Voice over Internet Protocol (VoIP): The Dynamics of Technology and Regulation

by

Chintan Vaishnav

Bachelor of Engineering, Electronics and Communications
Rastriya Vidyalaya College of Engineering, Bangalore University, India

Master of Science, Electrical Engineering
Colorado State University, USA

Submitted to the Engineering Systems Division in Partial Fulfillment of the
Requirements for the Degree of
Master of Science in Technology and Policy
at the
Massachusetts Institute of Technology
June 2006

Signature of Author.....
Technology and Policy Program, Engineering Systems Division
May 12, 2006

Certified by.....
Charles Fine
Chrysler LFM Professor of Management and Engineering Systems
Thesis Supervisor

Accepted by .....
Dava J. Newman
Professor of Aeronautics and Astronautics and Engineering Systems
Director, Technology and Policy Program

Voice over Internet Protocol (VoIP): The Dynamics of Technology and Regulation

by
Chintan Vaishnav
Submitted to the Engineering Systems Division on May 12, 2006 in Partial Fulfillment of the Requirements for the Degree of Master of Science in Technology and Policy

Abstract

"What Voice over Internet Protocol (VoIP) is going to do is start to weaken the foundation of the way we've done things for 100 years...Congress already should be discussing the next telecom bill," said Federal Communications Commission (FCC) Chairman Michael Powell in February 2004, before the United States Senate. The objective of this thesis is to study how VoIP challenges the incumbent US telecommunications act.

The appearance of VoIP comes at a juncture when telecommunications system has already turned into a large-scale, complex system with multiple, competing infrastructures. VoIP, however, greatly augments the nested complexity by affording a technology that enables multiple architectures and business models for delivering the same voice (and often converged voice and data) service, while remaining agnostic to the underlying infrastructure. The VoIP-enabled architectures have very different capabilities and costs from one another. Many do not – or cannot – support social regulations such as emergency 911, wiretapping and disability access. Most exploit the economic arbitrage opportunities by evading access charges and universal service contributions. Added to this is the combination of reduced asset specificity due to VoIP's layered architecture and a global standard based ubiquitous IP technology that frees the service providers of the need to own the delivery infrastructure, and enables them to offer service from anywhere globally. Such a misalignment – between regulatory obligations and technical capabilities – has the potential to incubate large-scale systemic failures due to lack of coordination between the local optimization focused private markets and the highly compartmentalized public institutions.

The case of Communications Assistance for the Law Enforcement Act (CALEA) – also known as the wiretapping act – is taken to study its implications on VoIP. A system dynamics model is used for the analysis. Four policy lessons emerge through the process of

arriving at the model and the subsequent sensitivity analysis. First, considering peer-to-peer (P2P) VoIP a non-issue for CALEA is exactly what might make it an issue. Second, if P2P VoIP aspires to be a telephony substitute, it will invite the threat of social regulation. Third, arms race between CALEA-compliant and non-compliant technologies may raise the cost of CALEA compliance. Fourth, prohibiting use of certain encryption techniques may help the LEA to keep their ability to wiretap intact, but it also deprives customers of the privacy the prohibited schemes would have offered, and thereby helps the Internet-crime.

Thesis Supervisor: Charles Fine
Title: Chrysler LFM Professor of Management and Engineering Systems

To Hetal

for her love, patience and encouragement,

without which MIT would not have happened.

Acknowledgements

I would like to thank the following people in helping me produce this thesis.

- Prof. Charles Fine
- Dirk Trossen, Nokia Research and everyone involved with the Communications Futures Program
- Sharon Eisner Gillett
- David Clark
- David Reed
- Gabriel Weinberg
- Natalie Klym
- Carlos Osorio
- Betsy Masiello
- David Zipkin
- Tony Lim
- Rita Adom
- Sydney Miller and everyone involved with the Technology Policy Program

A special thanks to Scott Marcus, Bob Pepper and others at the Office of Strategic Planning, Federal Communications Commission (FCC)

Table of Contents

Abstract 3
Acknowledgements 6
List of Tables 11
INTRODUCTION 12
  Tips for reading this thesis 13
TECHNOLOGY AND REGULATION 14
  What is VoIP? 14
  Call Signaling 16
    H.323 18
    Media Gateway Control Protocol (MGCP) and Megaco 37
  Transport 42
    Delay 43
  Voice Quality 44
  Regulation 47
    Statutory Definitions and Jurisdiction 47
    911/E911 51
    CALEA 54
    Disability Access 61
    Universal Service 69
    Inter-carrier Compensation 80
VoIP CLASSIFICATION AND THE REGULATORY CHALLENGES 81
  Need for VoIP Classification 81
  VoIP Classification 84
    VoIP in the Backbone 84
    Facility-based VoIP 85
    VoIP over Broadband 86
    P2P VoIP 87
  Nature of Technology and Regulatory Challenges 88
    911/E911 88
    CALEA 88
    Disability Access 89
    Universal Service 90
    Inter-carrier Compensation 91
    Numbering 92
METHODOLOGY: THE SYSTEM DYNAMICS STANDARD METHOD 94
  What is "standard method"? 94
  Example of the Standard Method 95
    Variables List 95
    Reference Modes 96
    Problem Statement 97
    Momentum Policies 97
    Causal Loop Diagram or Dynamic Hypotheses 98
    Modeling 99
SYSTEM DYNAMICS MODEL FOR CALEA 103

CALEA Background 103
Six Variables of interest 103
Reference Modes and Rough Dynamic Hypotheses 105
Variable 1: Number of Lawful Intercepts Required 105
Variable 2: Percentage of Voice Traffic that is VoIP 107
Variable 3: Percentage of Voice Communications Subjected to CALEA 109
Variable 4: Percentage of Voice Communications that can be wiretapped 111
Variable 5: Percentage Intercepts that can be decrypted 113
Variable 5: Percentage Intercepts that can be decrypted 113
Variable 6: Cost of CALEA Compliance 115
CALEA CAUSAL LOOPS 117
Simplified Version 117
Complete Version 118
CALEA - STOCK AND FLOW MODEL 119
Model Construction and Assumptions 119
Parameter Values and Ranges 127
MODEL ANALYSIS AND POLICY LESSONS FOR CALEA 130
MODEL BEHAVIOR 130
SENSITIVITY ANALYSIS AND POLICY LESSONS 136
Policy Lesson 1: Considering P2P a non-issue for CALEA is exactly what might make it an issue. 138
Policy Lesson 2: If P2P aspires to be a telephony substitute, it will invite the threat of social regulation. 140
Policy Lesson 3: Arms race between CALEA-compliant and non-compliant technologies may raise the cost of compliance. 140
Policy Lesson 4: Prohibiting use of certain encryption techniques may help the LEA to keep their ability to wiretap intact, but it also deprives customers of the privacy the prohibited schemes would have offered, and thereby helps the Internet-crime. 143
REFERENCES 144
Appendix A: Abbreviations 146
Appendix B: VoIP Timeline 149
Appendix C: List of all CALEA Variables 153
Appendix D: CALEA Model Equations 155

List of Figures

Figure 1. End-to-end VoIP 15
Figure 2 H.323 Gateway 19
Figure 3 Direct endpoint call signaling 22
Figure 4 Gatekeeper routed call signaling (Q.931) 23
Figure 5 Gatekeeper routed call signaling (Q.931/H.245) 23
Figure 6. Basic call setup with gatekeeper 25
Figure 7. Basic call setup with gatekeeper routed call signaling. 26
Figure 8 Gatekeeper routed call signaling involving two gatekeepers. 27
Figure 9 SIP session setup with one proxy server. 30
Figure 10. SIP call setup with two proxy servers. 34
Figure 11 Existing Circuit Switched Networks 38
Figure 12 Master/Slave architecture involving call agents, signaling and media gateways. 38
Figure 13 Hourglass model of the Internet 81
Figure 14 Core-Edge Movement 82
Figure 15 Example of a reference mode 97
Figure 16 Example of Causal Loops to form Dynamic Hypothesis 99
Figure 17 Example of a modeled causal loop, its equations and the output 101
Figure 18 Reference modes and rough dynamic hypotheses for number of lawful intercepts required 105
Figure 19 Number of Wiretaps authorized by US Courts between 1968 and 2002 106
Figure 20 Reference modes and rough dynamic hypotheses for percentage of voice traffic that is VoIP 107
Figure 21 Reference modes and rough dynamic hypotheses for percentage of voice subjected to CALEA 109
Figure 22 Reference modes and rough dynamic hypotheses for percentage of voice communications that can be wiretapped. 111
Figure 23 Reference modes and rough dynamic hypotheses for percentage intercepts that can be decrypted 113
Figure 24 Reference modes and rough dynamic hypotheses for cost of CALEA compliance 115
Figure 25 CALEA Causal Loops: Simplified Version 117
Figure 26 CALEA Causal Loops: Complete Version 118
Figure 27 CALEA stock-flow model: VoIP Diffusion 119
Figure 28 CALEA stock-flow model: CALEA compliance 122
Figure 29 CALEA stock-flow model: Impact of CALEA on P2P VoIP 123
Figure 30 Complete CALEA stock-flow model 125
Figure 31 Managed VoIP Diffusion 130
Figure 32 P2P Diffusion 131
Figure 33 Minutes of Use 132
Figure 34 CALEA Jurisdiction 133
Figure 35 CALEA Jurisdiction causal trace 135

Figure 36 CALEA Causal Loops with Policy Insights 136
Figure 37 Sensitivity Analysis: Sensitivity of Managed VoIP Users to varying Sociability 137
Figure 38 Sensitivity Analysis: Sensitivity of CALEA Jurisdiction and Compliance Cost to varying P2P and Managed VoIP Diffusion 139
Figure 39 Sensitivity Analysis: Sensitivity of CALEA Deployment and Compliance Cost to varying Development and Deployment Rate of Non-CALEA Solutions 142

List of Tables

Table 1. Types of services that can be offered using SIP 36
Table 2. Delay Budget 44
Table 3. VoIP Classification 84
Table 4. Five regulatory issues, current obligations and VoIP challenges 93
Table 5. Six important variables for CALEA 104
Table 6. Parameter Selection for CALEA Model 129

Chapter 1

INTRODUCTION

Since the introduction of the VocalTec's VocalChat PC-to-PC phone in March of 1995, many articles in the trade press frequently claimed that, in the near future, telephone traffic would be just another application running over the Internet. Such statements gloss over many engineering, regulatory and economic details that preclude voice from being just another Internet application. This thesis is an attempt to provide a framework for understanding how voice over Internet protocol (VoIP) technology will impact regulatory choices, without speculating on the nature of the new regulatory regime.

On the technical side, Internet Protocol (IP) being agnostic to the physical medium provides a way to run VoIP as an application on wired or wireless networks. The wired network could be a public switched telephone network (PSTN), cable, digital subscriber line (DSL) or the Ethernet. The wireless network could be the wireless carrier's network, such as code division multiple access (CDMA), time division multiple access (TDMA) or GSM network, or private networks such as WiFi, BlueTooth or WiMAX. There are multiple, different architectures under which a service provider can offer a VoIP based voice communications service. At one extreme, it is possible to offer VoIP as an application that utilizes any infrastructure that offers the Internet connectivity. The application provider in this case need not own any parts of the infrastructure. On the other, there can be a complete vertical integration of service where the provider owns the infrastructure and all the components necessary to deliver service. Therefore, the choice of architecture determines the service provider's underlying costs, capabilities and

limitations. This necessitates the study of infrastructure ownership when discussing options for regulating various scenarios under which VoIP services is delivered to customers.

On the regulatory side, voice communications service has been subjected to a 100-year-old regulatory regime. The Internet on the other hand has been exempt from regulation. As the VoIP bridges the two worlds of PSTN and the Internet, the question for the regulators is: should VoIP service be regulated as a common-carrier regulation, just like a PSTN telecommunication service provider, left unregulated like the Internet, or be regulated under a third regulatory regime?

In this thesis, we will first discuss a way to classify the current panoply of VoIP offerings and the challenges they pose if the current regulatory regime were to apply to them. We will then examine the case of Communications Assistance for the Law Enforcement Act (CALEA) – also known as the wiretapping act – to study its implications on VoIP. A system dynamics model is used for the analysis. In chapter 2, we discuss VoIP technology and regulation. In chapter 3, we provide a way to classify different ways in which VoIP service is currently offered. We then discuss the regulatory challenges that arise in light of this classification. In chapter 4, we provide details of the standard method for system dynamics modeling, which is the methodology used for this research. In chapter 5, we detail the system dynamics model for CALEA. And finally, in chapter 6, we discuss the model analysis and lessons learnt for CALEA.

Tips for reading this thesis

Here are some tips for readers with various backgrounds to read this thesis more efficiently. A reader very familiar with the VoIP technology and regulation but not with

system dynamics methodology could skim chapter 2 and read in detail from chapter 3 on. A reader familiar with system dynamics could skip chapter 4.

Chapter 2
TECHNOLOGY AND REGULATION

What is VoIP?

Voice communication carried out using the Internet Protocol (IP) for the transport is known as Voice over Internet Protocol (VoIP). Traditional phone networks, known as Public Switched Telephone Networks (PSTN[1]) used circuit-switching. In *Circuit-Switching*, resources are reserved along the entire communication channel for the duration of the call. Conversely, Internet Protocol (IP) uses packet-switching. In *Packet-Switching*, information is digitally transmitted into one or more packets. Packets know their destination, and may arrive there via different paths.

Implementing VoIP requires a range of protocols from those needed to do call signaling for call establishment and more, to transport real-time voice across the network, to do quality-of-service-aware routing, resource reservation, QoS-aware network management and billing. Later in this chapter, we will examine evolution of each of these protocols to understand how they fit the currently popular architectures.

[1] For abbreviations see Appendix B

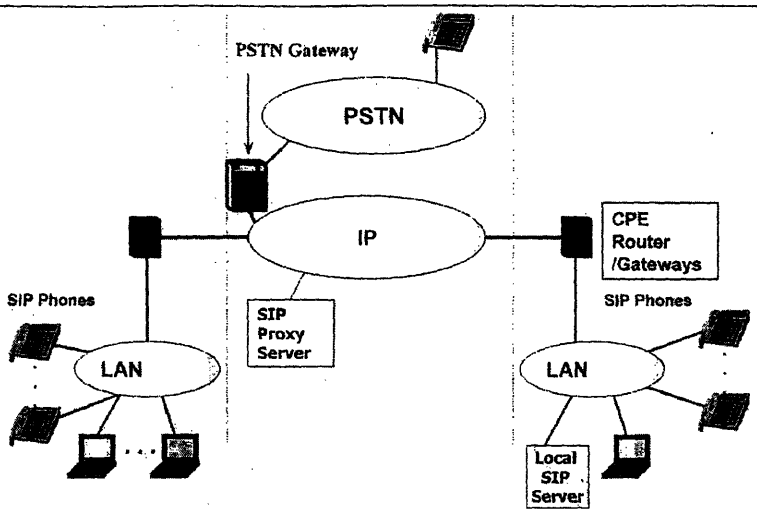


Figure 1. End-to-end VoIP

The purest VoIP implementation uses IP capable end-user equipment such as IP phones or a computer and does not rely on a standard telephone switch. Figure 1 is a simplified diagram of an IP telephone system connected to a wide area IP network. IP phones are connected to a LAN. Voice calls can be made locally over the LAN. The IP phones include codecs that digitize and encode (as well as decode) the speech. The IP phones also packetize and depacketize the encoded speech into IP packets. Calls between different sites can be made over the wide area IP network. Proxy servers perform IP phone registration and coordinate call signaling, especially between sites. Connections to the PSTN can be made through VoIP gateways.

As voice communication has been around for about 100 years, there exists a very well developed industry around the circuit-switched PSTN. There are many established incumbents with large customer bases. In the early days of VoIP, PSTN incumbents considered it a threat to their business, and an opportunity to the data networking vendors such as the Internet Service Providers (ISP). Over time, the PSTN incumbents and the

new entrants to voice communications alike view VoIP as an opportunity to provide voice service at a significantly reduced cost [1].

One way to understand the development of VoIP protocols is to take the perspective of these PSTN incumbents trying to preserve and grow their existing customer base, while the new entrants to voice communications from the data networking side begin to partake the entire pie of voice communication. Specific architectures and protocol development for VoIP, therefore comes from both the International Telecommunications Union domain [2], [3]), which is traditionally perceived as a standards organization that understands telephony better, and the Internet Engineering Task Force domain ([4], [5]), which is the primary standards body responsible for Internet and data networking standards. Recently, there is some protocol development in a joint domain [6]. These architectures and protocols have been validated in public telephone networks [7], in corporate telephone networks [8], and on the Internet [9]. In the following subsections we will examine the evolution of various protocols necessary to implement VoIP.

Call Signaling

VoIP requires a means for prospective communications partners to find each other and to signal to the other party their desire to communicate. This functionality is referred to as *Call Signaling*. The need for signaling functionality distinguishes Internet telephony from other Internet multimedia services such as broadcast and media-on-demand services.

VoIP, when used for synchronous voice or multimedia communication between two or more parties, uses signaling that creates and manages *calls*. The called can define a call as a named association between applications that is explicitly set up and torn down. Examples of calls are two-party phone calls, a multimedia conference or a multi-player game. A call may encompass a number of *connections*, where a connection is a logical relationship between a pair of end systems in a call. For example, a non-bridged three party audio only call will have three connections, creating a full mesh among the participants. A *media stream or session* is the flow of a single type of media among a set of users. This flow can either be unicast (in which case it is between two users), or multicast (more than two users). A media session is associated with one or more connections. In the above three party call example, if the media is distributed using unicast, there will be one audio session per connection. If the audio is distributed via multicast, there will be one audio session associated with all three connections. It is not required that calls have media streams associated with them, but this is likely to be the common case.

Internet telephony signaling may encompass a number of functions: *name translation and user location* involves the mapping between names of different levels of abstraction, *feature negotiation* allows a group of end systems to agree on what media to exchange and their respective parameters such as encoding, *call participant management* for participants to invite others on an existing call or terminate connections with them, *feature changes* that make it possible to adjust the composition of media sessions during the course of a call, either because the participants require additional or reduced

functionality or because of constraints imposed or removed by the addition or removal of call participants.

There are several VoIP call signaling protocols. We shall discuss and compare the characteristics of the H.323 protocol suite, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and Megaco/H.248. H.323 and SIP are peer-to-peer control-signaling protocols, while MGCP and Megaco are master–slave control-signaling protocols. MGCP is based on the PSTN model of telephony. H.323 and Megaco are designed to accommodate video conferencing as well as basic telephony, but they are still based on a connection-oriented paradigm similar to circuit-switching, despite their use for packet communications systems. H.323 gateways have more call control function than the media gateways using MGCP, which assumes that more of the intelligence resides in a separate media gateway controller. SIP was designed from scratch for IP networks, and accommodates intelligent terminals engaged in not only voice sessions, but other applications as well.

H.323

The ITU-T recommended H.323 protocol suite has evolved out of a video telephony standard [10]. When early IP telephony pioneers developed proprietary products[2], there was an industry call to develop a VoIP call control standard quickly so that users and service providers would be able to have a choice of vendors and products that would interoperate. The Voice-over-IP Activity Group of the International Multimedia Telecommunications Consortium (IMTC) recommended H.323, which had been

[2] After VocalTec introduced VocalChat and Free World Dial introduced their PC-to-PC products, one of the first waves was the introduction of telephony gateways. Delta Three, a company in Israel and a few others began to introduce gateways for carrying PSTN traffic over IP for the International calls (Financial Times, London, 2/3/1997).

developed for multimedia communications over packet data networks. These packet networks might include LANs or WANs. The IMTC held the view that VoIP was a special case of IP Video Telephony. Although not all VoIP pioneers agreed that video telephony would quickly become popular, the H.323 protocol suite became the early leading standard for VoIP implementations. Versions 2-4 of the standard include modifications to make H.323 more amenable to VoIP needs.

H.323 entities may be integrated into personal computers or routers or implemented in stand-alone devices. For VoIP, the important H.323 entities are *terminals, gateways, and gatekeepers.* An H.323 *gateway* provides protocol translation and media transcoding between an H.323 endpoint and a non-H.323 endpoint (see Figure 2). For example, a VoIP gateway provides translation of transmission formats and signaling procedures between a circuit-switched telephone and a packet network. In addition, the VoIP gateway may perform speech transcoding and compression, and it is usually capable of generating and detecting dual tone multiple frequencies (DTMF) (i.e. touch tone) signals.

