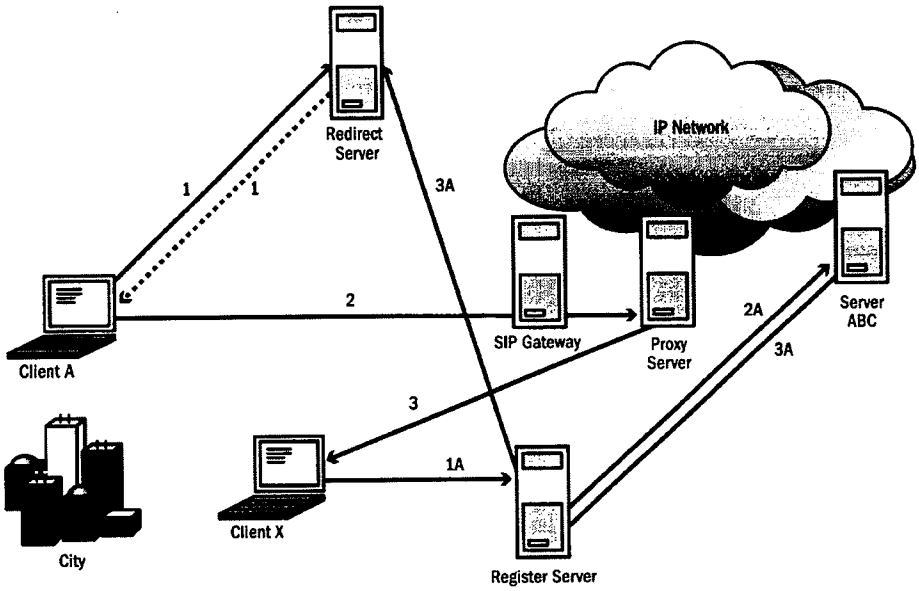


Figure 5.1. SIP Network Diagram

5. A meta buddy is an individual within a buddy list that has multiple service provider access points. Creating a meta buddy list involves locating all the service providers that the individual is registered to utilize.

8. IP MULTIMEDIA SUBSYSTEMS (IMS)

INTERNET TELEPHONY

INTRODUCTION

IP Multimedia Subsystem (IMS) Internet telephony—sometimes referred to as Multimedia Domain (MMD) telephony—is a 3GPP,[1] 3GPP2,[2] and Parlay Forum[3] effort to define an all-IP-based wireless network (see Figure 8.1), in contrast to disparate legacy voice, data, and control networks and their operations, administration, maintenance and provisioning support infrastructures. The important advantage of IMS is that it is independent of the underlying access technology, such as the 3G Radio Controller (RNC). Most service providers are adopting IMS as the de facto convergence model for fixed, mobile, and enterprise telephony. IMS includes support for management of user registration and mobility. The major IMS architectural components and functionality of IMS are well defined by standards and already are under product development by many of the major telecommunications equipment suppliers.

Internet telephony and multimedia communications services, supported by companies such as Microsoft, Yahoo!, AOL, and Skype, have devised proprietary architectures to compete with incumbent service providers. The IMS architecture enables incumbent service providers to avoid becoming low-margin "bit pipe" providers and to leverage their existing access networks and customer bases. IMS is optimized for the Internet, with no constraints from legacy telephony systems. It enables service providers to focus on user services rather than simply on transport. Moreover, under IMS service providers are not hindered by past commitments to Time Division Multiplex (TDM) networks.

IMS has no switches; there are no circuits to switch. Telephony is just another Internet application, similar to e-mail, file transfer, video streaming, and many others. The software technology comes from the IT industry—for example, standard operating systems, Java, and Session Initiation Protocol (SIP). SIP messages are structured in plain English text. They carry information about which codec to use, as well as parameters for the Real-Time Transport Protocol (RTP) connection.

The development cycles for IMS are short, and the platform for innovation is maximized. Because telephony is just another application, anyone can provide telephony services—even an entity that is not an access provider. The number of players will increase dramatically, as evidenced by the entry of Microsoft (MSN), Yahoo!, AOL, AT&T CallVantage, Skype, and Vonage, all of which already are active in this market.

Gateways connect the two worlds of TDM and IP. IMS is remarkably independent of the past and will be able to provide the platform for multimedia services for the next ten years, including new technologies, service concepts, players, and customer demands.