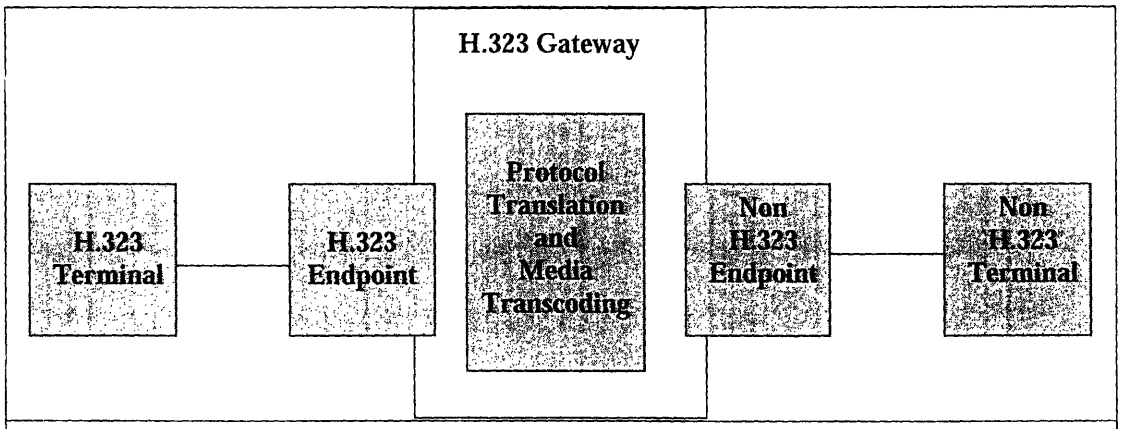


Figure 2 H.323 Gateway

The H.323 VoIP *terminal* elements include the following:

- A System Control Unit provides signaling for proper operation of the H.323 terminal that provides for call control using H.225.0 and H.245 (described below).
- H.225.0 layer formats the transmitted audio and control streams into messages, retrieves the audio streams from messages that have been received from the network interface, and performs logical framing, sequence numbering, error detection and error correction as appropriate.
- An audio codec transcodes and may also compress speech.

H.323 *gatekeepers* perform admission control and address translation functions. Several gatekeepers may communicate with each other to coordinate their control services. Networks with VoIP gateways should (but are not required to) have gatekeepers to translate incoming E.164 addresses into Transport Addresses (e.g., IP address and port number). The gatekeeper is logically separate from the other H.323 entities, but physically it may coexist with a terminal, gateway, or an H.323 proxy. When present in a VoIP network, the gatekeeper provides the following functions:

- Address translation—the gatekeeper translates alias addresses (e.g., E.164 telephone numbers) to Transport Addresses, using a translation table that is updated using Registration messages and other means.
- Admissions control—the gatekeeper authorizes network access using H.225 messages. Admissions criteria may include call authorization, bandwidth, or other policies.
- Bandwidth control—the gatekeeper controls how much bandwidth a terminal may use.

- Zone management—a terminal may register with only one gatekeeper at a time. The gatekeeper provides the above functions for terminals and gateways that have registered with it.
- Participation in call control signaling is optional.
- Directory services are optional.

When an endpoint (such as a phone) is connected to the network, the *Registration, Admissions, and Status (RAS) channel* carries messages used in gatekeeper endpoint registration processes that associate an endpoint's alias (e.g., E.164[3] telephone number) with its TCP/IP address and port number to be used for call signaling. The RAS channel is also used for transmission of admission, bandwidth change, status, and disengage messages between an endpoint and its gatekeeper. H.225.0 recommends time outs and retry counts for RAS messages, since they are transmitted on an unreliable User Datagram Protocol (UDP) channel[4].

The Call Signaling Channel carries H.225.0 call control messages using TCP, making it a reliable channel. H.323 endpoints and gatekeepers use Q.931 messages (with TCP) for call signaling. In networks with no gatekeeper, endpoints send call signaling messages directly to the called endpoint using the Call Signaling Transport Addresses. If the network has a gatekeeper, the calling endpoint sends the initial admission message to the gatekeeper using the gatekeeper's RAS Channel Transport Address. In the initial exchange of admissions messages, the gatekeeper tells the originating endpoint whether

[3] E.164 is an ITU-T standard for telephone numbering plan.
[4] Transport layer in the Internet offers two protocols for transporting packets – namely, transport control protocol (TCP) and user datagram protocol (UDP) – that every application must choose from. TCP is a connection-oriented protocol that guarantees packet delivery with a higher end-to-end delay necessary for extra processing. Conversely, UDP is a connectionless protocol that offers best-effort delivery at a lower delay. VoIP being a synchronous real-time application uses UDP for much of its operation.

to send the call signaling messages directly to the other endpoint or to route them through the gatekeeper. Call signaling may be routed in two ways: direct endpoint call signaling and gatekeeper routed call signaling.

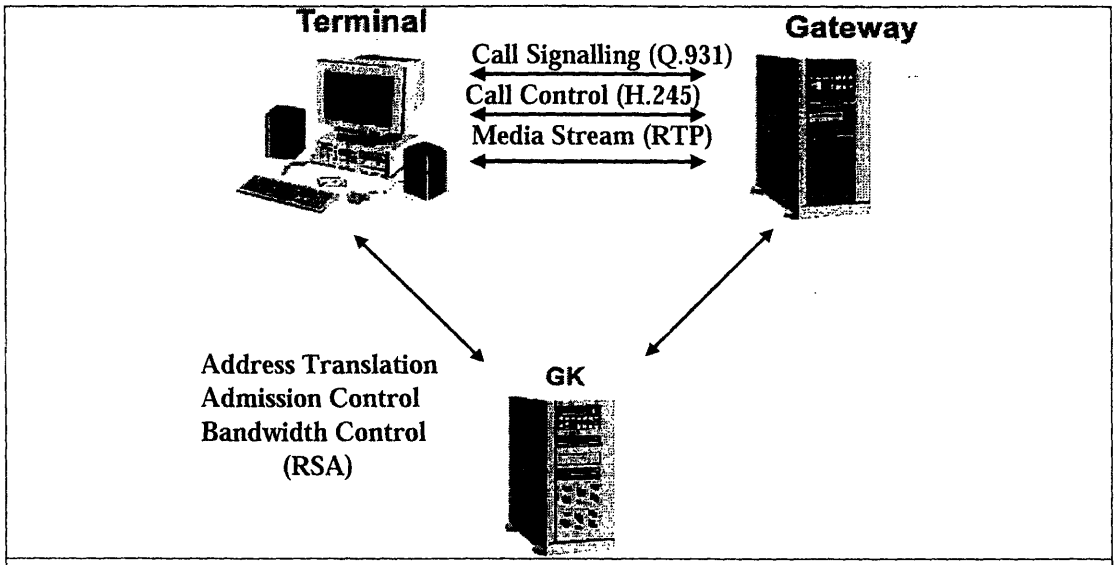


Figure 3 Direct endpoint call signaling

Figure 3 shows direct endpoint call signaling, which sends call signaling messages directly between the endpoints or gateways. In direct endpoint call signaling, the gatekeeper participates in call admission but has little direct knowledge of connections. Due to its limited involvement, a single gatekeeper can process a large number of calls, but the gatekeeper has a limited ability to perform service management functions. The gatekeeper cannot determine call completion rates, and, if it is to perform call detail recording, it must depend on the endpoints for call duration information.

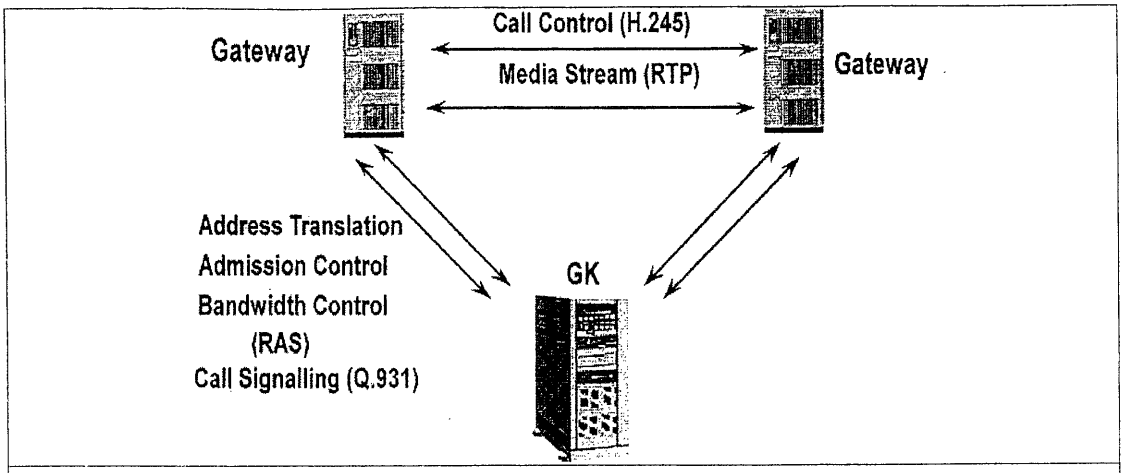


Figure 4 Gatekeeper routed call signaling (Q.931)

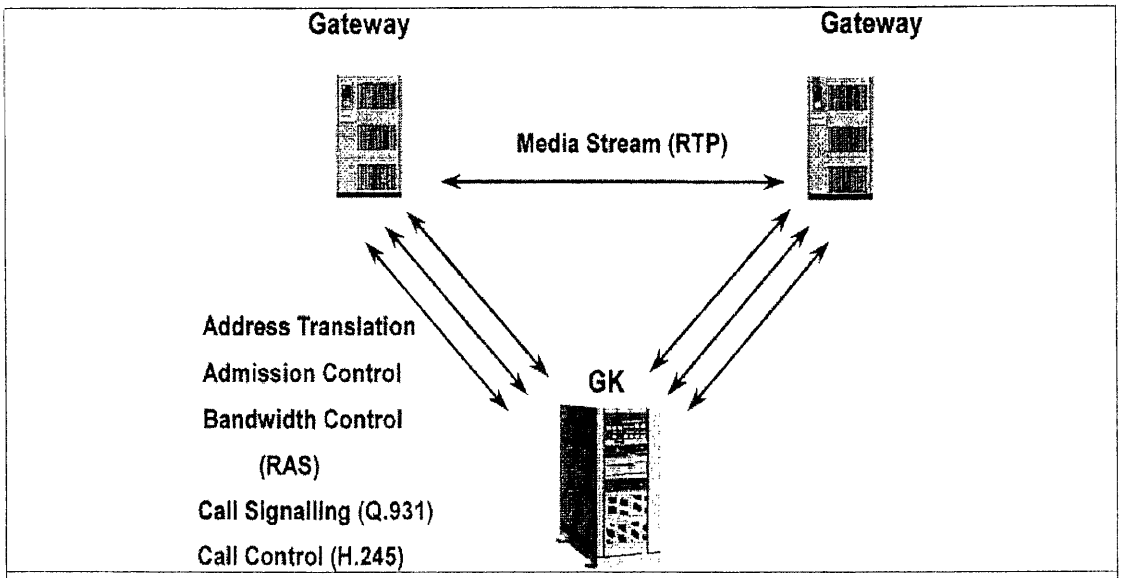


Figure 5 Gatekeeper routed call signaling (Q.931/H.245)

Figure 4 and Figure 5 show gatekeeper routed call signaling, which routes call-signaling messages from one endpoint through the gatekeeper to the other endpoint. The gatekeeper routed call signaling method results in more load on the gatekeeper, since it must process the Q.931 messages. The gatekeeper may close the call signaling channel after call setup is completed. However, if the gatekeeper remains involved in the call,

e.g., to produce call records or to support supplementary services, it will keep the channel open for the duration of the call[5].

The *H.245 Control Channel* carries end-to-end H.245 control messages governing operation of the H.323 entities (H.323 host, H.323 gateway or H.323 gatekeeper). The key function of the H.245 Control Channel is capabilities exchange. Other H.245 functions include opening and closing of logical channels, flow control messages, mode preference requests, and general commands and indications. The endpoint establishes an H.245 Control Channel for each call in which the endpoint participates. This logical H.323 Control Channel is open for the entire duration of the call. To conform to Recommendation H.245, H.323 endpoints must support the syntax, semantics, and procedures of the following protocol entities:

- master/slave determination;
- capability exchange;
- logical channel signaling;
- bidirectional logical channel signaling;
- close logical channel signaling;
- mode request;
- round-trip delay determination;

[5] Both H.225 and H.245 use TCP to establish a reliable transport connection between endpoints, gateways, and gatekeepers. In the case of gatekeeper-routed call signaling, the TCP connections are kept up for the duration of the call. Although normally reliable, the failure of a TCP connection could result in mid-call termination even though the TCP connection was not in use at the time. For example, suppose gatekeeper routed call signaling is used, and the TCP connection from gateway to gatekeeper is broken due to a timeout or a failure to exchange keepalive messages during a link failure or rerouting. Calls may be dropped even though the RTP voice media streams may have been unaffected by the network event that caused the TCP connection to the gatekeeper to fail.

- maintenance loop signaling.

As an example of how H.245 is used, let us discuss how it accommodates simple telephony signaling.

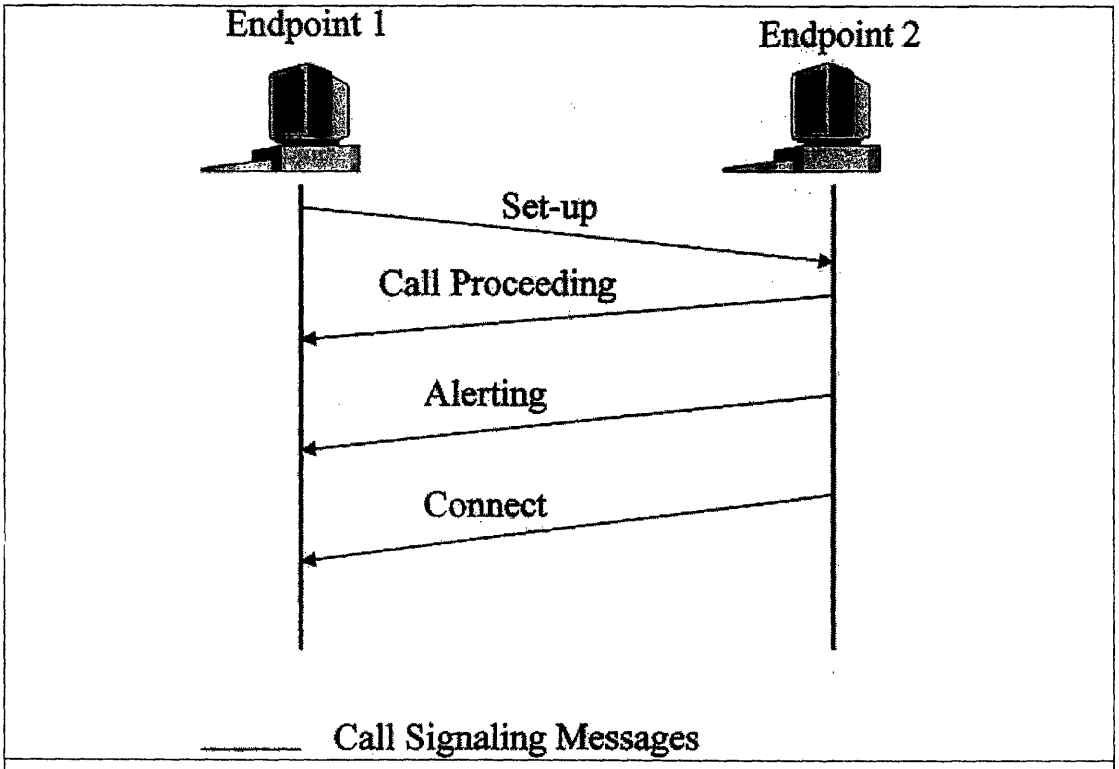


Figure 6. Basic call setup with gatekeeper.

Figure 6 shows basic call setup signaling for the case where neither endpoint is registered with a gatekeeper. The calling endpoint (endpoint 1) sends the setup (1) message to the well-known call signaling channel TSAP identifier (TCP port #1720) of endpoint 2. Endpoint 2 responds with call proceeding (2), alerting (3), and finally the connect (4) message containing an H.245 control channel transport address for use in H.245 signaling.

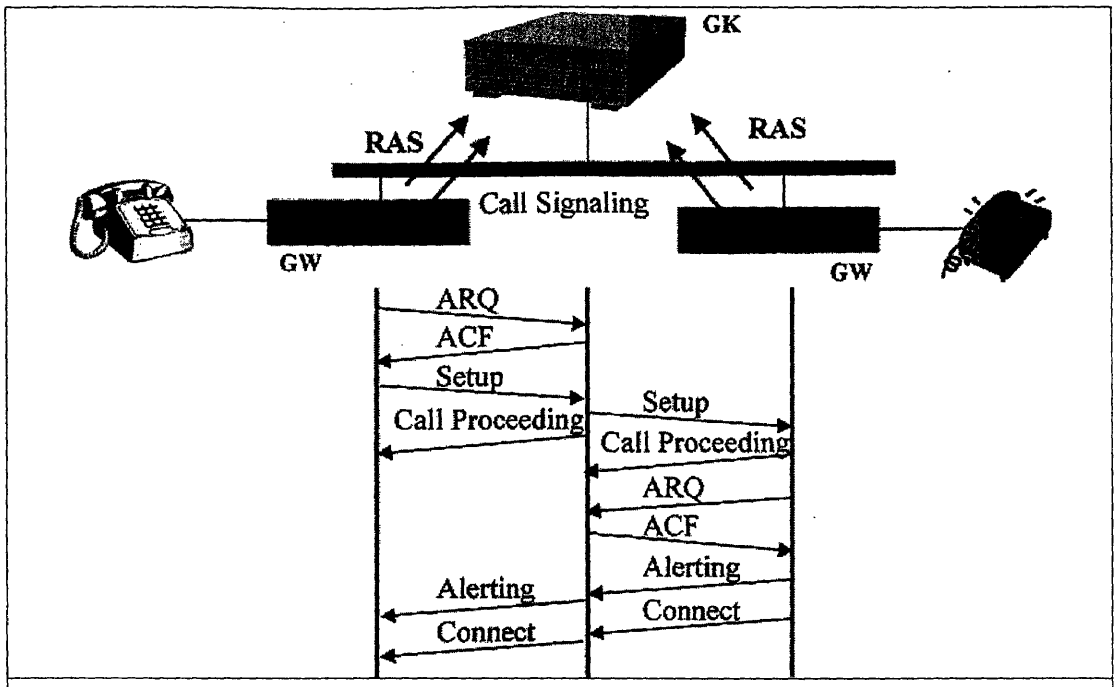


Figure 7. Basic call setup with gatekeeper routed call signaling.

Figure 7 shows a basic setup with gatekeeper routed call signaling. First, the originating gateway sends an admission request (ARQ) to the gatekeeper, which responds with an admission confirmation (ACF). Then setup proceeds as indicated.

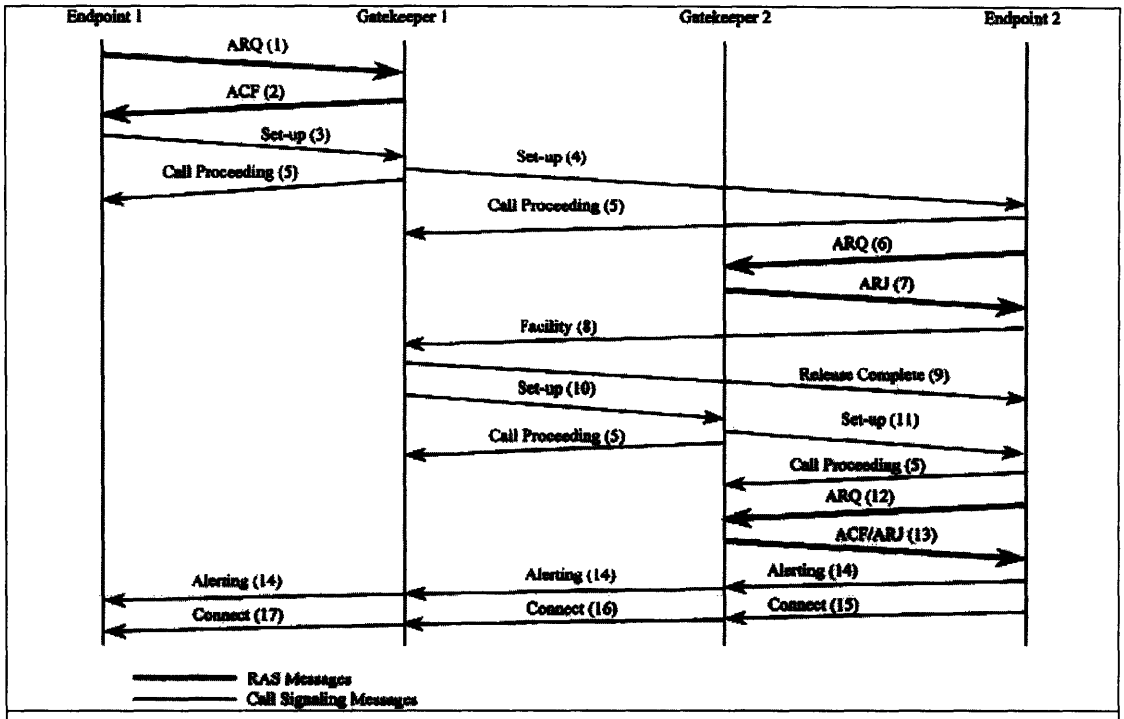


Figure 8 Gatekeeper routed call signaling involving two gatekeepers.