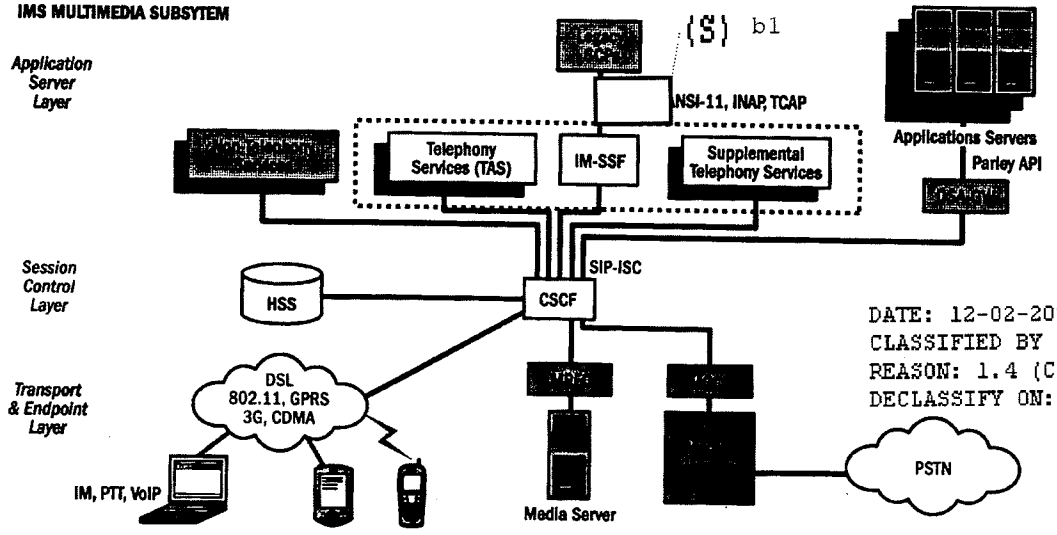


Figure 8.1. IMS Multimedia Subsystem

1. 3GPP Third Generation Partnership Project - European Telecommunications Standards Institute (ETSI).
2. 3GPP Third Generation Partnership Project2 - Developing the next generation of cdma2000 wireless communications.
3. The Parlay Group aims to intimately link IT applications with the capabilities of the telecommunications world by specifying and promoting Application Programming Interfaces (API) that are secure, easy to use, rich in functionality, and based on open standards (http://www.parlay.org/).

DATE: 12-02-2008
CLASSIFIED BY 60322/UCLRP/PJ/EHL
REASON: 1.4 (C)
DECLASSIFY ON: 12-02-2033

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

In Internet telephony, a constant identifier is the user's symbolic name (e.g., smith@service-provider.com), although the user's IP address will change. The required lookup, commonly known as ENUM, can be either centralized or decentralized. Microsoft MSN, Yahoo, and AOL telephony use a centralized lookup; Skype, through its free software downloads, uses a decentralized directory. Skype uses the FastTrack's well-known peer-to-peer file sharing application, KaZaA. Each PC stores and updates a part of the worldwide directory, using a Distributed Hash Table (DHT) algorithm. Updates and searches are done by cooperating individuals, and not by a single service provider function.

IMS provides a framework for communications of any type, anywhere, anytime—the ultimate goal of users and service providers alike. Concepts such as bandwidth-on-demand (based on the application, and only during the application session) and real-time, secure, multimedia, delivered via wireless broadband access, are designed into the standard, allowing individual equipment vendors and applications service providers to plug-and-play, thereby expanding the provider scope and assuring the greatest selection of value-added services.

b2
b7E

The IMS architecture is designed to support multivendor deployments. Layer functionality and protocols are well-defined. Many vendors will be offering components of the overall system, providing specific functionality or applications without knowledge or control of the system as a whole. The systems integrator and network service provider will be responsible for compliance with assistance to Communications for Law Enforcement Act (CALEA). Individual "box" manufacturers may have certain responsibilities as well, particularly if specified by the integrator.

IMS ARCHITECTURAL OVERVIEW

The IMS architecture comprises 12 major components (see Table 8.1); the IMS standard specifies the definition and functionality of each component. The ETR Bulletin Volume 2, Issue 2 (July 2005) highlighted the role of individual subsystems that assist in meeting overall CALEA capabilities, citing the Lucent Technologies IMS CALEA capability.

The IMS service architecture is a unified architecture that supports a range of services enabled by the session set-up capability provided by SIP. IMS can support multiple application servers offering traditional telephony as well as nontelephony services (e.g., Instant Messaging (IM), Push-to-Talk (PTT), video [illegible] recognition. The service architecture is a collection of logical functions, divided into three layers (see Figure 8.1):

- Transport and Endpoint Layer
- Session Control Layer
- Application Service Layer

TRANSPORT AND ENDPOINT LAYER

The transport and endpoint layer initiates and terminates SIP signaling to establish (and set up) sessions and provide bearer services, such as conversion of voice from analog/digital to IP packets using RTP. The media gateways convert Voice over IP (VoIP) bearer streams to the PSTN TDM format within this layer. The media server also provides related media services, such as user conferencing, service announcements, collection of in-band signaling tones, speech recognition, speech synthesis, and other services.