Figure 8 shows call setup where both endpoints are registered with separate gatekeepers, and both use gatekeeper routed call signaling. Note that these diagrams do not show explicitly the establishment of TCP connections between the endpoints and the gatekeepers. The first part of the call setup is similar to the single gatekeeper case shown in Figure 7. When the call setup message reaches endpoint 2, it initiates an ARQ(6) /ACF(7) exchange with gatekeeper 2. Assuming the call is acceptable, gatekeeper 2 sends its own call signaling address in a ARJ(7) reject message (instead of ACF) with a cause code commanding the endpoint to route the call signaling to it. The rest of the diagram is self-explanatory.

As one can see from Figure 8, call signaling can involve many messages passing back and forth among the H.323 entities. To reduce the call setup time for straightforward

calls such as VoIP, H.323v2 introduced an alternate call setup procedure called "Fast Connect [2]," which we will not discuss here.

Session Initiation Protocol (SIP)

SIP [5] is a control (or signaling) protocol similar to HTTP. It is a protocol that can set up and tear down any type of session. SIP call control uses Session Description Protocol (SDP) [11] to describe the details of the call (i.e., audio, video, a shared application, codec type, size of packets, etc.). SIP uses a Universal Resource Locator (URI)[6] to identify a *logical* destination, not an IP address. The address could be a nickname, an e-mail address (e.g., sip:chintanv@mit.edu), or a telephone number. In addition to setting up a phone call, SIP can notify users of *events*, such as "I am online," "a person entered the room," or "e-mail has arrived." SIP can also be used to send instant text messages.

SIP uses a client-server model. Clients send SIP requests, whereas servers accept SIP requests, execute the requested methods, and respond. The SIP specification defines six request methods:

- REGISTER allows either the user or a third party to register contact information with a SIP server.
- INVITE initiates the call signaling sequence.
- ACK and CANCEL support session setup.
- BYE terminates a session.

[6] A URI is a pointer to a resource that generates different responses at different times, depending on the input. A URI does not depend on the location of the resource. A URI usually consists of three parts: the protocol for communicating with the server (e.g., SIP), the name of the server (e.g., *www.nice.com*), and the name of the resource. A URL used for website addressing is a common form of URI; the reader need not worry about the difference.

- OPTIONS queries a server about its capabilities.

Some of the important SIP functional entities are listed below.

- *User agent* performs the functions of both a user agent client, which initiates a SIP request, and a user agent server, which contacts the user when a SIP request is received and returns a response on behalf of the user.
- *SIP proxy* acts as both a SIP client and a SIP server in making SIP requests on behalf of other SIP clients. A SIP proxy server may be either stateful or stateless. A proxy server must be stateful to support TCP, or to support a variety of services. However, a stateless proxy server scales better (supports higher call volumes).
- *Registrar* is a SIP server that receives, authenticates and accepts REGISTER requests from SIP clients. It may be collocated with a SIP proxy server.
- *Location server* stores user information in a database and helps determine where (to what IP address) to send a request. It may also be collocated with a SIP proxy server
- *Redirect server* is stateless. It responds to a SIP request with an address where the request originator can contact the desired entity directly. It does not accept calls or initiate its own requests.

SIP defines logical entities that may be implemented separately or together in the same product.

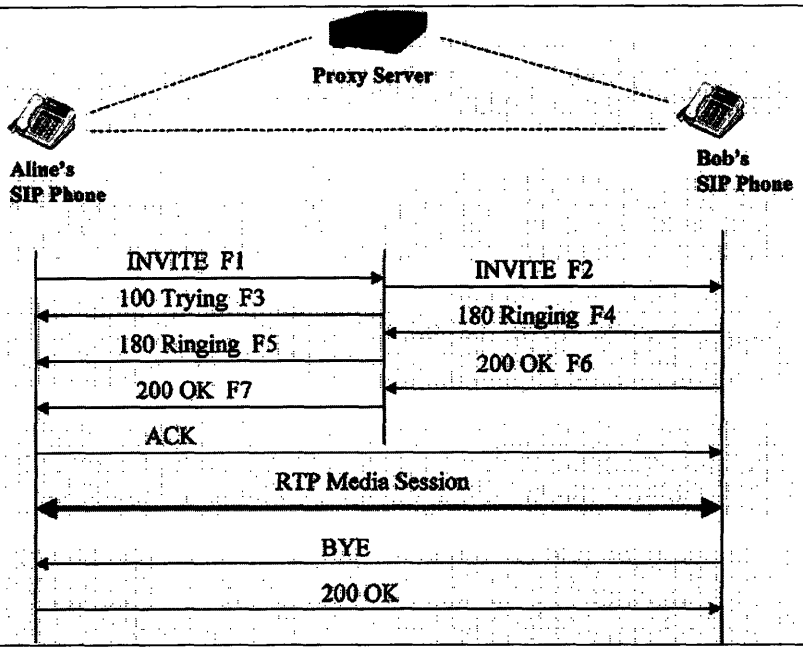


Figure 9 SIP session setup with one proxy server.

We use two simple examples to explain basic SIP operations. The first example uses a single proxy, as would be likely for SIP-based IP telephony within a single enterprise building or campus.

Aline calls Bob to ask a question about SIP. Aline and Bob work in the same corporate campus of buildings served by the same SIP proxy server. Since Aline and Bob do not call each other regularly, Aline's SIP phone does not have the IP address of Bob's SIP phone. Therefore, the SIP signaling goes through the SIP proxy server. Aline dials Bob's private number (555-6666). Her SIP phone converts this private number into a related SIP URI (sip:555-6666@nice.com) and sends an INVITE to the SIP proxy server. Figure 9 shows the SIP message exchange for this example.

SIP uses a request/response transaction model similar to HTTP. Each transaction starts with a request (in simple text) that invokes a server function ("method") and ends with a response. In our example, Aline's SIP phone starts the transaction by sending an

INVITE request to Bob's SIP URI (sip:555–6666@nice.com). The INVITE request contains header fields that provide information used in processing the message, such as a call identifier, the destination address, the originator's address, and the requested session type. Here is Aline's INVITE (message F1 in Figure 9):

- INVITE sip:bob@nice.com SIP/3.0
- Via: SIP/3.0/UDP 192.2.4.4:5060
- To: Bob <sip:555-6666@nice.com >
- From: Aline <sip:555-1234@nice.com >; tag=203 941 885
- Call-ID: b95c5d87f7721@192.2.4.4
- Cseq: 26 563 897 INVITE
- Contact: <sip:555-1234@192.2.4.4 >
- Content-Type: application/sdp
- Contact-Length: 142

(Aline's SDP not shown)

The first line gives the method name (INVITE). We will describe the header fields in the following lines of the example INVITE message, which contains a minimum required set:

- *Via* contains the IP address (192.2.4.4), port number (5060), and transport protocol (UDP) that Aline wants Bob to use in his response.
- *To* contains a display name (Bob) and a SIP URI (sip:555–6666@nice.com) toward which this request was sent.
- *From* contains a display name (Aline) and a SIP URI (sip:555–1234@nice.com) that identify the request originator.
- *Call-ID* contains a globally unique identifier for this call.

These three lines (*To, From,* and *Call-ID*) define a peer-to-peer SIP relationship between Aline's SIP phone and Bob's SIP phone that is sometimes referred to as a "dialog."

The command sequence (*Cseq*) contains an integer and a method name. Aline's SIP phone increments the *Cseq* number for each new request.

Contact contains Aline's username and IP address in the form of a SIP URI. While the *Via* header tells Bob's SIP phone where to send a response, the *Contact* header tells both the proxy server and Bob's SIP phone where to send future requests for this dialog.

Content-type describes the message body.

Content-length gives the length (in octets) of the message body.

The body of the SIP message contains a description of the session, such as media type, codec type, packet size, etc., in a format prescribed (usually) by SDP. The way the SIP message carries a SDP message is analogous to the way an HTTP message carries a web page.

Since Aline's SIP phone does not know Bob's IP address, the INVITE message goes first to the SIP proxy server. When it receives the INVITE request, the proxy server sends a 100 Trying response back to Aline's SIP phone, indicating that the proxy is trying to route the INVITE to Bob's SIP phone. In general, SIP responses have a numerical three- digit code followed by a descriptive phrase. This response (Message F3 in Figure 9) contains the same to, from, call-ID and Cseq header values as the INVITE message, and Aline's SIP phone can correlate this response with what it sent. The proxy server adds another Via header with its own IP address to the INVITE and forwards it (Message F2 in Figure 9) to Bob's SIP phone.

When Bob's SIP phone receives the INVITE, it alerts (rings) Bob, so that he can decide whether to answer. Since Aline's name is in the To header, Bob's SIP phone could display Aline's name. Bob's SIP phone sends a 180 Ringing response through the proxy

server back to Aline's SIP phone. The proxy uses the Via header to determine where to send the response, and it removes its own address from the top. When Aline's SIP phone receives the 180 ringing response, it indicates ringing by displaying a message on the SIP phone display or by an audible ringback tone.

When Bob pushes the speakerphone button, his SIP phone sends a 200 OK response to indicate that he has answered the call. The 200 OK message body contains the SDP media description of the type of session that Bob's SIP phone can establish on this call. Thus there is a two-way exchange of SDP messages, negotiating the capabilities to be used for the call. Aline's SIP phone sends ACK directly to Bob's SIP phone (it does not pass through the stateless proxy server), and Aline can talk to Bob through an RTP media session. Note that the actual voice packets are routed directly from one SIP phone to another, and their headers have no information about the SIP messages or proxy servers that set up the RTP media session.

In this example, Bob is unable to answer Aline's question, but suggests that she call Henry in Dallas. Henry is an SIP expert, but he is with a different company, global.com. Bob has Henry's email address, but not his telephone number. When Bob says goodbye and presses the button, his SIP phone sends a BYE directly to Aline's SIP phone. Aline's SIP phone responds with a 200 OK, which terminates the call, including the RTP media session.

Now Aline calls Henry (follow Figure 10) using the laptop computer connected to her SIP phone, Aline types Henry's email address and clicks on the button to establish a SIP phone call. Aline's SIP phone sends an INVITE addressed to Henry's SIP URI, which is based on his email address (henry@global.com). Since the Nice.com proxy server does

not know how to route the call to Henry, it uses domain name service (DNS) to find the global.com SIP server.

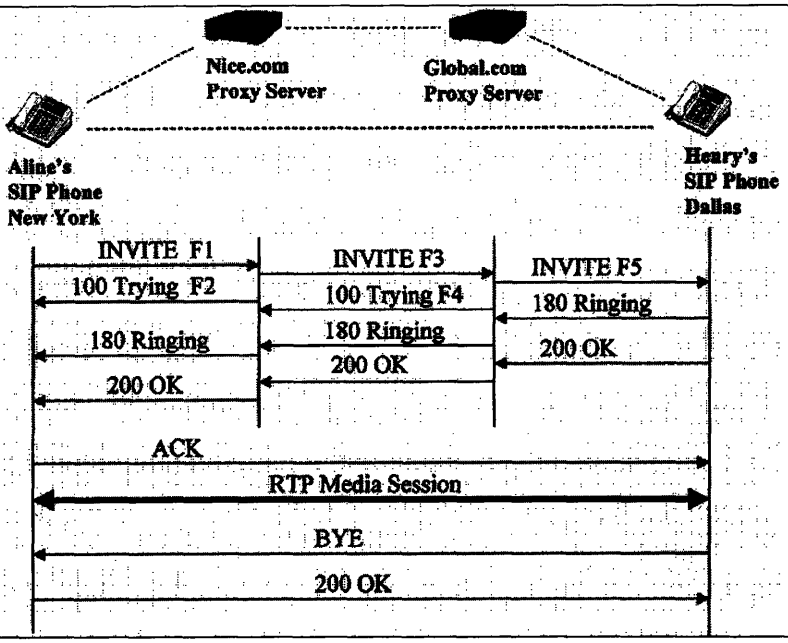


Figure 10. SIP call setup with two proxy servers.

Actually, what the Nice.com server needs is a list of next hops that can be used to reach the global.com server. The *next hop* is defined by the combination of IP address, port and transport protocol. The SIP specification gives an algorithm for determining an ordered list of next hops.

Aline's INVITE (message F1 in Figure 10) looks similar to the one she sent to Bob:

- INVITE sip:henry@global.com SIP/3/0
- Via: SIP/3.0/UDP 192.2.4.4:5060
- To: Henry <sip:henry@global.com >
- From: Aline <sip:aline@nice.com >; tag=9 817 514 140
- Call-ID:z73a3b65d55609@192.2.4.4
- Cseq: 704 452 INVITE

- Contact: <sip:aline@192.2.4.4 >
- Content-Type: application/sdp, etc.

Note that, in this INVITE message, the SIP URI's are based on email addresses instead of telephone numbers. The flow of messages is similar to the setup of the call to Bob, except that the SIP messages now pass through the global.com proxy server as well as the nice.com proxy server, as shown in Figure 10.

SIP allows proxy servers to make complex decisions about where to send the INVITE. In the example, Henry could have been traveling and had his calls forwarded to a company office in Washington, DC. A proxy server can send an INVITE to several locations at the same time, so the call could be routed simultaneously to Henry's voicemail server in Dallas and his guest office in Washington. If Henry answers the call in Washington, the session with the voicemail server can be terminated.

The INVITE request could contain information to be used by the destination proxy server to determine the set of destinations to ring. For instance, destination sets may be constructed based on time of day, the interface on which the request has arrived, failure of previous requests, or current level of utilization of a call distributor. Aline might program her SIP phone to request a follow-me service only to business locations. On the other hand, Henry might program his SIP server to forward calls to his mobile phone, but only a privileged access list (family and boss?) would have calls forwarded to his home.

SIP facilitates mobility, because the same person can use different terminals with the same address and same services. SIP promises to be used by many programmers to develop new services. Many of these new services may be offered on the public Internet.

PSTN-like services	New Services
Caller ID	Web/Voice integration
PBX-like features	Programmable services
Call forwarding	Multi-destination routing
Call transfer	Presence
AIN-like features	Instant messaging
Freephone	Multimedia
Find me/follow me	Event notification
Conference calls	Caller and called party preferences
	Unified messaging

Table 1. Types of services that can be offered using SIP

SIP allows the easy addition of new services by third parties. Microsoft has included a SIP stack in Windows XP, its latest desktop operating system, and it has a definite schedule for rolling out a new .NET server API that is the successor to the Windows 2000 server. Since SIP will support intelligent devices that need little application support from the network as well as unintelligent devices that need a lot of support from the network, we have an opportunity analogous to the transition from shared computers to personal computers. In the 1960s and 1970s, we used dumb terminals to access applications on a mainframe computer shared by many hundreds of users. Starting in the 1980s, we began to use sophisticated applications on a PC, but we were also able to use the PC as a communications terminal to gain access to applications and databases on shared computers (servers) in the network. SIP hosts with various degrees of

sophistication will perform some functions locally while allowing us to access applications in the network. SIP is different from H.323 in this regard. Whereas the H.323 model requires application interaction through call control, SIP users can interact directly with applications.

SIP can be used to create new services in addition to replicating traditional telephone services. Presence and instant messaging is an example of a new type of service that can use SIP. There are several popular instant-messaging systems that allow users to create buddy lists and convey status to other member of the buddy list. Status messages can show that one is talking on the phone, or in an important meeting, out to lunch, or available to talk. The members of the buddy list can use these "presence" status messages to choose an appropriate time to make a phone call, rather than interrupting at an inopportune time. Several leading suppliers of instant messaging software have committed to converting their systems to the use of instant messaging software have committed to converting their systems to the use of SIP.

Error! Reference source not found. describes some of the types of services that can be offered using SIP.

Media Gateway Control Protocol (MGCP) and Megaco

In MGCP and Megaco, the call processing function can be separated from the VoIP gateway function. We can define a new entity, a *"call agent,"* (CA) to control the gateways and perform call processing. The physical product implementing the call agent function need not be located near the gateway and could control many gateways. This architecture simplifies the VoIP gateway product, allowing the gateway to be located in

homes and small offices at low cost.

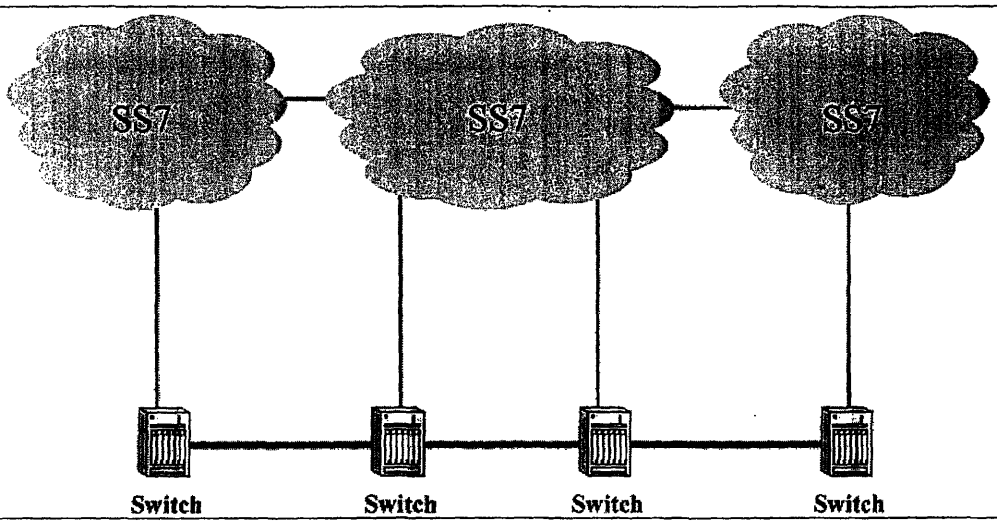


Figure 11 Existing Circuit Switched Networks

Consider the diagram of a circuit-switched network in Figure 11. The switches send telephone traffic directly from one to the other, but communicate call-signaling information among each other using a separate packet-signaling SS7 network. Note that, although packet switched, the SS7 protocol is not related to the IP.

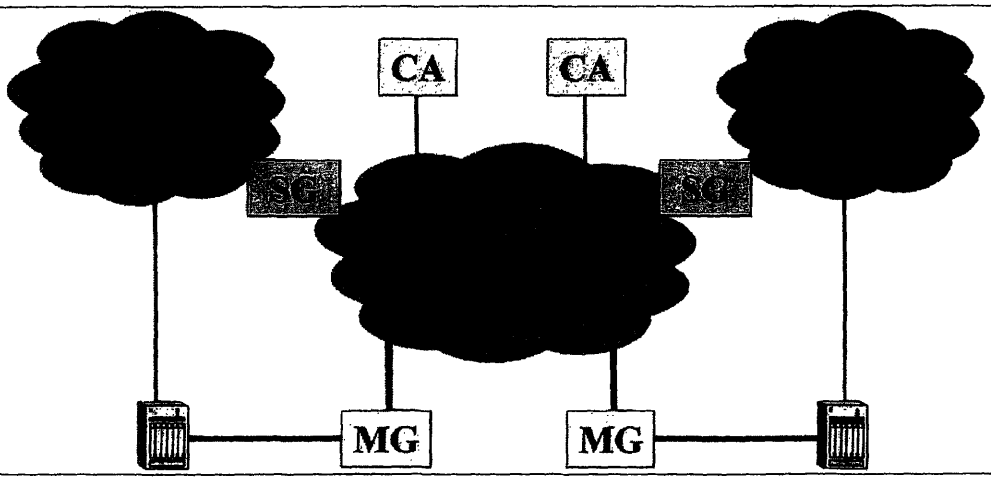


Figure 12 Master/Slave architecture involving call agents, signaling and media gateways.

PSTN vendors say IP telephony must replace the PSTN in such a way that the essential functions of the PSTN will continue to work throughout an extended migration period. This leads to two types of gateways. *Media Gateways* (MG) accept voice or "media" traffic from the circuit switches and packetize the voice to be transmitted over the IP network. *Signaling Gateways* (SG) connect the signaling (e.g., SS7) networks and IP networks, so that the call agents connected to the IP network can communicate with the circuit switches connected to the signaling networks, as diagrammed in Figure 12.

The MG allows connections between dissimilar networks by providing media conversion and/or transcoding functions. For example, an MG may receive packets from an IP network, depacketize them, transcode them, and pass the media stream to a switched circuit network. In some cases an MG may act like a switch in joining two terminations or resources of the same type. Hence, other functions that an MG could perform include a conference bridge with all packet interfaces, an interactive voice response unit, or a voice recognition system. An MG also supports resource functions including event notification, resource allocation and management, as well as system functions, such as establishing and maintaining an association with the Call Agent.

An SG function resides at the edge of the data network, relaying, translating or terminating call control signals between the packet data network and the circuit switched telephony network. An SS7-IP gateway would employ the SG function. On the other hand, the MG could also employ an SG function to process traditional telephony signaling associated with trunk or line terminations at the MG, such as the D channel of an ISDN BRI line or PRI trunk.