Media server resources are shared across all applications. Any application that requires service calls on a common server to meet its need. Applications include voicemail, advanced 800 service, and interactive Voice eXtensible Markup Language (VXML) services, among others. The media server also supports nontelephony functions such as replicating media to provide for PTT service.

SESSION CONTROL LAYER

This layer includes the Call Session Control Function (CSCF), which provides registration of endpoints and routing of SIP signaling messages to the appropriate applications server. The CSCF plays a critical role in intercepting call identification information for law enforcement. The CSCF interacts with the transport and endpoint layer to guarantee QoS across all services. The session control layer includes the Home Subscriber Server (HSS) database, which maintains the unique service profile for each authorized user. This user service profile includes all user service information and preferences in a central location which provides critical information for law enforcement. This database includes users' current registration information (IP address), roaming information, telephony services (call forwarding information and call acceptance), IM information (buddy lists), and voice mailbox options. Centralized information supports and simplifies administration of user data and provides consistent views of user profiles across applications, regardless of service provider. This function enables creation of unified personal directories, multiclient presence information, and blended services.

APPLICATION SERVICE LAYER

The application service layer incorporates application servers that provide the user service logic. The IMS architecture and SIP signaling are designed to support a variety of telephony and nontelephony applications servers, including IP multimedia services.[4]

4. IETF RFC 3428, "Session Initiation Protocol Extensions for Instant Messaging"

1. Access Gateway (AG): Provides an interface between the IP-based network and the radio access network. (MOBILE)

2. Access Network (AN): Radio component of the network. (MOBILE)

3. Breakout Gateway Control Function (BGCF): Controls all resources allocated to the IP session. (NETWORK CONTROL)

4. Call Session Control Function (CSCF): Provides control and routing function for IP sessions. (NETWORK CONTROL)

5. Foreign Agent (FA): Advertises itself to mobile stations in the serving area. Provides registration information to Home Agent. Forwards packets from mobile to Home Agent. (MOBILE)

6. Home Agent (HA): Tracks all current FAs serving the mobile. Forwards packets to the current FA. (MOBILE)

7. IP network. Contains Authentication, Authorization and Accounting (AAA) function and other required service databases; can be IPv4 or IPv6 (NETWORK)

8. Media Gateway (MGW): Provides an interface for bearer traffic to/from the public switched telephone network (PSTN) and IP networks. (PSTN TRAFFIC _ LEGACY)

9. Media Gateway Control Function (MGCF): Provides signaling interoperability between IP and PSTN domains (e.g., SIP to Integrated Services Digital Network User Part (ISUP), ISUP to SIP) (PSTN SIGNALING _ LEGACY)

10. Policy Decision Function (PDF): Assigns resources according to application demand and required Quality of Service (QoS); unlike TDM networks, IP networks assign network bandwidth and resources in real time (NETWORK CONTROL)

11. Position Determination Entity (PDE): Although a growing number of mobiles incorporate Global Positioning System (GPS), the PDE can provide assistance in determining geolocation by using network measurements and complex algorithms (NETWORK SERVICES)

12. SIP Application Server (SAS): A platform for SIP application development and operation (IP CALL SETUP)

Telephone Application Server (TAS): The TAS is a back-to-back SIP user agent that maintains the call state. The TAS contains the service logic that provides basic call processing services, including digit analysis, routing, call setup, call waiting, call forwarding, conference bridging, and other well-known telephone features. The logic required to invoke the media server to support appropriate call process tones and announcements resides in the TAS. If calls originate or terminate on the PSTN, the TAS provides SIP signaling to the Media Control Gateway Function (MCGF) to instruct the gateway to convert the PSTN TDM voice bitstream to an IP RTP stream and direct it to the IP address of the corresponding IP phone.

[redacted] triggers, including mid-call triggers. If a trigger is observed, the TAS suspends call progress and determines, on the basis of the subscriber's service profile, what additional application services are to be applied at that point in the call. If called for, the TAS formats an SIP IP Multimedia Service Control (ISC) message and passes call control to the appropriate application server. The TAS supports legacy AIN functionality as well as new SIP-based applications servers.