The call agent, which is often termed the "media gateway controller," (MGC)

must communicate with the media gateway to control its actions. Several protocols have been developed for this type of communication, including simple gateway control protocol (SGCP) [12], IP device control (IPDC) protocol, media gateway control protocol (MGCP) ([12], [4]), and Megaco/H.248 [13]. SGCP is the original ASCII string-based master-slave signaling protocol for VoIP. MGCP followed the following year, combining characteristics of SGCP and IPDC with more capabilities. Megaco is a similar protocol that the IETF has developed with still more capabilities.

Although the MGCP RFC was not a standards-track document, many vendors have implemented gateways and call agents using MGCP. It is also the basis for the network-based call signaling (NCS) protocol developed by the PacketCable group of Cable Labs [14]. There are several available implementations of NCS 1.0.

Both SCGP and MGCP are designed as distributed system protocols that give the user the appearance of a single VoIP system. They are stateless protocols in the sense that the sequence of transactions between the MG and the call agent can be performed without any memory of previous transactions. On the other hand, MGCP does require the MGC to keep call state.

Both MGCP and Megaco support the following media gateway functions:

- Create, modify and delete connections using any combination of transit network, including frame relay, ATM, TDM, Ethernet or analog. Connections can be established for transmission of audio packets over several types of bearer networks:
    - IP networks using RTP and/or UDP;

    - an internal connection, such as the TDM backplane or the interconnection bus of a gateway. This is used for connections that terminate in a gateway but are immediately rerouted over the telephone network ("hairpin" connections).

- Detect or generate events on end points or connections. For example, a gateway may detect dialed digits or generate a ringback tone on a connection.
- Collect digits according to a digit map received from the call agent, and send a complete set of dialed digits to the call agent.
- Allow mid-call changes, such as call hold, playing announcements, and conferencing.
- Report call statistics.

Aside from some differences in terminology, the Megaco protocol gives the call agent more flexibility of transport type and control over the media gateway, as well as some hooks for applications such as video conferencing. Both MGCP and Megaco provide a procedure for the call agent to send a package of properties, signals, or events. Megaco has a defined way for the call agent and the gateway to negotiate the version to be used, but MGCP does not have a version control mechanism, so one must rely on a vendor proprietary negotiation process.

In the areas of security and quality of service, Megaco is more flexible than MGCP. While MGCP supports only IPSEC, Megaco also supports an authentication header. Both protocols support authentication of the source address. While MGCP only supports UDP for signaling messages, Megaco supports UDP, TCP, ATM, and SCTP.

Megaco also has better stream management and resource allocation mechanisms.

Either MGCP or Megaco (or even SGCP or IPDC) may be used for a master-slave VoIP architecture, especially when the goal is to control many low-cost IP telephony gateways. For communications among call agents, or for control of trunk groups, SIP may be more appropriate. While MGCP and Megaco have specific verbs for VoIP call control, SIP allows a single primitive to be used to provide different services. Consequently, SIP offers the promise of supporting a wide range of services beyond basic telephony, including instant messaging, presence management, and voice-enabled web-based e-commerce, and SIP facilitates new application development by independent third parties. Some soft switch vendors use MGCP or Megaco to control gateways, but use SIP at the application layer [15].

Transport

Typical Internet applications use TCP/IP protocol for communication. Although IP is a connectionless best effort network communications protocol, TCP is a reliable transport protocol that uses acknowledgments and retransmission to ensure packet receipt. Used together, TCP/IP is a reliable connection-oriented network communications protocol suite. TCP/IP is not suitable for real-time communications, such as speech transmission, because the acknowledgment/retransmission feature would lead to excessive delays.

VoIP, therefore, uses a combination of RTP and UDP over IP. UDP provides unreliable connectionless delivery service using IP to transport messages between end points in an Internet. RTP, used in conjunction with UDP, provides end-to-end network transport functions for applications transmitting real-time data, such as audio and video, over unicast and multicast network services. RTP does not reserve resources and does not

guarantee quality of service. A companion protocol RTCP does allow monitoring of a link, but most VoIP applications offer a continuous stream of RTP/UDP/IP packet without regard to packet loss or delay in reaching the receiver.

Delay

Transmission time includes delay due to codec processing as well as propagation delay. ITU-T Recommendation G.114 [16] recommends the following one-way transmission time limits for connections with adequately controlled echo (complying with G.131 [17]):

- 0 to 150 ms: acceptable for most user applications;
- 150 to 400 ms: acceptable for international connections;
- > 400 ms: unacceptable for general network planning purposes; however, it is recognized that in some exceptional cases this limit will be exceeded.

Delay variation, sometimes called jitter, is also important. The receiving gateway or telephone must compensate for delay variation with a jitter buffer, which imposes a delay on early packets and passes late packets with less delay so that the decoded voice streams out of the receiver at a steady rate. Any packets that arrive later than the length of the jitter buffer are discarded. Since we want low packet loss, the jitter buffer delay is the maximum delay variation that we expect. This jitter buffer delay must be included in the total end-to-end delay that the listener experiences during a conversation using packet telephony.

Packetized voice has larger end-to-end delays than a TDM system, making the above delay objectives challenging. A sample on-net delay budget for the G.729 (8 kb/s) codec is shown in Table 2.

Delay Source	On-net Budget (ms)
Device Sample Capture	0.1
Encoding Delay (Algorithmic Depay + Processing Delay)	17.5
Packetization/Depackatization Delay	20
Move to Output Queue/Queue Delay	0.5
Access (up) Link Transmission Delay	10
Backbone Network Transmission Delay	Dnw
Access (down) Link Transmission Delay	10
Input Queue to Application	0.5
Jitter Buffer	60
Decoder Processing Delay	2
Device Playout Delay	0.5
Total	121.1 + Dnw

Table 2. Delay Budget

This budget is not precise. The allocated jitter buffer delay of 60 ms is only an estimate; the actual delay could be larger or smaller. Since the sample budget does not include any specific delays for header compression and decompression, we may consider that, if those functions are employed, the associated processing delay is lumped into the access link delay.

This delay budget allows us to stay within the G.114 guidelines, leaving 29 ms for the one-way backbone network delay (Dnw) in a national network. This is achievable in small countries. Network delays in the Asia Pacific region, as well as between North America and Asia, may be higher than 100 ms. According to G.114, these delays are acceptable for international links. However, the end-to-end delays for VoIP calls are considerably larger than for PSTN calls.

Voice Quality

There are various approaches to providing QoS in IP networks. However, the first question is whether QoS is really necessary. Some Internet engineers argue that if the

occupancy is low, then performance should be good. Essentially, the debate is over whether excess network capacity (including link bandwidth and routers) is less expensive than QoS implementation.

QoS can be achieved by managing router queues and by routing traffic around congested parts of the network. Two key QoS concepts are the IntServ [18] and DiffServ. The IntServ concept is to reserve resources for each flow through the network. RSVP [19] was originally designed to be the reservation protocol. When an application requests a specific QoS for its data stream, RSVP can be used to deliver the request to each router along the path and to maintain router state to provide the requested service. RSVP transmits two types of Flow Specs conforming to IntServ rules. The traffic specification (Tspec) describes the flow, and the service request specification (Rspec) describes the service requested under the assumption that the flow adheres to the Tspec. Current implementations of IntServ allow a choice of Guaranteed Service or Controlled-Load Service.

There are several reasons for not using IntServ with RSVP for IP telephony. Although IntServ with RSVP would work on a private network for small amounts of traffic, the large number of voice calls that IP telephony service providers carry on their networks would stress an IntServ RSVP system. First, the bandwidth required for voice itself is small, and the RSVP control traffic would be a significant part of the overall traffic. Second, RSVP router code was not designed to support many thousands of simultaneous connections per router[20].

Since IntServ with RSVP does not scale well to support many thousands of simultaneous connections, the IETF has developed a simpler framework and architecture

to support DiffServ [18]. The architecture achieves scalability by aggregating traffic into classifications that are conveyed by means of IP-layer packet marking using the DS field in IPv4 or IPv6 headers. Sophisticated classification, marking, policing, and shaping operations need only be implemented at network boundaries. The primary goal of differentiated services is to allow different levels of service to be provided for traffic streams on a common network infrastructure. A variety of resource management techniques may be used to achieve this, but the end result will be that some packets will receive different (e.g., better) service than others. This will, for example, allow service providers to offer a real-time service giving priority to the use of bandwidth and router queues, up to the configured amount of capacity allocated to real-time traffic. The appeal of DiffServ is that it is relatively simple (compared to IntServ), yet provides applications like VoIP some improvement in performance compared to "best-effort IP networks.

One more approach to achieving voice quality is to use MPLS. MPLS offers IP networks the capability to provide traffic engineering as well as a differentiated services approach to voice quality. For several decades, traffic engineering and automated rerouting of telephone traffic have increased the efficiency and reliability of the PSTN. Frame relay and ATM also offer source (or "explicit") routing capabilities that enable traffic engineering. It is possible to design an IP network to run on top of a frame relay or ATM ("Layer 2") network, providing some traffic engineering features, but this approach adds cost and operational complexity. MPLS offers IP networks the capability to provide traffic engineering as well as a differentiated services approach to voice quality.

A VoIP network designer can choose DiffServ, MPLS-TE plus DiffServ, or DS-TE according to the economics of the situation. If VoIP is to be a small portion of the

total traffic, DiffServ or MPLS-TE plus DiffServ may be sufficient. DS-TE promises more efficient use of an IP network carrying a large proportion of VoIP traffic, with perhaps more operational complexity[20].

Regulation

VoIP arrives on the communications scene at a time when telecommunications regulation has existed for nearly one hundred years. It is therefore important to understand the relevant regulations as they exist before discussing the challenges VoIP will pose. This section provides the necessary regulatory context and discusses the VoIP relevant regulations, as identified in the Federal Communications Commission's (FCC)[7] IP-Enabled Services Notice for Proposed Rulemaking[8]. Actual text of the Act is provided in a box, and can be skipped if so desired.

Statutory Definitions and Jurisdiction

Several definitions set forth in the Communications Act and prior Commission orders are relevant for understanding the VoIP context.

First, the Act defines the terms "common carrier" and "carrier" to include "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio." The Act specifically excludes persons "engaged in radio broadcasting" from this definition[9].

The Federal Communications Commission has long distinguished between "basic" and "enhanced" service offerings. In the *Computer Inquiry* line of decisions[10], the

---

[7] Hereafter "the Commission."
[8] IP-Enabled Services Notice for Proposed Rulemaking, FCC Docket No. 04-36.
[9] 47 U.S.C. § 153(10).
[10] *See Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication*

Commission specified that a "basic" service is a service offering transmission capacity for the delivery of information without net change in form or content. Providers of "basic" services were subjected to common carrier regulation under Title II of the Act. By contrast, an "enhanced" service contains a basic service component but also "employ[s] computer processing applications that act on the format, content, code, protocol or similar aspects of the subscriber's transmitted information; provide the subscriber additional, different, or restructured information; or involve subscriber interaction with stored information[11]."

The Commission concluded that enhanced services were subject to the Commission's jurisdiction[12]. It further found, however, that the enhanced service market was highly competitive with low barriers to entry; therefore, the Commission declined to treat providers of enhanced services as "common carriers" subject to regulation under Title II of the Act[13].

Services and Facilities, Docket No. 16979, Notice of Inquiry, 7 FCC 2d 11 (1966) (*Computer I NOI*); *Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities*, Docket No. 16979, Final Decision and Order, 28 FCC 2d 267 (1971) (*Computer I Final Decision*); *Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry)*, Docket No. 20828, Tentative Decision and Further Notice of Inquiry and Rulemaking, 72 FCC 2d 358 (1979) (*Computer II Tentative Decision*); *Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry)*, Docket No. 20828, Final Decision, 77 FCC 2d 384 (1980) (*Computer II Final Decision*); *Amendment of Section 64.702 of the Commission's Rules and Regulations (Third Computer Inquiry)*, CC Docket No. 85-229, Report and Order, 104 FCC 2d 958 (1986) (*Computer III*) (subsequent cites omitted) (collectively the *Computer Inquiries*).

[11] 47 C.F.R. § 64.702; *see also Computer II Final Decision*, 77 FCC 2d at 420-21, para. 97.

[12] *Computer II Final Decision*, 77 FCC 2d at 432, para. 125.

[13] *Id.* at 432-35, paras. 126-132.

The 1996 Act defined "telecommunications" to mean "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received[14]."

The 1996 Act also defined "telecommunications service" to mean "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available to the public, regardless of facilities used[15]." The Commission has concluded, and courts have agreed, that the "telecommunications service" definition was "intended to clarify that telecommunications services are common carrier services[16]."

Various entitlements and obligations set forth in the Act – including, for example, the entitlement to access an incumbent's unbundled network elements for local service[17] and the obligation to render a network accessible to people with disabilities[18] – attach only to entities providing "telecommunications service."

By contrast, the 1996 Act defined "information service" to mean "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the

---

[14] 47 U.S.C. § 153(43).
[15] 47 U.S.C. § 153(46).

[16] *Cable & Wireless, PLC,* Order, 12 FCC Rcd 8516, 8521, para. 13 (1997); *see also Virgin Islands Tel. Corp. v. FCC,* 198 F.3d 921, 926-27 (D.C. Cir. 1999).

[17] *See* 47 U.S.C. § 251(c)(3).
[18] *See* 47 U.S.C. § 255(c).

management, control, or operation of a telecommunications network or the management of a telecommunications service[19]."

The Act did not establish any particular entitlements or requirements with regard to providers of information services, but the Commission has exercised its ancillary authority under Title I of the Act to apply requirements to information services[20].

In a 1998 Report to Congress known as the "Stevens Report[21],"the Commission considered the proper classification of IP telephony services under the 1996 Act. In that Report, the Commission declined to render any conclusions regarding the proper legal and regulatory framework for addressing these services, stating "definitive pronouncements" would be inappropriate "in the absence of a more complete record focused on individual service offerings[22]."

The Commission did, however, observe that in the case of "computer-to-computer" IP telephony, where "individuals use software and hardware at their premises to place calls between two computers connected to the Internet," the Internet service

---

[19] 47 U.S.C. § 153(20). "Information service" category includes all services that the Commission previously considered to be "enhanced services." *See Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, CC Docket No. 96-149.

[20] *See, e.g., Implementation of Section 255 and 251(a)(2) of the Communications Act of 1934, as Enacted by the Telecommunications Act of 1996*, WT Docket No. 96-198, Report and Order and Further Notice of Inquiry, 16 FCC Rcd 6417, 6455-62, paras. 93-108 (1999) (*Disability Access Order*) (invoking ancillary authority to impose section 255-like obligations on providers of voicemail and interactive menu services); *see also Computer II Final Decision; Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry)*, Memorandum Opinion and Order, 84 FCC 2d 50 (1980) (*Computer II Reconsideration Decision*); *Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry)*, Memorandum Opinion and Order on Further Reconsideration, 88 FCC 2d 512 (1981) (*Computer II Further Reconsideration Decision*) (asserting ancillary jurisdiction over enhanced services, including voicemail and interactive menus, as well as over CPE).

[21] *Federal-State Joint Board on Universal Service*, CC Docket No. 96-45, Report to Congress, 13 FCC Rcd 11501 (1998) (*Stevens Report*).

[22] *See id.* at 11541, para. 83.

provider did not appear to be "providing" telecommunications, and the service therefore appeared not to constitute "telecommunications service" under the Act's definition of that term. In contrast, a "phone-to-phone" IP telephony service relying on "dial-up or dedicated circuits ... to originate or terminate Internet-based calls" appeared to "bear the characteristics of 'telecommunications services[23],'" so long as the particular service met four criteria: (1) it holds itself out as providing voice telephony or facsimile transmission service; (2) it does not require the customer to use CPE different from that CPE necessary to place an ordinary touchtone call (or facsimile transmission) over the public switched telephone network; (3) it allows the customer to call telephone numbers assigned in accordance with the North American Numbering Plan, and associated international agreements; and (4) it transmits customer information without net change in form or content[24].

911/E911

Under the Commission's rules, there are two sets of requirements for 911. The first set, "basic 911," requires covered carriers to deliver all 911 calls to the appropriate public safety answering point (PSAP) or designated statewide default answering point[25]. Basic 911 service does not address what sort of information the PSAP should receive from that call; rather it seeks to ensure the delivery of 911 calls.

The Commission, therefore, also adopted requirements for covered wireless carriers to be capable of delivering the calling party's callback number and the calling

---

[23] Id. at 11544, para. 89.
[24] Id. at 11543-44, para. 88.
[25] 47 C.F.R. §§ 20.18(b), 64.3001.

party's location information[26]. These rules, referred to as the Commission's "enhanced 911" (E911) rules, are currently being phased in across the country and deployment of E911 capability is ongoing.

The *E911 Scope Order* states that the Commission has statutory authority under Sections 1, 4(i), and 251(e)(3) of the Act to determine what entities should be subject to the Commission's 911 and E911 rules. However, the FCC in the IP-Enabled Services NPRM[27] stated that "in deciding whether to exercise our regulatory authority in the context of IP-enabled services, we are mindful that development and deployment of these services is in its early stages, that these services are fast-changing and likely to evolve in ways that we cannot anticipate, and that imposition of regulatory mandates, particularly those that impose technical mandates, should be undertaken with caution."

§ 615. Support for universal emergency telephone number

The Federal Communications Commission shall encourage and support efforts by States to deploy comprehensive end-to-end emergency communications infrastructure and programs, based on coordinated statewide plans, including seamless, ubiquitous, reliable wireless telecommunications networks and enhanced wireless 9-1-1 service. In encouraging and supporting that deployment, the Commission shall consult and cooperate with State and local officials responsible for emergency services and public safety, the telecommunications industry (specifically including the cellular and other wireless telecommunications service providers), the motor vehicle manufacturing industry, emergency medical service providers and emergency dispatch providers, transportation officials, special 9-1-1 districts, public safety, fire service and law enforcement officials, consumer groups, and hospital emergency and trauma care personnel (including emergency physicians, trauma surgeons, and nurses). The Commission shall encourage each State to develop and implement coordinated statewide deployment plans, through an entity designated by the governor, and to include representatives of the foregoing organizations and entities in development and implementation of such plans. Nothing in this section shall be construed to authorize or require the Commission to impose obligations or costs on any person.

[26] *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102, RM 8143, Report and Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd 18676, 18689-18722, paras. 24-91 (1996).

[27] IP-Enabled Services Notice for Proposed Rulemaking, FCC Docket No. 04-36.

§ 615a. Parity of protection for provision or use of wireless service

(a) Provider parity
A wireless carrier, and its officers, directors, employees, vendors, and agents, shall have immunity or other protection from liability in a State of a scope and extent that is not less than the scope and extent of immunity or other protection from liability that any local exchange company, and its officers, directors, employees, vendors, or agents, have under Federal and State law (whether through statute, judicial decision, tariffs filed by such local exchange company, or otherwise) applicable in such State, including in connection with an act or omission involving the release to a PSAP, emergency medical service provider or emergency dispatch provider, public safety, fire service or law enforcement official, or hospital emergency or trauma care facility of subscriber information related to emergency calls or emergency services.

(b) User parity
A person using wireless 9-1-1 service shall have immunity or other protection from liability of a scope and extent that is not less than the scope and extent of immunity or other protection from liability under applicable law in similar circumstances of a person using 9-1-1 service that is not wireless.

(c) PSAP parity
In matters related to wireless 9-1-1 communications, a PSAP, and its employees, vendors, agents, and authorizing government entity (if any) shall have immunity or other protection from liability of a scope and extent that is not less than the scope and extent of immunity or other protection from liability under applicable law accorded to such PSAP, employees, vendors, agents, and authorizing government entity, respectively, in matters related to 9-1-1 communications that are not wireless.

(d) Basis for enactment
This section is enacted as an exercise of the enforcement power of the Congress under section 5 of the Fourteenth Amendment to the Constitution and the power of the Congress to regulate commerce with foreign nations, among the several States, and with Indian tribes.

§ 615b. Definitions

As used in this Act:

(1) Secretary
The term "Secretary" means the Secretary of Transportation.

(2) State
The term "State" means any of the several States, the District of Columbia, or any territory or possession of the United States.

(3) Public safety answering point; PSAP
The term "public safety answering point" or "PSAP" means a facility that has been designated to receive 9-1-1 calls and route them to emergency service personnel.

(4) Wireless carrier
The term "wireless carrier" means a provider of commercial mobile services or any

other radio communications service that the Federal Communications Commission requires to provide wireless 9-1-1 service.

(5) Enhanced wireless 9-1-1 service
The term "enhanced wireless 9-1-1 service" means any enhanced 9-1-1 service so designated by the Federal Communications Commission in the proceeding entitled "Revision of the Commission's Rules to Ensure Compatibility with Enhanced 9-1-1 Emergency Calling Systems" (CC Docket No. 94-102; RM-8143), or any successor proceeding.

(6) Wireless 9-1-1 service
The term "wireless 9-1-1 service" means any 9-1-1 service provided by a wireless carrier, including enhanced wireless 9-1-1 service.

(7) Emergency dispatch providers
The term "emergency dispatch providers" shall include governmental and nongovernmental providers of emergency dispatch services.

CALEA

In the *Second Report and Order* ("*Second R&O*"), the Commission concluded that the language and legislative history of CALEA provide sufficient guidance as to what the term "telecommunications carrier" means, such that it can be applied to particular carriers, their offerings and facilities.[28] The *Second R&O* further stated that CALEA does not apply to certain entities and services, *e.g.* information services and private network services. Additionally, the *Second R&O* stated that CALEA's definitions of "telecommunications carrier" and "information services" were not modified by the Telecommunications Act of 1996, and that the CALEA definitions therefore remain in force. The *Second R&O* concluded as a matter of law that the entities and services

[28]Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, Second Report and Order, 15 FCC Rcd 7105 (2000), at 7110, ¶ 9. The Second R&O stated that the legislative history contains examples of the types of service providers subject to CALEA: "The definition of 'telecommunications carrier' includes such service providers as local exchange carriers, interexchange carriers, competitive access providers, cellular carriers, providers of personal communications services, satellite-based service providers, cable operators, and electric and other utilities that provide telecommunications services for hire to the public, and any other wireline or wireless service for hire to the public." Id. at 7111, ¶ 10, citing 140 Cong. Rec. H-10779 (daily ed. October 7, 1994) (statement of Rep. Hyde). See also H.R. Rep. No. 103-827(I), at 23, reprinted in 1994 U.S.C.C.A.N. 3489, 3500.

subject to CALEA must be based on the CALEA definitions, independently of their classification for the separate purposes of the Communications Act[29].

Section 103 of CALEA establishes four general "assistance capability requirements" that telecommunications carriers must meet to achieve compliance with CALEA.[30] Subsection 103(a) requires, in pertinent part, that a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of:

(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably

---

[29] Id. at 7112, ¶ 13. The Commission later clarified, in an Order on Reconsideration of the Second R&O, the CALEA obligations of resellers who rely on the facilities of an underlying carrier that does not provide telecommunications service for purposes of CALEA. Specifically, the Commission stated that under such circumstances, a non-facilities based reseller of telecommunications services is not exempt from "its overall obligation to ensure that its services satisfy all the assistance capability requirements of section 103." Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, Second Order on Reconsideration, 16 FCC Rcd 8959 (2001) at 8971, ¶ 37. The Commission also noted that when "a reseller does not resell the services of a facilities-based carrier subject to CALEA, it can contract with its facilities provider or third parties for CALEA assistance capabilities in the same way it contracts for any other network capabilities." Id. at 8971, ¶ 38.

[30]Section 103(a)(1)-(4) of CALEA, 47 U.S.C. § 1002(a)(1)-(4).

available[31] to the carrier (a) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government) and (b) in a manner that allows it to be associated with the communication to which it pertains;

(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects (a) the privacy and security of communications and call-identifying information not authorized to be intercepted and (b) information regarding the government's interception of communications and access to call-identifying information.[32]

Section 104 of CALEA sets forth notices of maximum and actual capacity requirements to accommodate all electronic surveillance events that telecommunications carriers may need to conduct for LEAs.

Section 109 of CALEA addresses the payment of costs by the Attorney General to telecommunications carriers who comply with the capability requirements of section 103.

---

[31]CALEA does not define or interpret the term "reasonably available."

[32]47 U.S.C. § 1002(a)(1)-(4). "Call-identifying information" is defined in section 102(2) of CALEA as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2). For a discussion of call-identifying information, *see, supra.*

The statute distinguishes between equipment, facilities and services installed or deployed on or before January 1, 1995, and after that date.

§ 1001. Definitions

For purposes of this subchapter--

(1) The terms defined in section 2510 of Title 18 have, respectively, the meanings stated in that section.

(2) The term "call-identifying information" means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.

(3) The term "Commission" means the Federal Communications Commission.

(4) The term "electronic messaging services" means software-based services that enable the sharing of data, images, sound, writing, or other information among

(6) The term "information services"--

(A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and

(B) includes--

(i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities;

(ii) electronic publishing; and

(iii) electronic messaging services; but

(C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network.

(7) The term "telecommunications support services" means a product, software, or service used by a telecommunications carrier for the internal signaling or switching functions of its telecommunications network.

(8) The term "telecommunications carrier"--

(A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and

(B) includes--

(i) a person or entity engaged in providing commercial mobile service (as defined in section 332(d) of this title); or

(ii) a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this subchapter; but

(C) does not include--

(i) persons or entities insofar as they are engaged in providing information services; and

(ii) any class or category of telecommunications carriers that the Commission exempts by rule after consultation with the Attorney General.

§ 1002. Assistance capability requirements

(a) Capability requirements

Except as provided in subsections (b), (c), and (d) of this section and sections 1007(a) and 1008(b) and (d) of this title, a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of--

(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier--

(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and

(B) in a manner that allows it to be associated with the communication to which it pertains,

except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);

(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects--

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and

(B) information regarding the government's interception of communications and access to call-identifying information.

(b) Limitations

(1) Design of features and systems configurations

This subchapter does not authorize any law enforcement agency or officer--

(A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or

(B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

(2) Information services; private networks and interconnection services and facilities

The requirements of subsection (a) of this section do not apply to--

(A) information services; or

(B) equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.

(3) Encryption

A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

(c) Emergency or exigent circumstances

In emergency or exigent circumstances (including those described in sections 2518(7) or (11)(b) and 3125 of Title 18 and section 1805(e) of Title 50), a carrier at its discretion may comply with subsection (a)(3) of this section by allowing monitoring at its premises if that is the only means of accomplishing the interception or access.

(d) Mobile service assistance requirements

A telecommunications carrier that is a provider of commercial mobile service (as defined in section 332(d) of this title) offering a feature or service that allows subscribers to redirect, hand off, or assign their wire or electronic communications to another service area or another service provider or to utilize facilities in another service area or of another service provider shall ensure that, when the carrier that had been providing assistance for the interception of wire or electronic communications or access to call-identifying information pursuant to a court order or lawful authorization no longer has access to the content of such communications or call-identifying information within the service area in which interception has been occurring as a result of the subscriber's use of such a feature or service, information is made available to the government (before, during, or immediately after the transfer of such communications) identifying the provider of a wire or electronic communication service that has acquired access to the communications.

§ 1004. Systems security and integrity

A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.

§ 1008. Payment of costs of telecommunications carriers to comply with capability requirements

(a) Equipment, facilities, and services deployed on or before January 1, 1995

The Attorney General may, subject to the availability of appropriations, agree to pay telecommunications carriers for all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995, to establish the capabilities necessary to comply with section 1002 of this title.

(b) Equipment, facilities, and services deployed after January 1, 1995

(1) Determinations of reasonably achievable

The Commission, on petition from a telecommunications carrier or any other interested person, and after notice to the Attorney General, shall determine whether compliance with the assistance capability requirements of section 1002 of this title is reasonably achievable with respect to any equipment, facility, or service installed or deployed after January 1, 1995. The Commission shall make such determination within 1 year after the date such petition is filed. In making such determination, the Commission shall determine whether compliance would impose significant difficulty or expense on the carrier or on the users of the carrier's systems and shall consider the following factors:

(A) The effect on public safety and national security.

(B) The effect on rates for basic residential telephone service.

(C) The need to protect the privacy and security of communications not authorized to be intercepted.

(D) The need to achieve the capability assistance requirements of section 1002 of this title by cost-effective methods.

(E) The effect on the nature and cost of the equipment, facility, or service at issue.

(F) The effect on the operation of the equipment, facility, or service at issue.

(G) The policy of the United States to encourage the provision of new technologies and services to the public.

(H) The financial resources of the telecommunications carrier.

(I) The effect on competition in the provision of telecommunications services.

(J) The extent to which the design and development of the equipment, facility, or service was initiated before January 1, 1995.

(K) Such other factors as the Commission determines are appropriate.

(2) Compensation

If compliance with the assistance capability requirements of section 1002 of this title is not reasonably achievable with respect to equipment, facilities, or services deployed after January 1, 1995--

(A) the Attorney General, on application of a telecommunications carrier, may agree, subject to the availability of appropriations, to pay the telecommunications carrier for the additional reasonable costs of making compliance with such assistance capability requirements reasonably achievable; and

(B) if the Attorney General does not agree to pay such costs, the telecommunications carrier shall be deemed to be in compliance with such capability requirements.

(c) Allocation of funds for payment

The Attorney General shall allocate funds appropriated to carry out this subchapter in accordance with law enforcement priorities determined by the Attorney General.

(d) Failure to make payment with respect to equipment, facilities, and services deployed on or before January 1, 1995

If a carrier has requested payment in accordance with procedures promulgated pursuant to subsection (e) of this section, and the Attorney General has not agreed to pay the telecommunications carrier for all reasonable costs directly associated with modifications necessary to bring any equipment, facility, or service deployed on or before January 1, 1995, into compliance with the assistance capability requirements of

section 1002 of this title, such equipment, facility, or service shall be considered to be in compliance with the assistance capability requirements of section 1002 of this title until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modification.

(e) Cost control regulations

(1) In general

The Attorney General shall, after notice and comment, establish regulations necessary to effectuate timely and cost-efficient payment to telecommunications carriers under this subchapter, under chapters 119 and 121 of Title 18, and under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(2) Contents of regulations

The Attorney General, after consultation with the Commission, shall prescribe regulations for purposes of determining reasonable costs under this subchapter. Such regulations shall seek to minimize the cost to the Federal Government and shall--

(A) permit recovery from the Federal Government of--

(i) the direct costs of developing the modifications described in subsection (a) of this section, of providing the capabilities requested under subsection (b)(2) of this section, or of providing the capacities requested under section 1003(e) of this title, but only to the extent that such costs have not been recovered from any other governmental or nongovernmental entity;

(ii) the costs of training personnel in the use of such capabilities or capacities; and

(iii) the direct costs of deploying or installing such capabilities or capacities;

(B) in the case of any modification that may be used for any purpose other than lawfully authorized electronic surveillance by a law enforcement agency of a government, permit recovery of only the incremental cost of making the modification suitable for such law enforcement purposes; and

(C) maintain the confidentiality of trade secrets.

(3) Submission of claims

Such regulations shall require any telecommunications carrier that the Attorney General has agreed to pay for modifications pursuant to this section and that has installed or deployed such modification to submit to the Attorney General a claim for payment that contains or is accompanied by such information as the Attorney General may require.

Disability Access

In September 1999, the Commission issued an order adopting rules to implement sections 255 and 251(a)(2) (*Disability Access Order*)[33], which included a Notice of Inquiry

[33] Disability Access Order, 16 FCC Rcd 6417. Among other things, the Commission (1) required manufacturers and service providers to develop processes to evaluate the accessibility, usability, and compatibility of covered services and equipment, see Disability Access Order, 16 FCC Rcd at 6429-33, paras. 21-30; (2) required manufacturers and service providers to ensure that information and documentation provided in connection with equipment or service be accessible to people with disabilities, where readily achievable, and that employee training, where provided at all, account for accessibility

regarding, among other things, section 255's applicability in the context of "Internet telephony" and "computer-based equipment that replicates telecommunications functionality."

In the IP Enabled Services NPRM, the FCC noted that, "in the *Disability Access Order*, the Commission relied on Title I to apply section 255 obligations to providers of voicemail and interactive menu services, both of which were deemed "information services," and asked if that approach will be appropriate with regard to any providers of VoIP or other IP-enabled services that we deem to be "information services"?

Section 225 of the Communications Act requires common carriers offering voice telephone service to also provide Telecommunications Relay Service (TRS) so that persons with disabilities will have equal access to the telecommunications network. Beyond traditional TRS, which requires the use of a teletypewriter (TTY), the Commission has implemented this mandate by determining that two IP-enabled services, IP Relay and Video Relay Service (VRS), are forms of TRS[34]. In both scenarios, the

---

requirements, see id.; (3) required the maximum feasible deployment of accessibility features that can be incorporated into product design, see id. at 6440-42, paras. 49-54; and (4) prohibited telecommunications carriers from installing network features, functions, or capabilities that do not comply with the accessibility requirements set forth elsewhere in the Order, see id. at 6435-37, paras. 37-42.

[34] IP Relay functions in a similar manner to traditional TRS except that instead of a TTY, which is generally linked to the PSTN, the text is provided to, and received from, the communications assistant (CA) via the TRS consumer's computer or other Internet-enabled device. *See generally Provision of Improved Telecommunications Relay Services and Speech-To-Speech Services for Individuals with Hearing and Speech Disabilities; Petition for Clarification of WorldCom, Inc.*, CC Docket No. 98-67, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 17 FCC Rcd 7779 (2002) (*IP Relay Order*). TRS is a telecommunications relay service that allows persons with hearing or speech disabilities who use sign language to communicate with the CA in sign language (rather than by text) through video equipment. A video link allows the CA to view and interpret the party's signed conversation (and vice versa), and then relay the conversation back and forth with the other party to the call (the voice caller). In almost all cases, the video link is provided over the Internet. *See Improved TRS Order & FNPRM*, 15 FCC Rcd at 5152-54, paras. 21-27.

Commission determined that TRS, as defined, was not limited to "telecommunications" and that Congress intended the term "telephone transmission services" to be interpreted broadly to implement section 225's goal to "ensure that interstate and intrastate [TRS] are available, to the extent possible and in the most efficient manner, to hearing-impaired and speech-impaired individuals in the United States."

§ 610. Telephone service for disabled

(a) Establishment of regulations
The Commission shall establish such regulations as are necessary to ensure reasonable access to telephone service by persons with impaired hearing.

(b) Hearing aid compatibility requirements

(1) Except as provided in paragraphs (2) and (3), the Commission shall require that--

(A) all essential telephones, and
(B) all telephones manufactured in the United States (other than for export) more than one year after August 16, 1988, or imported for use in the United States more than one year after August 16, 1988,

provide internal means for effective use with hearing aids that are designed to be compatible with telephones which meet established technical standards for hearing aid compatibility.

(2)(A) The initial regulations prescribed by the Commission under paragraph (1) of this subsection after August 16, 1988, shall exempt from the requirements established pursuant to paragraph (1)(B) of this subsection only--

(i) telephones used with public mobile services;
(ii) telephones used with private radio services;
(iii) cordless telephones; and
(iv) secure telephones.

(B) The exemption provided by such regulations for cordless telephones shall not apply with respect to cordless telephones manufactured or imported more than three years after August 16, 1988.

(C) The Commission shall periodically assess the appropriateness of continuing in

effect the exemptions provided by such regulations for telephones used with public mobile services and telephones used with private radio services. The Commission shall revoke or otherwise limit any such exemption if the Commission determines that--

(i) such revocation or limitation is in the public interest;
(ii) continuation of the exemption without such revocation or limitation would have an adverse effect on hearing-impaired individuals;
(iii) compliance with the requirements of paragraph (1)(B) is technologically feasible for the telephones to which the exemption applies; and
(iv) compliance with the requirements of paragraph (1)(B) would not increase costs to such an extent that the telephones to which the exemption applies could not be successfully marketed.

(3) The Commission may, upon the application of any interested person, initiate a proceeding to waive the requirements of paragraph (1)(B) of this subsection with respect to new telephones, or telephones associated with a new technology or service. The Commission shall not grant such a waiver unless the Commission determines, on the basis of evidence in the record of such proceeding, that such telephones, or such technology or service, are in the public interest, and that (A) compliance with the requirements of paragraph (1)(B) is technologically infeasible, or (B) compliance with such requirements would increase the costs of the telephones, or of the technology or service, to such an extent that such telephones, technology, or service could not be successfully marketed. In any proceeding under this paragraph to grant a waiver from the requirements of paragraph (1)(B), the Commission shall consider the effect on hearing-impaired individuals of granting the waiver. The Commission shall periodically review and determine the continuing need for any waiver granted pursuant to this paragraph.

(4) For purposes of this subsection--

(A) the term "essential telephones" means only coin-operated telephones, telephones provided for emergency use, and other telephones frequently needed for use by persons using such hearing aids;
(B) the term "public mobile services" means air-to-ground radiotelephone services, cellular radio telecommunications services, offshore radio, rural radio service, public land mobile telephone service, and other common carrier radio communication services covered by part 22 of title 47 of the Code of Federal Regulations;
(C) the term "private radio services" means private land mobile radio services and other communications services characterized by the Commission in its rules as private radio services; and
(D) the term "secure telephones" means telephones that are approved by the United States Government for the transmission of classified or sensitive voice communications.

(c) Technical standards

The Commission shall establish or approve such technical standards as are required to enforce this section.

(d) Labeling of packaging materials for equipment

The Commission shall establish such requirements for the labeling of packaging materials for equipment as are needed to provide adequate information to consumers on the compatibility between telephones and hearing aids.

(e) Costs and benefits; encouragement of use of currently available technology

In any rulemaking to implement the provisions of this section, the Commission shall specifically consider the costs and benefits to all telephone users, including persons with and without hearing impairments. The Commission shall ensure that regulations adopted to implement this section encourage the use of currently available technology and do not discourage or impair the development of improved technology.

(f) Periodic review of regulations; retrofitting

The Commission shall periodically review the regulations established pursuant to this section. Except for coin-operated telephones and telephones provided for emergency use, the Commission may not require the retrofitting of equipment to achieve the purposes of this section.

(g) Recovery of reasonable and prudent costs

Any common carrier or connecting carrier may provide specialized terminal equipment needed by persons whose hearing, speech, vision, or mobility is impaired. The State commission may allow the carrier to recover in its tariffs for regulated service reasonable and prudent costs not charged directly to users of such equipment.

(h) State enforcement

The Commission shall delegate to each State commission the authority to enforce within such State compliance with the specific regulations that the Commission issues under subsections (a) and (b) of this section, conditioned upon the adoption and enforcement of such regulations by the State commission.

47 U.S.C.A. § 225

§ 225. Telecommunications services for hearing-impaired and speech-impaired individuals

(a) Definitions
As used in this section--

(1) Common carrier or carrier

The term "common carrier" or "carrier" includes any common carrier engaged in interstate communication by wire or radio as defined in section 153 of this title and any common carrier engaged in intrastate communication by wire or radio, notwithstanding sections 152(b) and 221(b) of this title.

(2) TDD

The term "TDD" means a Telecommunications Device for the Deaf, which is a machine that employs graphic communication in the transmission of coded signals through a wire or radio communication system.

(3) Telecommunications relay services

The term "telecommunications relay services" means telephone transmission services that provide the ability for an individual who has a hearing impairment or speech impairment to engage in communication by wire or radio with a hearing individual in a manner that is functionally equivalent to the ability of an individual who does not have a hearing impairment or speech impairment to communicate using voice communication services by wire or radio. Such term includes services that enable two-way communication between an individual who uses a TDD or other nonvoice terminal device and an individual who does not use such a device.

(b) Availability of telecommunications relay services

(1) In general

In order to carry out the purposes established under section 151 of this title, to make available to all individuals in the United States a rapid, efficient nationwide communication service, and to increase the utility of the telephone system of the Nation, the Commission shall ensure that interstate and intrastate telecommunications relay services are available, to the extent possible and in the most efficient manner, to hearing-impaired and speech-impaired individuals in the United States.

(2) Use of general authority and remedies

For the purposes of administering and enforcing the provisions of this section and the regulations prescribed thereunder, the Commission shall have the same authority, power, and functions with respect to common carriers engaged in intrastate communication as the Commission has in administering and enforcing the provisions of this subchapter with respect to any common carrier engaged in interstate communication. Any violation of this section by any common carrier engaged in intrastate communication shall be subject to the same remedies, penalties, and procedures as are applicable to a violation of this chapter by a common carrier engaged in interstate communication.

(c) Provision of services

Each common carrier providing telephone voice transmission services shall, not

later than 3 years after July 26, 1990, provide in compliance with the regulations prescribed under this section, throughout the area in which it offers service, telecommunications relay services, individually, through designees, through a competitively selected vendor, or in concert with other carriers. A common carrier shall be considered to be in compliance with such regulations--

(1) with respect to intrastate telecommunications relay services in any State that does not have a certified program under subsection (f) of this section and with respect to interstate telecommunications relay services, if such common carrier (or other entity through which the carrier is providing such relay services) is in compliance with the Commission's regulations under subsection (d) of this section; or

(2) with respect to intrastate telecommunications relay services in any State that has a certified program under subsection (f) of this section for such State, if such common carrier (or other entity through which the carrier is providing such relay services) is in compliance with the program certified under subsection (f) of this section for such State.

(d) Regulations

(1) In general

The Commission shall, not later than 1 year after July 26, 1990, prescribe regulations to implement this section, including regulations that--

(A) establish functional requirements, guidelines, and operations procedures for telecommunications relay services;

(B) establish minimum standards that shall be met in carrying out subsection (c) of this section;

(C) require that telecommunications relay services operate every day for 24 hours per day;

(D) require that users of telecommunications relay services pay rates no greater than the rates paid for functionally equivalent voice communication services with respect to such factors as the duration of the call, the time of day, and the distance from point of origination to point of termination;

(E) prohibit relay operators from failing to fulfill the obligations of common carriers by refusing calls or limiting the length of calls that use telecommunications relay services;

(F) prohibit relay operators from disclosing the content of any relayed conversation and from keeping records of the content of any such conversation beyond the duration of the call; and

(G) prohibit relay operators from intentionally altering a relayed conversation.