A single IMS supports multiple TASs that provide specific features to endpoints, based on authorized services (user profile). For example, one TAS can support IP Business Centrex features (i.e., private dialing plans, shared directory numbers, multiple call appearances, Automatic Call Distribution (ACD) and attendant services), and another could support Private Branch Exchange (PBX) and provide for advanced Virtual Private Network (VPN) services. Multiple application servers can use SIP-I signaling to complete calls between different classes of users.

{S}

IP Multimedia – Services Switching Function (IM-SSF): The IM-SSF provides the interworking of SIP messages to corresponding [redacted] b1 American National Standards Institute-41 (ANSI-41), Intelligent Network Application Protocol (INAP), or Transaction Capabilities Application Part (TCAP) messages. This interworking is required to allow IP phones supported by IMS to access services such as calling name service, 800 services, Local Number Portability (LNP) services, and one-number services ("find-me-follow-me" services).

Supplemental Telephony Application Servers: The application server layer also supports standalone independent servers that provide supplemental telephony services at the start, middle, or end of a call, via AIN-like triggers (user-to-network signals). Such services include "click to dial," "click to transfer," "click to conference," voicemail services, Independent Voice Recognition (IVR) services, VoIP VPN services, prepaid billing, and inbound/outbound call blocking services.

Nontelephony Application Servers: The application layer also can support SIP based application servers that operate outside the telephony call model. These application servers can interwork with user endpoint clients to provide services such as IM, PTT, and presence-enabled services. Implementation of nontelephony SIP-based services in a common IMS architecture permits interworking of telephony and nontelephony services to create new, blended communication features and capabilities. An example is a "click to contact" buddy list that displays end user presence and availability information, which provides a point-and-click interface across multiple communication services (telephone, IM, and PTT). Another example is the use of a single prepaid account for telephone and nontelephony services.

Open Service Access – Gateway (OSA-GW): The IMS architecture has a flexible design which allows services to be added into the VoIP networks by interacting with legacy applications or by

Privileged, Deliberative, Sensitive Information Which May Impact Law Enforcement Procedures and Capabilities · For Official Law Enforcement Use Only · Redisclosure Authorized by FBI Only

Integrating SIP-based application [illegible] specific applications. IMS supports service providers permitting their customers to develop and implement services that leverage VoIP network resources. For example, if an enterprise wanted to voice-enable a back-office operation to automatically initiate a call if an order was rejected because of missing shipping information, this function could be triggered by a Personal Digital Assistant (PDA)-like scanning device that recognizes information is missing and communicates the trigger function to the applications server.

(S) In many cases, IT programmers are not familiar with complex telephony signaling protocols such as SIP, ANSI41, Integrated

b1 Services Digital Network (ISDN), and [redacted] To provide a simple Applications Program Interface (API) the Parlay Forum, working with 3GPP and ETSI, has defined an API for telephony networks. This interface between SIP and the API is provided in the OSA-GW, which is part of the application service layer. The OSA-GW allows enterprise-based API applications to access presence and call-state information, set up and take down sessions, and manage and change call legs. The enterprise applications servers can register with the network and manage access to network resources. This capability introduces enhanced third-party applications programming to the communications path.

IMS CALL FLOW

IMS is based on the Internet, which carries packets over fixed or mobile networks. IMS implements roaming and enables users to take their phones anywhere as long as they identify themselves via a login and password process. The architecture is not limited to Internet telephony. It is a platform for a wide range of new communications and information services.

IP Telephony: When a phone is connected to the network, it sends an SIP message to register with the HSS, which stores the directory for its domain. This function manages the association between the symbolic name and the IP address. To initiate a call, the user SIP phone sends an INVITE message via the Serving - Call Session Control Function (S-CSCF), where the address is resolved. The S-CSCF determines which application to activate–e-mail, voice, or video–and, for law enforcement, whether interception is required. The S-CSCF then forwards the INVITE message to the appropriate IP address. The S-CSCF is not a switch. It is a serving function that is integral to the application of lawful interception. It performs the following functions:

1. Identifies the caller's service privileges and S-CSCF of called party
2. Replaces the symbolic name of called party with IP address
3. As required, the SIP message is forwarded to an applications server and performs an operation based on the applications server directions.

[illegible] address of the system to send its SIP messages. IMS specifies a proxy CSCF or P-CSCF as this entry point. All phones have the address of the P-CSCF. Messages are then forwarded to the home interrogating CSCF (I-CSCF). The P-CSCF serves as the visiting Session Control Function Server, and the I-CSCF is the home Session Control Function Server.

Legacy Network Interaction: If the call terminates on a legacy number, the S-CSCF detects this and interfaces with the BGCF. The MGCF is selected and performs the translation between SIP messages and the ISUP Signaling System 7 (SS7) message. It also controls the MGW, which performs the translation between the Internet voice flow (RTP) and the legacy PCM voice flow.

MIGRATION TO IMS

The SIP[5] signaling, RTP,[6] and IMS architecture were developed to rapidly move beyond broadband voice and data services and into the realm of advanced broadband multimedia services such as broadcast television using multicast IP video streams, video-on-demand, video surveillance, video telephony, videoconferencing, virtual classrooms, video e-mail, and similar applications yet to be invented. All of these services and more can be introduced by equipping the network with additional multimedia application servers and supporting endpoint devices. (Figure 8.2 highlights standardized architectural support for traditional non-SIP telephony.)

As new broadband multimedia services become prevalent, bandwidth management will be required to provide for QoS beyond the basics available today. Monitoring and control of available bandwidth will affect the number of active, real-time communications sessions. Endpoints will send their SIP requests

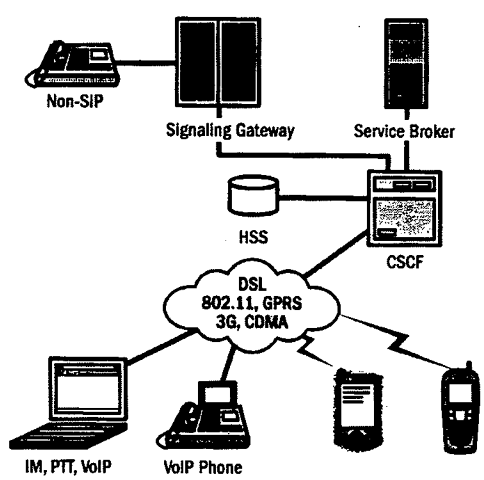


Figure 8.2: Location Service Infrastructure Example

5. SIP is used to set up calls between hosts, starting with the INVITE message, with parameters for the RTP connection. The answer is a RINGING message, followed by an off-hook, OK message. Following the ACK message, a RTP connection is established. SIP also can be used for instant messaging.
6. RTP transports voice and video. The sender uses a codec to encode the flow in a format such as G711, MP3, Advanced Video Coding (AAC), or Motion Picture Experts Group (MPEG).

[redacted] a common QoS standard. The QoS manager interfaces to transport and endpoint layers of the network to assess current traffic levels and can deny requests for additional sessions or applications that request additional bandwidth.

3. [redacted]

Extensions of the IMS architecture to support new services are on the horizon. Today only a fraction of the endpoints support SIP signaling. IP-PBX typically uses H.323 signaling. Integrated Access Devices (IAD) use Media Gateway Control Protocol (MGCP) to provide VoIP over Digital Subscriber Lines (DSL). Supporting these numerous endpoints in an IMS network will require supporting non-SIP signaling (e.g., non-SIP to SIP). 3GPP proposes the introduction of new border signaling gateways to provide for this interworking. The architecture clearly is flexible enough to provide for this specific functionality, enabling a linkage from present to future. IMS is well suited to support specific interworking and brokering services, enabling blended features to offer new services to users without major changes in the basic platform. The result will be rapid introduction of new, value-added services that are proprietary to a specific service provider yet are fully compatible with the over all "public" network. The concept entails a service broker or interaction manager element that will share application state and communication status information between applications, allowing for smooth introduction of new capabilities.

IMPLICATIONS FOR LAW ENFORCEMENT

There are three significant implications for law enforcement:

1. [redacted]

2. [redacted]

b2
b7E

CONCLUSION

IMS is the future architecture for Internet multimedia telephony. It provides an ideal standardized architecture that will allow service providers—large or small, incumbent or start up—to introduce a plethora of broadband multimedia services that require bandwidth on demand and rely heavily on a broad spectrum of third-party application developers and independent applications service providers. In many cases, applications will be proprietary to the provider, and complete knowledge of the communication will not reside at a single point. Furthermore, as with all IP network applications, the server need not be centralized or in a defined geographic territory.

IMS involves no circuits, or circuit emulation, and there are no switches. It is not constrained by legacy telephony and thus will take advantage of advances in Internet technology.

IMS adds functions in the network (i.e., between the hosts) to make the services easier to use or to add functionality to the services. It is easy to add a new application, in the form of a SIP message processing function for each new service created. Network operators propose to use IMS in place of proprietary solutions proposed by Microsoft, Yahoo!, Skype, and AOL. [redacted]

[redacted]