(2) Technology

The Commission shall ensure that regulations prescribed to implement this section encourage, consistent with section 157(a) of this title, the use of existing technology and do not discourage or impair the development of improved technology.

(3) Jurisdictional separation of costs

(A) In general

Consistent with the provisions of section 410 of this title, the Commission shall prescribe regulations governing the jurisdictional separation of costs for the services provided pursuant to this section.

(B) Recovering costs

Such regulations shall generally provide that costs caused by interstate telecommunications relay services shall be recovered from all subscribers for every interstate service and costs caused by intrastate telecommunications relay services shall be recovered from the intrastate jurisdiction. In a State that has a certified program under subsection (f) of this section, a State commission shall permit a common carrier to recover the costs incurred in providing intrastate telecommunications relay services by a method consistent with the requirements of this section.

(e) Enforcement

(1) In general

Subject to subsections (f) and (g) of this section, the Commission shall enforce this section.

(2) Complaint

The Commission shall resolve, by final order, a complaint alleging a violation of this section within 180 days after the date such complaint is filed.

(f) Certification

(1) State documentation

Any State desiring to establish a State program under this section shall submit documentation to the Commission that describes the program of such State for implementing intrastate telecommunications relay services and the procedures and remedies available for enforcing any requirements imposed by the State program.

(2) Requirements for certification

After review of such documentation, the Commission shall certify the State program if the Commission determines that--

(A) the program makes available to hearing-impaired and speech-impaired individuals, either directly, through designees, through a competitively selected vendor, or through regulation of intrastate common carriers, intrastate telecommunications relay services in such State in a manner that meets or exceeds the requirements of regulations prescribed by the Commission under subsection (d) of this section; and

(B) the program makes available adequate procedures and remedies for enforcing the requirements of the State program.

(3) Method of funding

Except as provided in subsection (d) of this section, the Commission shall not refuse to certify a State program based solely on the method such State will implement for funding intrastate telecommunication relay services.

(4) Suspension or revocation of certification

The Commission may suspend or revoke such certification if, after notice and opportunity for hearing, the Commission determines that such certification is no longer warranted. In a State whose program has been suspended or revoked, the Commission shall take such steps as may be necessary, consistent with this section, to ensure continuity of telecommunications relay services.

(g) Complaint

(1) Referral of complaint

If a complaint to the Commission alleges a violation of this section with respect to intrastate telecommunications relay services within a State and certification of the program of such State under subsection (f) of this section is in effect, the Commission shall refer such complaint to such State.

(2) Jurisdiction of Commission

After referring a complaint to a State under paragraph (1), the Commission shall exercise jurisdiction over such complaint only if--

(A) final action under such State program has not been taken on such complaint by such State--

(i) within 180 days after the complaint is filed with such State; or

(ii) within a shorter period as prescribed by the regulations of such State; or

(B) the Commission determines that such State program is no longer qualified for certification under subsection (f) of this section.

Universal Service

Regulatory classification of VoIP is only one among many issues that would affect the FCC's ability to continue to fund Universal Service. Section 254(d) of the Telecommunications Act states that "[e]very telecommunications carrier that provides interstate telecommunications services *shall* contribute" to universal service. This section

is often referred to as the Commission's mandatory contribution authority. In the *Wireline Broadband NPRM*, the Commission sought comment on whether facilities-based broadband Internet access providers are required to contribute, pursuant to its mandatory authority[35], or should be required to contribute to universal service, pursuant to its permissive authority[36], which states that "[a]ny other provider of interstate Telecommunications may be required to contribute ... if the public interest so requires." This section is often referred to as the Commission's permissive contribution authority.

In the IP Enabled Services, this enquire is further burdened by asking if the contribution obligations of both facilities-based and non-facilities-based providers of IP-enabled services.

§ 254. Universal service

(a) Procedures to review universal service requirements

(1) Federal-State Joint Board on universal service

Within one month after February 8, 1996, the Commission shall institute and refer to a Federal-State Joint Board under section 410(c) of this title a proceeding to recommend changes to any of its regulations in order to implement sections 214(e) of this title and this section, including the definition of the services that are supported by Federal universal service support mechanisms and a specific timetable for completion of such recommendations. In addition to the members of the Joint Board required under section 410(c) of this title, one member of such Joint Board shall be a State-appointed utility consumer advocate nominated by a national organization of State utility consumer advocates. The Joint Board shall, after notice and opportunity for public comment, make its recommendations to the Commission 9 months after February 8, 1996.

(2) Commission action

The Commission shall initiate a single proceeding to implement the recommendations from the Joint Board required by paragraph (1) and shall

[35] 47 U.S.C. § 254(d).

[36] Wireline Broadband NPRM, 17 FCC Rcd at 3053, para. 74;

complete such proceeding within 15 months after February 8, 1996. The rules established by such proceeding shall include a definition of the services that are supported by Federal universal service support mechanisms and a specific timetable for implementation. Thereafter, the Commission shall complete any proceeding to implement subsequent recommendations from any Joint Board on universal service within one year after receiving such recommendations.

(b) Universal service principles

The Joint Board and the Commission shall base policies for the preservation and advancement of universal service on the following principles:

(1) Quality and rates

Quality services should be available at just, reasonable, and affordable rates.

(2) Access to advanced services

Access to advanced telecommunications and information services should be provided in all regions of the Nation.

(3) Access in rural and high cost areas

Consumers in all regions of the Nation, including low-income consumers and those in rural, insular, and high cost areas, should have access to telecommunications and information services, including interexchange services and advanced telecommunications and information services, that are reasonably comparable to those services provided in urban areas and that are available at rates that are reasonably comparable to rates charged for similar services in urban areas.

(4) Equitable and nondiscriminatory contributions

All providers of telecommunications services should make an equitable and nondiscriminatory contribution to the preservation and advancement of universal service.

(5) Specific and predictable support mechanisms

There should be specific, predictable and sufficient Federal and State mechanisms to preserve and advance universal service.

(6) Access to advanced telecommunications services for schools, health care, and libraries

Elementary and secondary schools and classrooms, health care providers, and libraries should have access to advanced telecommunications services as described in subsection (h) of this section.

(7) Additional principles

Such other principles as the Joint Board and the Commission determine are necessary and appropriate for the protection of the public interest, convenience, and necessity and are consistent with this chapter.

(c) Definition

(1) In general

Universal service is an evolving level of telecommunications services that the Commission shall establish periodically under this section, taking into account advances in telecommunications and information technologies and services. The Joint Board in recommending, and the Commission in establishing, the definition of the services that are supported by Federal universal service support mechanisms shall consider the extent to which such telecommunications services--

(A) are essential to education, public health, or public safety;
(B) have, through the operation of market choices by customers, been subscribed to by a substantial majority of residential customers;
(C) are being deployed in public telecommunications networks by telecommunications carriers; and
(D) are consistent with the public interest, convenience, and necessity.

(2) Alterations and modifications

The Joint Board may, from time to time, recommend to the Commission modifications in the definition of the services that are supported by Federal universal service support mechanisms.

(3) Special services

In addition to the services included in the definition of universal service under paragraph (1), the Commission may designate additional services for such support mechanisms for schools, libraries, and health care providers for the purposes of subsection (h) of this section.

(d) Telecommunications carrier contribution

Every telecommunications carrier that provides interstate telecommunications services shall contribute, on an equitable and nondiscriminatory basis, to the specific, predictable, and sufficient mechanisms established by the Commission to preserve and advance universal service. The Commission may exempt a carrier or class of carriers from this requirement if the carrier's telecommunications activities are limited to such an extent that the level of such carrier's contribution to the preservation and advancement of universal service would be de minimis. Any other provider of interstate telecommunications may be required to contribute to the preservation and advancement of universal service if the public interest so

requires.

(e) Universal service support

After the date on which Commission regulations implementing this section take effect, only an eligible telecommunications carrier designated under section 214(e) of this title shall be eligible to receive specific Federal universal service support. A carrier that receives such support shall use that support only for the provision, maintenance, and upgrading of facilities and services for which the support is intended. Any such support should be explicit and sufficient to achieve the purposes of this section.

(f) State authority

A State may adopt regulations not inconsistent with the Commission's rules to preserve and advance universal service. Every telecommunications carrier that provides intrastate telecommunications services shall contribute, on an equitable and nondiscriminatory basis, in a manner determined by the State to the preservation and advancement of universal service in that State. A State may adopt regulations to provide for additional definitions and standards to preserve and advance universal service within that State only to the extent that such regulations adopt additional specific, predictable, and sufficient mechanisms to support such definitions or standards that do not rely on or burden Federal universal service support mechanisms.

(g) Interexchange and interstate services

Within 6 months after February 8, 1996, the Commission shall adopt rules to require that the rates charged by providers of interexchange telecommunications services to subscribers in rural and high cost areas shall be no higher than the rates charged by each such provider to its subscribers in urban areas. Such rules shall also require that a provider of interstate interexchange telecommunications services shall provide such services to its subscribers in each State at rates no higher than the rates charged to its subscribers in any other State.

(h) Telecommunications services for certain providers

(1) In general

(A) Health care providers for rural areas

A telecommunications carrier shall, upon receiving a bona fide request, provide telecommunications services which are necessary for the provision of health care services in a State, including instruction relating to such services, to any public or nonprofit health care provider that serves persons who reside in rural areas in that State at rates that are reasonably comparable to rates charged for similar services in urban areas in that State. A telecommunications carrier providing service under this paragraph shall be entitled to have an amount equal to the difference, if any, between the rates for services provided to

health care providers for rural areas in a State and the rates for similar services provided to other customers in comparable rural areas in that State treated as a service obligation as a part of its obligation to participate in the mechanisms to preserve and advance universal service.

(B) Educational providers and libraries

All telecommunications carriers serving a geographic area shall, upon a bona fide request for any of its services that are within the definition of universal service under subsection (c)(3) of this section, provide such services to elementary schools, secondary schools, and libraries for educational purposes at rates less than the amounts charged for similar services to other parties. The discount shall be an amount that the Commission, with respect to interstate services, and the States, with respect to intrastate services, determine is appropriate and necessary to ensure affordable access to and use of such services by such entities. A telecommunications carrier providing service under this paragraph shall--

(i) have an amount equal to the amount of the discount treated as an offset to its obligation to contribute to the mechanisms to preserve and advance universal service, or

(ii) notwithstanding the provisions of subsection (e) of this section, receive reimbursement utilizing the support mechanisms to preserve and advance universal service.

(2) Advanced services

The Commission shall establish competitively neutral rules--

(A) to enhance, to the extent technically feasible and economically reasonable, access to advanced telecommunications and information services for all public and nonprofit elementary and secondary school classrooms, health care providers, and libraries; and

(B) to define the circumstances under which a telecommunications carrier may be required to connect its network to such public institutional telecommunications users.

(3) Terms and conditions

Telecommunications services and network capacity provided to a public institutional telecommunications user under this subsection may not be sold, resold, or otherwise transferred by such user in consideration for money or any other thing of value.

(4) Eligibility of users

No entity listed in this subsection shall be entitled to preferential rates or treatment as required by this subsection, if such entity operates as a for-profit business, is a school described in paragraph (7)(A) with an endowment of more than $50,000,000, or is a library or library consortium not eligible for assistance from a State library administrative agency under the Library Services and Technology Act [20 U.S.C.A. § 9121 et seq.].

(5) Requirements for certain schools with computers having internet access

(A) Internet safety

(i) In general

Except as provided in clause (ii), an elementary or secondary school having computers with Internet access may not receive services at discount rates under paragraph (1)(B) unless the school, school board, local educational agency, or other authority with responsibility for administration of the school--

(I) submits to the Commission the certifications described in subparagraphs (B) and (C);
(II) submits to the Commission a certification that an Internet safety policy has been adopted and implemented for the school under subsection (l) of this section; and
(III) ensures the use of such computers in accordance with the certifications.

(ii) Applicability

The prohibition in clause (i) shall not apply with respect to a school that receives services at discount rates under paragraph (1)(B) only for purposes other than the provision of Internet access, Internet service, or internal connections.

(iii) Public notice; hearing

An elementary or secondary school described in clause (i), or the school board, local educational agency, or other authority with responsibility for administration of the school, shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy. In the case of an elementary or secondary school other than an elementary or secondary school as defined in section 8801 of Title 20, the notice and hearing required by this clause may be limited to those members of the public with a relationship to the school.

(B) Certification with respect to minors

A certification under this subparagraph is a certification that the school, school board, local educational agency, or other authority with responsibility for administration of the school--

(i) is enforcing a policy of Internet safety for minors that includes monitoring the online activities of minors and the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--

(I) obscene;
(II) child pornography; or

(III) harmful to minors; and
(ii) is enforcing the operation of such technology protection measure during any use of such computers by minors.

(C) Certification with respect to adults

A certification under this paragraph is a certification that the school, school board, local educational agency, or other authority with responsibility for administration of the school--
(i) is enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--
(I) obscene; or
(II) child pornography; and
(ii) is enforcing the operation of such technology protection measure during any use of such computers.

(D) Disabling during adult use

An administrator, supervisor, or other person authorized by the certifying authority under subparagraph (A)(i) may disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose.

(E) Timing of implementation

(i) In general

Subject to clause (ii) in the case of any school covered by this paragraph as of the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certification under subparagraphs (B) and (C) shall be made--
(I) with respect to the first program funding year under this subsection following such effective date, not later than 120 days after the beginning of such program funding year; and
(II) with respect to any subsequent program funding year, as part of the application process for such program funding year.

(ii) Process

(I) Schools with internet safety policy and technology protection measures in place

A school covered by clause (i) that has in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C) shall certify its compliance with subparagraphs (B) and (C) during each annual program application

cycle under this subsection, except that with respect to the first program funding year after the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certifications shall be made not later than 120 days after the beginning of such first program funding year.

(II) Schools without internet safety policy and technology protection measures in place

A school covered by clause (i) that does not have in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C)--
(aa) for the first program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is undertaking such actions, including any necessary procurement procedures, to put in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C); and
(bb) for the second program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is in compliance with subparagraphs (B) and (C).

Any school that is unable to certify compliance with such requirements in such second program year shall be ineligible for services at discount rates or funding in lieu of services at such rates under this subsection for such second year and all subsequent program years under this subsection, until such time as such school comes into compliance with this paragraph.

(III) Waivers

Any school subject to subclause (II) that cannot come into compliance with subparagraphs (B) and (C) in such second year program may seek a waiver of subclause (II)(bb) if State or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required by such subclause. A school, school board, local educational agency, or other authority with responsibility for administration of the school shall notify the Commission of the applicability of such subclause to the school. Such notice shall certify that the school in question will be brought into compliance before the start of the third program year after the effective date of this subsection in which the school is applying for funds under this subsection.

(F) Noncompliance

(i) Failure to submit certification

Any school that knowingly fails to comply with the application guidelines regarding the annual submission of certification required by this paragraph

shall not be eligible for services at discount rates or funding in lieu of services at such rates under this subsection.

(ii) Failure to comply with certification

Any school that knowingly fails to ensure the use of its computers in accordance with a certification under subparagraphs (B) and (C) shall reimburse any funds and discounts received under this subsection for the period covered by such certification.

(iii) Remedy of noncompliance

(I) Failure to submit

A school that has failed to submit a certification under clause (i) may remedy the failure by submitting the certification to which the failure relates. Upon submittal of such certification, the school shall be eligible for services at discount rates under this subsection.

(II) Failure to comply

A school that has failed to comply with a certification as described in clause (ii) may remedy the failure by ensuring the use of its computers in accordance with such certification. Upon submittal to the Commission of a certification or other appropriate evidence of such remedy, the school shall be eligible for services at discount rates under this subsection.

(i) Consumer protection

The Commission and the States should ensure that universal service is available at rates that are just, reasonable, and affordable.

(j) Lifeline assistance

Nothing in this section shall affect the collection, distribution, or administration of the Lifeline Assistance Program provided for by the Commission under regulations set forth in section 69.117 of title 47, Code of Federal Regulations, and other related sections of such title.

(k) Subsidy of competitive services prohibited

A telecommunications carrier may not use services that are not competitive to subsidize services that are subject to competition. The Commission, with respect to interstate services, and the States, with respect to intrastate services, shall establish any necessary cost allocation rules, accounting safeguards, and guidelines to ensure that services included in the definition of universal service bear no more than a reasonable share of the joint and common costs of facilities used to provide those services.

(l) Internet safety policy requirement for schools and libraries

(1) In general

In carrying out its responsibilities under subsection (h) of this section, each school or library to which subsection (h) of this section applies shall--

(A) adopt and implement an Internet safety policy that addresses--

(i) access by minors to inappropriate matter on the Internet and World Wide Web;

(ii) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

(iii) unauthorized access, including so-called "hacking", and other unlawful activities by minors online;

(iv) unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and

(v) measures designed to restrict minors' access to materials harmful to minors; and

(B) provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy.

(2) Local determination of content

A determination regarding what matter is inappropriate for minors shall be made by the school board, local educational agency, library, or other authority responsible for making the determination. No agency or instrumentality of the United States Government may--

(A) establish criteria for making such determination;

(B) review the determination made by the certifying school, school board, local educational agency, library, or other authority; or

(C) consider the criteria employed by the certifying school, school board, local educational agency, library, or other authority in the administration of subsection (h)(1)(B) of this section.

(3) Availability for review

Each Internet safety policy adopted under this subsection shall be made available to the Commission, upon request of the Commission, by the school, school board, local educational agency, library, or other authority responsible for adopting such Internet safety policy for purposes of the review of such Internet safety policy by the Commission.

(4) Effective date

This subsection shall apply with respect to schools and libraries on or after the date that is 120 days after December 21, 2000.

Inter-carrier Compensation

47 C.F.R. Section 69.5(b) of the Commission's rules states that "[c]arrier's carrier charges shall be computed and assessed upon all interexchange carriers that use local exchange switching facilities for the provision of interstate or foreign telecommunications services." To keep local telephone rates low, access charges traditionally have exceeded the forward-looking economic costs of providing access services[37].

Since 1983 the Commission has exempted enhanced service providers (ESPs) from the payment of certain interstate access charges (the "ESP exemption")[38]. Consequently, ESPs are treated as end users for the purpose of applying access charges and are, therefore, entitled to pay local business rates for their connections to the LEC central offices and the PSTN[39].

As economic regulation of VoIP such as imposing inter-carrier compensation is considered unnecessary at this point owing to the competitive nature of technology, the pertinent statutory definitions are omitted here.

In the next chapter, we begin to analyze the classification of VoIP services and the challenges it poses for imposing the current regulations.

---

[37] Intercarrier Compensation NPRM, 16 FCC Rcd at 9614, para. 7 (citing Federal-State Joint Board on Universal Service, CC Docket No. 96-45, Report and Order, 12 FCC Rcd 8776 (1997) (First Universal Service Report and Order)).

[38] Implementation of the Local Competition Provisions in the Telecommunications Act of 1996; Intercarrier Compensation for ISP-Bound Traffic, CC Docket Nos. 96-98, 99-68, Order on Remand and Report and Order, 16 FCC Rcd 9151, 9158, para. 11 (2001) (ISP Remand Order) (citing MTS/WATS Market Structure Order, 97 FCC 2d at 715, para. 83); see also ESP Exemption Order, 3 FCC Rcd at 2633, para. 17; Access Charge Reform, CC Docket Nos. 96-262, 94-1, 91-213, 95-72, First Report and Order, 12 FCC Rcd 15982, 16133, para. 344 (1997) (Access Charge Reform First Report and Order).

[39] ISP Remand Order, 16 FCC Rcd at 9158, para. 11 (citing ESP Exemption Order, 3 FCC Rcd at 2635 n.8, 2637 n.53); see also Access Charge Reform First Report and Order, 12 FCC Rcd at 16133-35, paras. 344-48.

Chapter 3

VoIP CLASSIFICATION AND THE REGULATORY CHALLENGES

Need for VoIP Classification

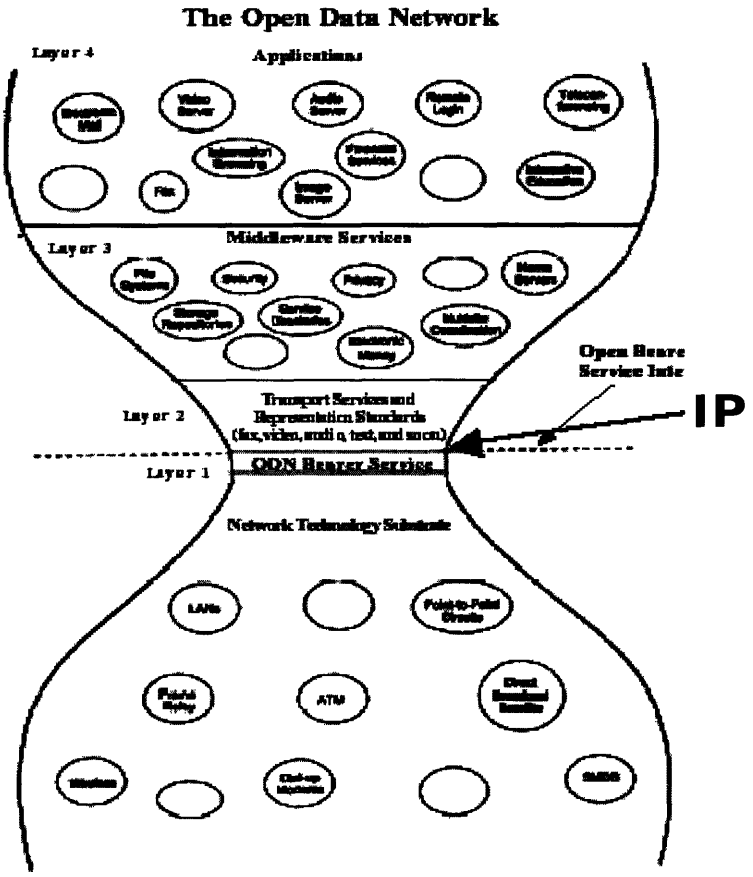


Figure 13 Hourglass model of the Internet

Figure 13 shows the hourglass model of the Internet [21]. The concept illustrated here is that the Internet Protocol (IP) layer provides a single interface to enable running of a

range of applications (at the top) over a range of technologies (at the bottom). This picture vividly shows that once voice or any other application is transported over IP, it can go over a variety of physical media such as wireless and wireline technologies of the past and future. As these technologies have different technical capabilities and cost structures, it becomes important to understand their differences before considering their regulation.

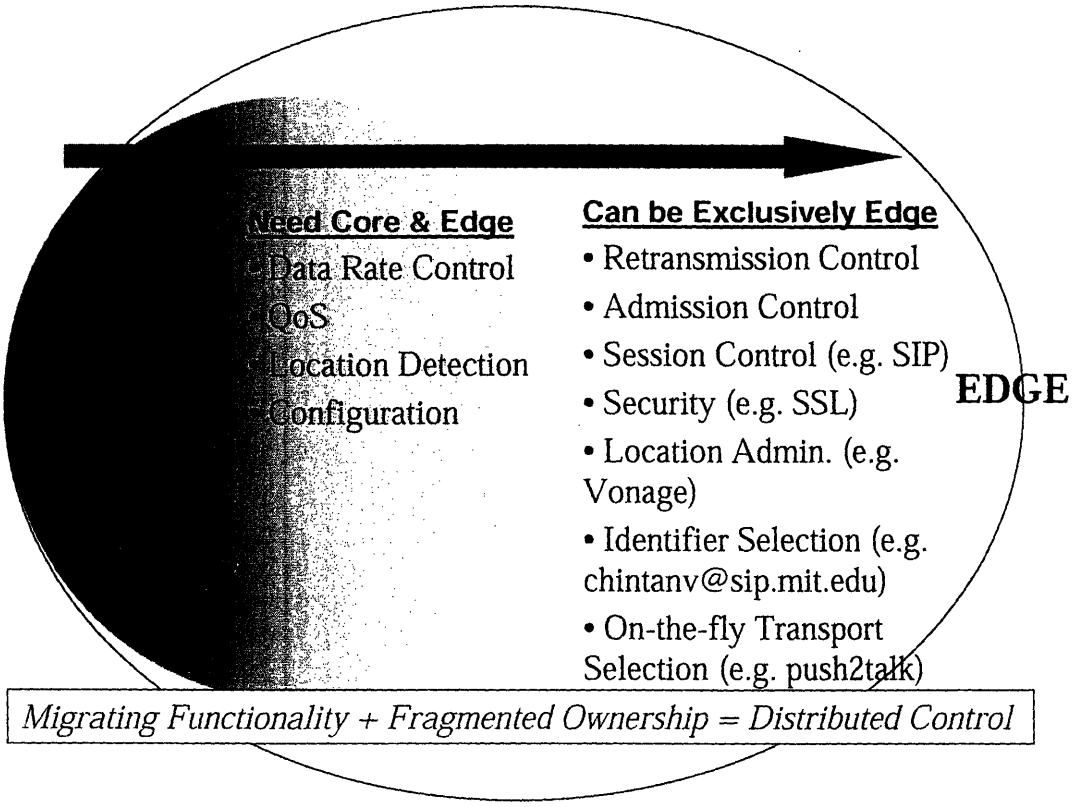


Figure 14 Core-Edge Movement

Furthermore, it is important to understand the movement of functionality from the center of the network (referred to as the "core") towards the end-user of the network (referred to as the "edge"). Figure 14 is one illustrations of how the functionality has been steadily

moving towards the edge as more and more of the applications adopt the end-to-end principle [22] in their design. The illustration here is drawn specifically from the perspective of VoIP related functionality specifically necessary to deliver regulatory compliance.

In the world of circuit-switched PSTN, the telephone at the edge of the network was dumb, while the network switches in the core possessed all the intelligence. With more and more of the applications moving to the packet-based networks, much of the functionality can be implemented exclusively in the edge device or using a combination of a device at the edge and another at the core. The early examples of the protocol functionality moving to the edge were retransmission and admission control. Control over call admission that originally resided exclusively in the core began to move towards the boxes at the edge of the network that were operated by third-party vendors. With the recent standardization of signaling protocols such as H.323 and SIP, the signaling can now done exclusively by the edge devices and applications. Examples of the protocol functionality that can be carried out combining functionality of the core and the edge devices are data rate control and quality of service. Both require the knowledge of traffic and buffering capacity in the core of the network as well in the edge devices. Application level functionality such as location administration and detection, identifier selection and on-the-fly transport selection used to either reside in the core of the traditional network or were absent. These functions and their control are moving to the edge of the network in some architectural scenarios. Such a migration of functionality, combined with the fragmented ownership of the network (discussed more in the next subsection) leads to distributed control in delivering voice service that is different from the nature of

capability and control that existed in the old, vertically integrated PSTN architecture. In the next section, we propose one way of classifying the different architectural scenarios that exist today to provide the ability to do voice communications using VoIP.

VoIP Classification

VoIP in the backbone A	[illegible] Based [illegible]	VoIP over Broadband B2	P2P VoIP C
- Circuit Switching - Same Operator and Service Provider (e.g. AT&T, Sprint, MCI)	- Packet Switching - Same Operator and Service Provider (e.g. VoCable, VoDSL, VoIP over Wireless)	- Packet Switching - Different Operator and Service Provider (e.g. Vonage, SkypeOut, SkypeIn)	- Packet Switching - Operator agnostic Service Provider (e.g. FWD, Skype, Yahoo!, IM)

Table 3. VoIP Classification

Table 3 shows the proposed VoIP classification. The bases for such a classification are the architecture and the ownership of the network in various scenarios for delivering VoIP service.

VoIP in the Backbone

This class of VoIP uses circuit-switching to the end-point (i.e. phone), and packet-switching in the core network. Most local exchange carriers (LEC), such as Verizon, Qwest, and inter-exchange carriers (IXC), such as MCI, Sprint, use IP in the backbone to transport traffic for long distance.

This is a highly vertically integrated model, where the phone company is the network operator, service provider and feature provider. The usage pricing is based on minutes of use (MOU).

Voice communication delivered in this model offers the reliability and the features of PSTN. Also, the service provider is considered a telecommunications service provider[40] under the 1996 Telecommunications Act, and is subject to common carrier regulations.

Facility-based VoIP

In this class of VoIP, end-to-end communication is done using packet-switching, and the network operator (i.e. the owner of the facility) and the service provider is the same entity. Examples of this class of VoIP are: Voice over cable (VoCable) providers (often referred to as cable telephony providers), Voice over Digital Subscriber Line (VoDSL) providers, and IP voice over wireless providers. In this class of service, the service provider manages call signaling and audio transport.

This class of service is also highly vertically integrated, where the same entity is the network operator, service provider and feature provider. In many cases, the same service provider sells the end device such as cable model or DSL route. The voice service

[40] AT&T's service consists of a portion of its interexchange traffic routed over AT&T's Internet backbone. AT&T argued that there is a net protocol conversion and therefore it is information service, and shall be exempted from the Access Charge Obligations.
End-users customers do not order a different service, pay different rates, or lace and receive calls any differently than they do through AT&T's traditional circuit-switched long distance service; the decision to use its Internet backbone to route certain calls is made internally by AT&T. To the extent that protocol conversions associated with AT&T's specific service take place within its network, they appear to be internetworking conversions, which the commission has found to be Telecommunications Service (Non-Accounting Safeguard Order, 11 FCC Rcd at 21957-58, para. 106.

here is offered as a bundled good with data (i.e. Internet service) or video (i.e. Television programming).

Facility-based VoIP provides Phone-to-Phone communication, with most features of PSTN. Single bill for voice, video and data is often sited as one of its attractions. This class of service providers has the unique ability to bundle voice, video and data services.

VoIP over Broadband

In this class of VoIP, a customer who already has a broadband access, purchases VoIP service on top of it. Here, the Internet Service Provider (ISP) and the VoIP service provider are different entities. The VoIP service provider manages the signaling (e.g. SIP signaling), and the audio coding to RTP. However, the ISP then carries the signaling over TCP/IP, and audio over UDP/IP.

This model is not vertically integrated. In an extreme example, a customer can have a different network operator (e.g. Municipal Broadband Connection), ISP (e.g. Earthlink) and VoIP service provider (e.g.. Vonage). VoIP Service Provider is the feature provider. They also sell the end devices such as a software client, often called a softphone; or a Phone Adaptor, which is nothing but a SIP client (if SIP is the signaling protocol they use). The voice communication service is most often offered at monthly flat rate. In some cases (e.g. SkypeOut/SkypeIN), it is MOU based.

VoIP over Broadband class of service provides Phone-to-Phone, PC-to-Phone or Phone-to-PC communication. With the use of SIP or other proprietary protocols, it provides "presence" features such as the user's availability and other status. It can also provide virtual phone numbers to provide access charge arbitrage opportunity, as a user

can keep multiple virtual numbers and assign one to the phone based upon their current geographical locale. They also offer number portability. Some providers of VoIP over Broadband support 911[41] voluntarily.

P2P VoIP

In this class of VoIP, a customer with any form of Internet connectivity, over PSTN using a modem, or through a broadband connection etc., downloads a free voice-enabled application for Peer-to-Peer communication. Traditionally, MSN Messenger, AOL Instant Messenger (IM), Yahoo! Messenger were the big three providers of this mode of voice communication. Recently, Skype and GoogleTalk have emerged as popular P2P VoIP provider. The P2P VoIP provider manages the signaling (e.g. proprietary P2P signaling for Skype), and the audio coding to RTP. However, the ISP then carries the signaling over TCP/IP, and audio over UDP/IP.

This class of service is not vertically integrated. A P2P VoIP provider only provides the end application and the directory service. The service is usually free[42].

P2P VoIP provides PC-to-PC connectivity. Today, customers do not use this class of voice communication as their primary service. Most users use it for recreation or to make international voice communication. However, this class of VoIP is the one that has a very different look-and-feel from the traditional telephony. It remains to be seen if such a mode can disrupt telephony, as we know it today.

---

[41] http://www.vonage.com/products.php

[42] Yahoo! Messenger and MSN Messenger have begun to provide a more secure version of their application for a charge.

Nature of Technology and Regulatory Challenges

911/E911

Current "basic" and "enhanced" 911 regulatory requirements can be summarized as follows:

1.Identify emergency call and route to appropriate PSAP (Basic 911)

2.Provide call back information (E911)

3.Provide Location (E911)

In the case of VoIP, there are several challenges. First, the identifier looks very different than the phone number. The currently installed network equipment do not understand an identifiers such as sip:chintanv@mit.edu that is not a phone number. They are not designed to operate based upon anything but a ten digit phone number. Additionally, the new identifiers identify a person, not the connection. Second, the device is nomadic (more than cellular phones). As VoIP over broadband works from any broadband connection, a phone adapter can be taken to any part of the world[43] as long as there is a broadband connection available. Also, the devices may change, but the identifier remains the same. For example, a P2P VoIP (e.g. skype) customer may log in to any PC and still communicate using the same username.

CALEA

Current CALEA regulatory requirements can be summarized as follows:

1.Provide call-identifying information

2.Provide content tracing (lawful intercept) capability

[43] Today, many Vonage consumers carry a phone adapter to Europe and East Asian countries.

3.Ensure security and privacy

In the case of VoIP, call identification information is known to the entity that manages call signaling; whereas, the actual audio transport is known to the entity that manages transport. For the class of service where these entities are different, for example in the case of VoIP over broadband, the VoIP service provider manages signaling, but the ISP manages the audio transport. This means that coordination between these entities will be required for a lawful intercept, to synchronize the origination and termination of the call with turning the recording on or off.

Balancing the needs for wiretap, security, privacy and innovation is delicate. Probability of a successful wiretap is highly dependent on the security measures customer takes. Channel encryption techniques make it increasingly difficult to tap a communication. Moreover, it is not enough to simply tap the communication. Subsequent decryption of the tapped communications is equally important for it to be of any use. Customer's use of content encryption increasingly challenges the ability to decrypt the tapped content.

For the privacy perspective, the converged voice, video, data connections carry much more information about the customer than the old phone lines. This makes it more challenging to tap only the information the law enforcement requests for, which maintaining the customer's privacy.

Disability Access

Current Disability Access regulatory requirements can be summarized as follows:

1. Manufacture accessible telecommunications equipment and CPE

2. Provide relay service (TRS, IP, VRS etc.)

3. Do not install network features, functions or capabilities not compliant with disability access requirement

In this area, VoIP provides more opportunities than challenges. Serving the person with disabilities using a multimode (voice, text or video) leads to more people with disability being served. Also, using IP based video and text provides a higher probability of reaching functional equivalence of communicating with a person with no impairment.

The challenges that do remain when considering VoIP based disability access are related to standardization and funding. Multimode support for disability access compliance must be standardized, so that manufacturers can provide it easily.

Universal Service

Current Universal Service regulatory requirements can be summarized as follows:

1. Making contribution to Universal Service Fund (USF)
2. Receiving contributions from Universal Service Fund

If certain classes of VoIP are determined to be information services, should the providers of such service – who own *no* facility – be required to contribute? Would such providers "provide" telecommunications? If the Commission were to exercise its permissive authority over facilities-based and non-facilities-based providers of IP-enabled services, how could it do so in an equitable and nondiscriminatory fashion? Would the Commission identify specific services that are subject to its permissive authority? The opposite issue is in considering how the USF shall be disbursed to VoIP providers, who

own no facility, if any. Finally, the methodology for calculating contributions is also unclear for VoIP based service.

Inter-carrier Compensation

Current inter-carrier compensation regulatory requirements can be summarized as follows:

1. Access Charges
2. Reciprocal Compensation
3. Voluntary Negotiations

Access charges are typically paid by the IXCs to the LECs for using their local loop facilities. Reciprocal compensation is typically the charges paid by two IXCs for reaching each other's customers. Voluntary negotiations are typically between a wireless carrier and an LEC for using the local loop. As the name suggests, these charges are determined voluntarily, as opposed to the access charges and reciprocal compensations that are determined by the FCC.

In the case of inter-carrier compensation, the questions that arise are beyond just the issue of regulating VoIP. The first question is, should there be the inter-carrier compensation? In the current regime, the access charges have diverged greatly from the costs of interconnection. IP being agnostic to the physical media only exacerbates the arbitrage opportunity, as the underlying costs of various architectures are vastly different. Further, should the rates be uniform across the providers and what should they be? This question is important as the call signaling and bearer (content) channels are separable. As a result, the underlying cost structure for the facility-based VoIP class of provider that

own the infrastructure are very different from the VoIP over Broadband class of providers that have no infrastructure ownership.

Numbering

With separation of signaling channels have come features such as being able to choose a number in any area code and keeping your number when moving. While offering some convenience to a small number of customers, such features bring along several policy and technical challenges. On the policy side, usage assumptions about the ownership, association with the geographical area and the rate center are distorted. As a result assignment, relief, exhaustion, utilization and forecasting of numbering resources becomes difficult. On the technical side, the number portability between ILECs, CLECs and IXCs could often be a problem. Similarly, there is a question of number portability between a PSTN and VoIP service provider.

Table 4 summarizes the five regulatory issues, current obligations and the VoIP challenges.

Issues	Current Obligations	VoIP Challenges
911/E911	1.Identify emergency call and route to appropriate PSAP 2.Provide call back information 3.Provide location	1.Different Identifier 2.Devices are Nomadic 3.Separation of Access, Transport and Application
CALEA	1.Provide call-identifying information 2.Provide content tracing (lawful intercept) capability 3.Ensure security and privacy	1.Call-identification Information unknown to the service provider 2.Tension between wiretap, security, privacy and innovation
Disability Access	1.Manufacture accessible telecommunications equipment and CPE 2.Provide relay service (TRS, IP, VRS etc.) 3.Do not install network features, functions or capabilities not compliant with disability access requirement	1.Standardization of multimode communications 2.Funding multimode communications
Universal Service	1.Contribution to the USF 2.Receive subsidy from the USF	1.Should VoIP support the USF? 2.Should the USF support VoIP?
Inter-carrier Compensation	1.Access Charges 2.Reciprocal Compensation 3.Voluntary Negotiations	1.IP agnostic to physical media exacerbates the existing arbitrage opportunities 2.Signaling and bearer (content) separation

Table 4. Five regulatory issues, current obligations and VoIP challenges

Chapter 4

METHODOLOGY: THE SYSTEM DYNAMICS STANDARD METHOD

What is "standard method"?

Practitioners of system dynamics[44] use the standard method to define the problem and create a model, while gaining useful insights along the way. In this chapter we will describe the the standard method. The steps of the standard method are:

1. Problem definition
2. List of variables
3. Reference modes
4. Problem statement
5. Momentum policies
6. Dynamic hypotheses (i.e. causal loops)
7. Model first loop
8. Analyze first loop
9. Model second loop
10. Analyze second loop

---

[44] For System Dynamics basics, please refer to 23. Sterman, J., *Business dynamics: systems thinking and modeling for a complex world.* c2000, Boston: Irwin/McGraw-Hill.

11. Etc.

Conclusions and insights emerge at every step during the standard method.

Example of the Standard Method

The easiest way to understand standard method is to use an example. Let us take an example of building a classic diffusion model. Momentarily, let's pretend that we don't know what a diffusion model is.

Let us take an example of a company that manufactures an Automated Fly Swatter, and is trying to understand the key drivers in the fly market. Here's how the system dynamics standard method would work to structure the thinking around understanding the key drivers.

Variables List

Variables are entities in the system that can go up or down. In our example, the following is a possible list of variables.

Fly population

Revenues

Unit Sales

Annoyance at flies

Market saturation

Manufacturing costs

Price

Cost of batteries

Word of mouth about our product

Product recalls

Health problems with our products

...etc.

The method calls for listing as many variables as possible. In a complex system, it is possible to list 100 – 150 variables that are somehow related to the problem at hand. *The next step is to identify five to six variables that are most important. System dynamics experts believe that focusing on five or six variables can capture behavior of most complex systems we encounter.*

Reference Modes

The next step is to create reference modes. A reference mode is a graph of the behavior of each of the variables. Figure 15 shows an example of a reference mode for a variable, in this case "unit sales." It is important to understand the timeline on a reference mode. In the cases where documenting approximate time line is difficult, that itself is a useful insight.

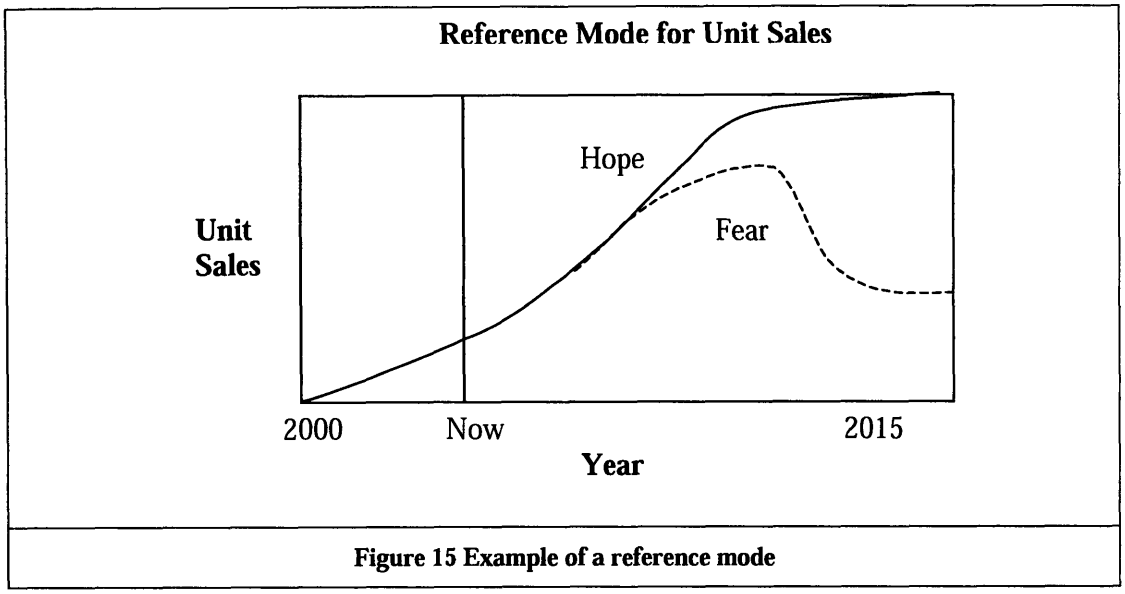


Figure 15 Example of a reference mode

Problem Statement

Now it is time to identify the reference mode(s) that capture the true concern of this problem. This is the problem statement. For example, we hope that the initial growth trend of AFS sales continues and that the product ultimately becomes a stable, high-volume seller. But we're worried that sales, after appearing to be on track, might take a nosedive leaving us with mediocre or low sales, and way too much capacity. If we are successful in our project here we will increase the likelihood of the curve labeled "hope" and decrease the likelihood of the curve labeled "fear". It is important to phrase it mentally, but not get caught up into wording it precisely at this point, after all a picture is worth a thousand words.

Momentum Policies

Momentum policies (i.e. solutions) are what you would implement now to solve the problem, if there was no further time to collect information or ponder. Once you have a problem focus, it is possible to collect momentum policies.

The momentum policies give a way to gauge at the end of the process, whether anything beyond the additional specificity has come out of the project. Consequently, it is important to record what one would do *now* about the problem, if decisions had to be made *immediately.*

Let's say in this example we record ideas like:

"We need to do a market study"

"We should start a competitor intelligence unit"

"We need to get data on the drivers of the market"

"We've got to get better forecasts from the Economics Group".

Store them away. These may be used to suggest tests or directions of inquiry, but at least (and in most cases at most), they useful to assess how far our understanding has come at the end of the exercise.

Causal Loop Diagram or Dynamic Hypotheses

With variables, reference modes, and a problem-focus, we are in position to start coming up with *dynamic hypotheses*; that is, loops that describe feedback processes capable of generating the patterns in the reference modes. Coming up with a diagram often take several weeks, and most often results in a number of insights and good ideas.

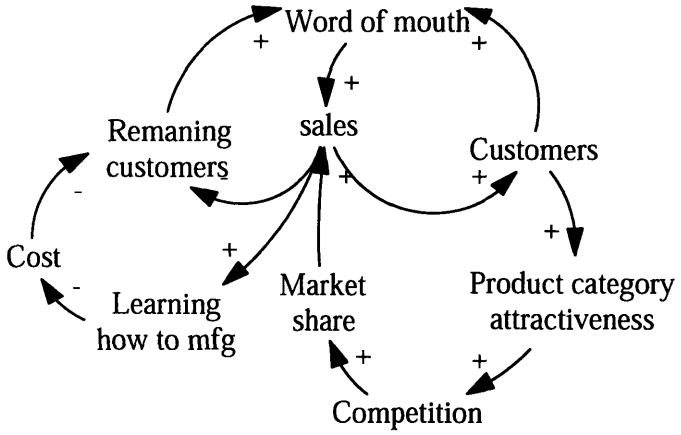


Figure 16 Example of Causal Loops to form Dynamic Hypothesis

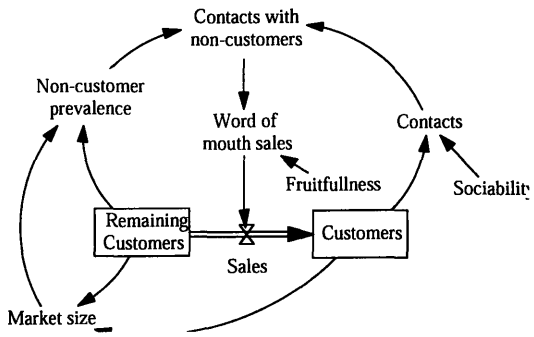
Figure 16 shows an example of a causal loop diagram to form a rough dynamic hypothesis around the reference modes we earlier drew for the "unit sales" variable. This process of drawing causal loops and may lead to additional insights. For example, "The learning loop counteracts the running-out-of customers loop" and "We can strengthen the word-of-mouth loop with a sign-up-a-friend promotion". It is important to record insights as they come up.

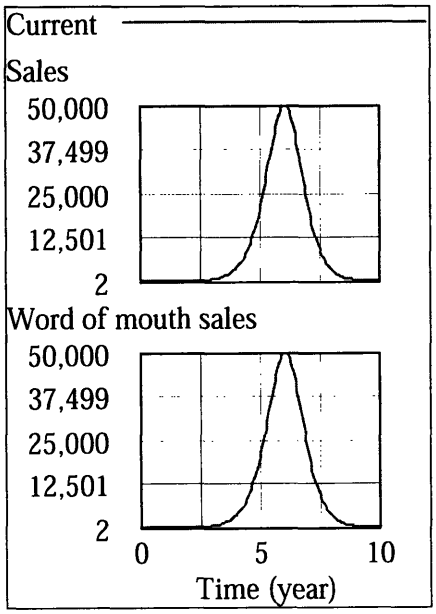
Modeling

Finally, it is time to model. However, it is important to realize that that the model is not the actual objective, rather the process is. The modeling is simply the next step in the process, it may help people refine some of the insights already recorded, it will probably result in additional insights, but it probably won't contradict any of the insights already recorded.

To model, choose a loop, model it, simulate, analyze, and work with your client to develop insights and ideas. Then choose another loop, add it to your growing model,

simulate, analyze again, and work on further developing new or existing ideas. As always record insights and conclusions as you go along. For example, "Strengthening the positive word-of-mouth loop creates a faster rise and a deeper collapse." and "Replacement sales may lesson the severity of the down-turn in sales".






```
**********************************

  .diffusion

**********************************

Sales = Word of mouth sales

        Units: people/year

Word of mouth sales =

   "Contacts with non-customers" * Fruitfulness

        Units: people/year

Fruitfulness = 0.05

        Units: fraction

"Contacts with non-customers" =

   Contacts * "Non-customer prevalence"

        Units: people/year

Contacts = Customers * Sociability

        Units: people/year

Sociability = 40

        Units: people/(year*person)

Customers = INTEG( Sales , 1)

        Units: people
```

	"Non-customer prevalence" = Remaining Customers / Market size Units: fraction Remaining Customers = INTEG(- Sales , 100000) Units: people Market size = Customers + Remaining Customers Units: people ********** .Control ********** FINAL TIME = 10 Units: year INITIAL TIME = 0 Units: year SAVEPER = TIME STEP Units: year TIME STEP = 0.0625 Units: year

Figure 17 Example of a modeled causal loop, its equations and the output

Figure 17 shows an example of a model for our causal loop. The graphs show how two of the variables behave over time. The equations on the right hand column indicate the units and relationships among various variables.

It is possible that the modeling leads to the best insights. Or in retrospect the causal loops, or even the reference modes, may have been the source of the most important insights and conclusions. The important lesson from this is that the model is *not* the goal of the engagement. The goal is to use the entire process. Modeling is just one piece – in any particular situation it might provide the brightest illumination, but in another situation a different part of the process might turn out to be the real source of light, and in yet another situation, the entire process may shine with a uniform brilliance.

Chapter 5

SYSTEM DYNAMICS MODEL FOR CALEA

In this chapter, we apply the system dynamics standard method to build a model for CALEA, as it applies to VoIP.

CALEA Background

First, let us quickly recap the current CALEA obligations and VoIP related challenges that we have already discussed in Chapter 3.

Current Obligations:

1. Provide call-identifying information
2. Provide content tracing (lawful intercept) capability
3. Ensure security and privacy

VoIP Challenges:

1. Call-identification Information unknown to the service provider
2. Tension between wiretap, security, privacy and innovation

Six Variables of interest

As a first step, we made a list of variables as they pertain to CALEA regulation for VoIP. Appendix C has the complete list of CALEA related variables. Next, six variables that are most important to the system are chosen. *An important thing to note here is that the Law Enforcement Agencies (LEA), or the regulatory agency such as the Federal Communication Commission (FCC) is considered the client when selecting the important*

variables. As one would realize, if the client were to be some other stakeholder, for example, facility-based VoIP provider, this list of six important variables may look a little different.

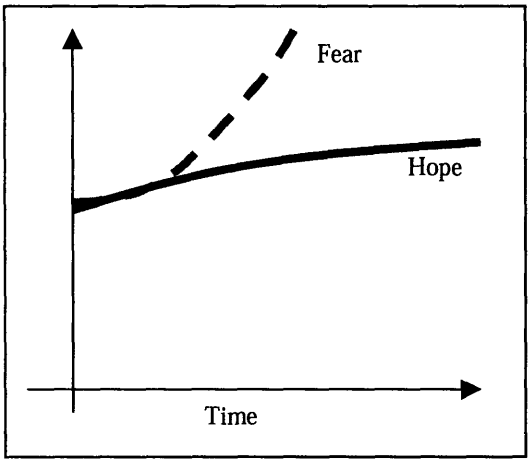
Variable #	6 Variables	Unit
1	Number of lawful-intercepts Required	#/year
2	% of voice traffic that is VoIP	
3	% of Voice Communications subjected to CALEA	
4	% of Voice Communications that can be wire-tapped	
5	% Intercepts that can be decrypted	
6	Cost of CALEA Compliance	$/intercept

Table 5. Six important variables for CALEA

Table 5 lists the six important CALEA variables. In the next subsection, the definition of each variable and their likely behavior will be discussed.

Reference Modes and Rough Dynamic Hypotheses

Variable 1: Number of Lawful Intercepts Required



Rough Dynamic Hypotheses

Hope:
- Intercepts required may rise, but will not rise exponentially

Fear:
- Intercepts required will rise exponentially due to post 9/11 syndrome

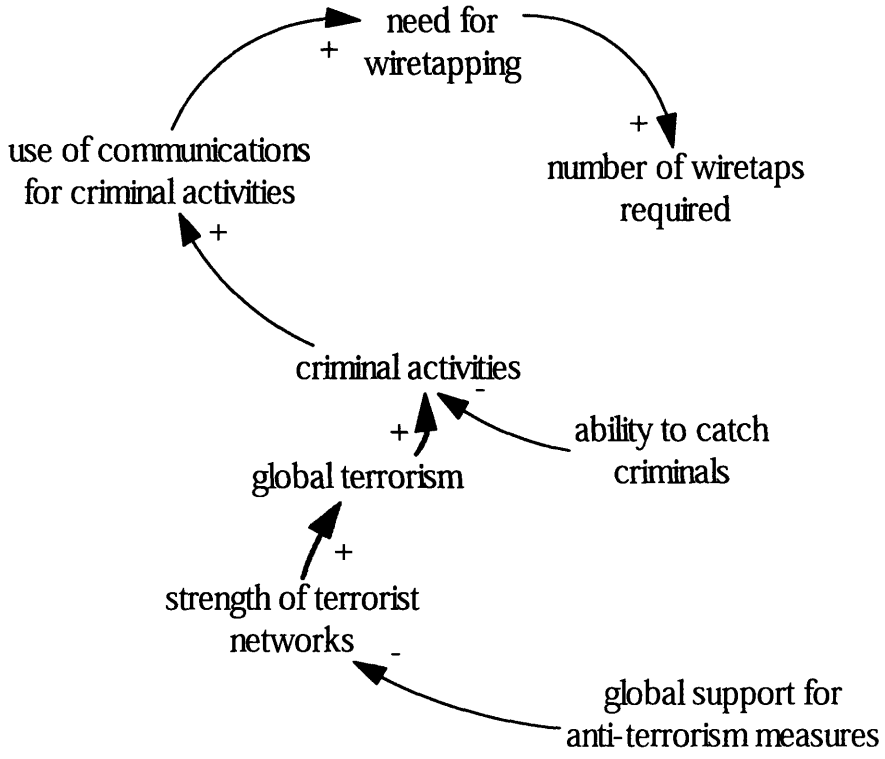


Figure 18 Reference modes and rough dynamic hypotheses for number of lawful intercepts required

Number of lawful intercepts required is the number of lawful intercepts (wiretaps) the US courts actually authorize. Figure 18 shows that our client, the LEAs or the FCC, hopes that the number of lawful intercepts required every year will rise at a steady pace, while they fear that it might rise rapidly compared to the past.

As shown in Figure 19, the number of wiretaps the US courts authorized have risen steadily for the past three decades. General increase in the use of electronic communications may have led to its higher use for criminal activities, and therefore the need for more wiretaps each year.

The LEAs or FCC's fear that the number of lawful intercepts required may rise significantly is from the threat of increase in global terrorism.

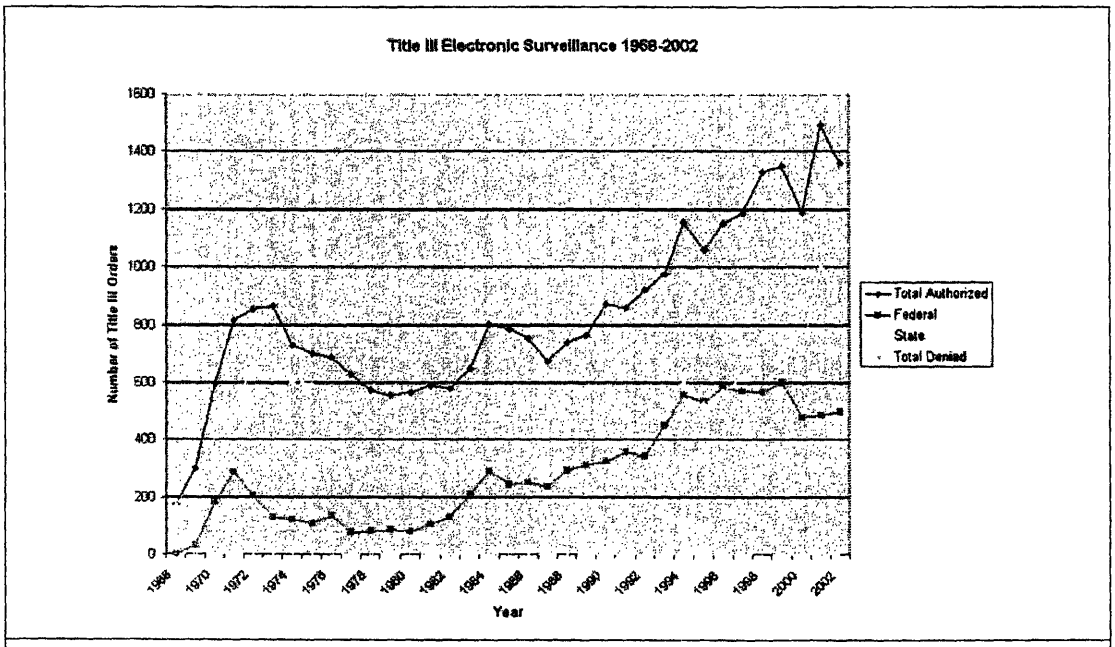


Figure 19 Number of Wiretaps authorized by US Courts between 1968 and 2002[45]

[45] Source: Administrative Office of the US Courts, See http://www.uscourts.gov/wiretap.html for 1997-2004 wiretap reports.

Variable 2: Percentage of Voice Traffic that is VoIP

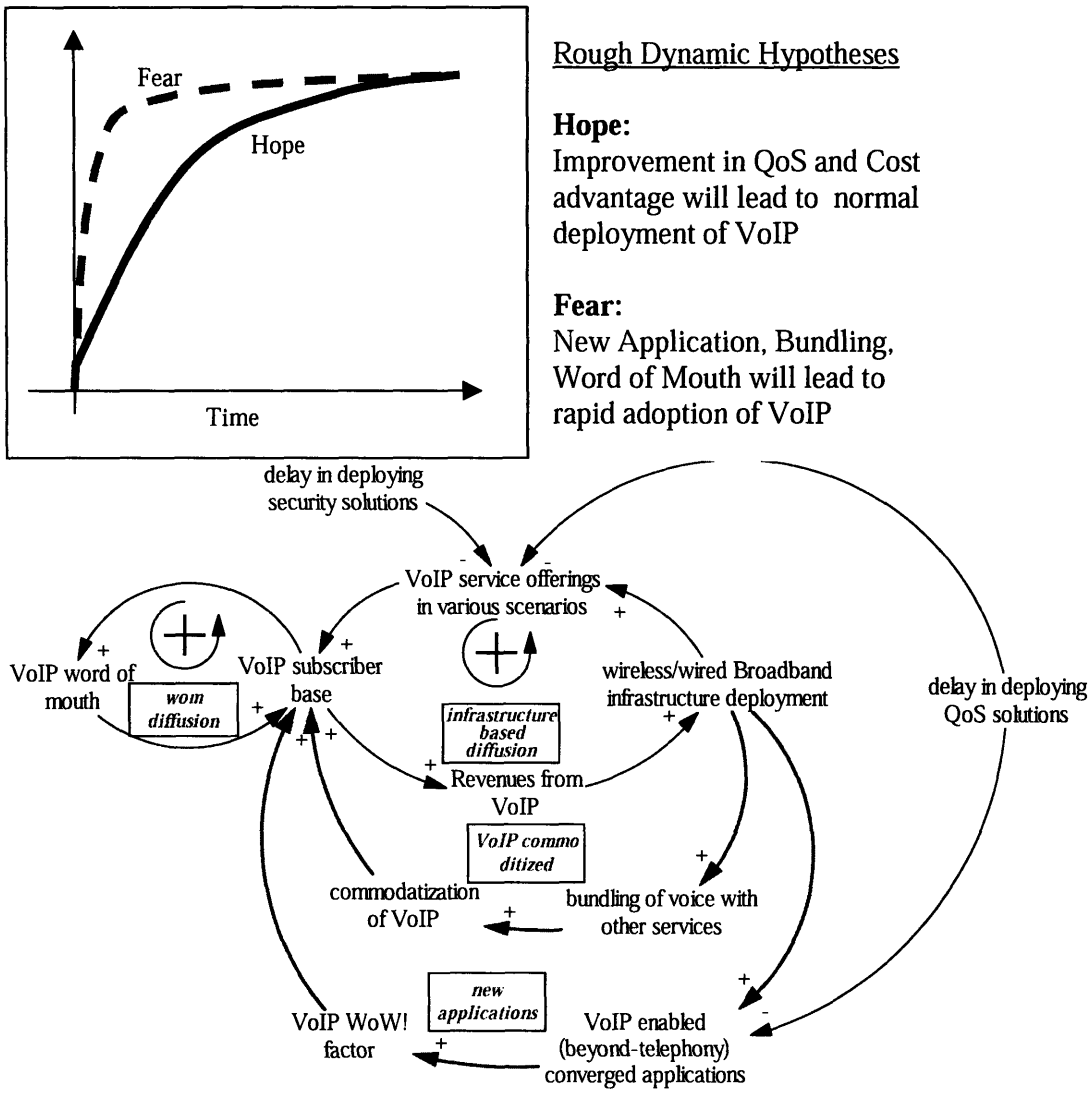


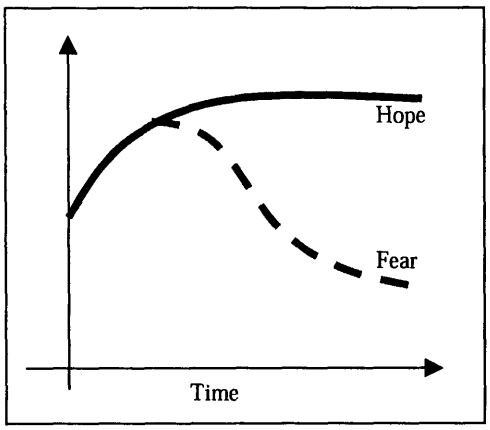
Figure 20 Reference modes and rough dynamic hypotheses for percentage of voice traffic that is VoIP

Percentage of voice traffic that is VoIP is the percentage of voice communication, as measured in their minutes of use (MOU), that is packet-voice, and not circuit-switched voice communications. Figure 20 shows the LEAs hope and fear for this parameter.

LEAs hope that lower costs of VoIP offerings will lead to customer migration. However, the diffusion will be slowed down by impediments such as QoS and security, which will take time to resolve. This may allow for the necessary re-engineering of the networks to ensure sufficient ability to wiretap.

LEAs fear that VoIP will lead to attractive applications, price bundling and commoditization of voice, thereby leading to bandwagon effect and rapid diffusion. Such a scenario will leave LEAs electronic surveillance capability far behind what may be necessary, if VoIP providers are not required to be CALEA compliant.

Variable 3: Percentage of Voice Communications Subjected to CALEA



Rough Dynamic Hypotheses

Hope:
Initially, only those VoIP scenarios that have a service provider will be regulated. Overtime, as CALEA compliant technology is available, all necessary scenarios will be regulated.

Fear:
More scenarios will be outside the jurisdictions. More service providers will be outside US. CALEA compliance will be technically infeasible.

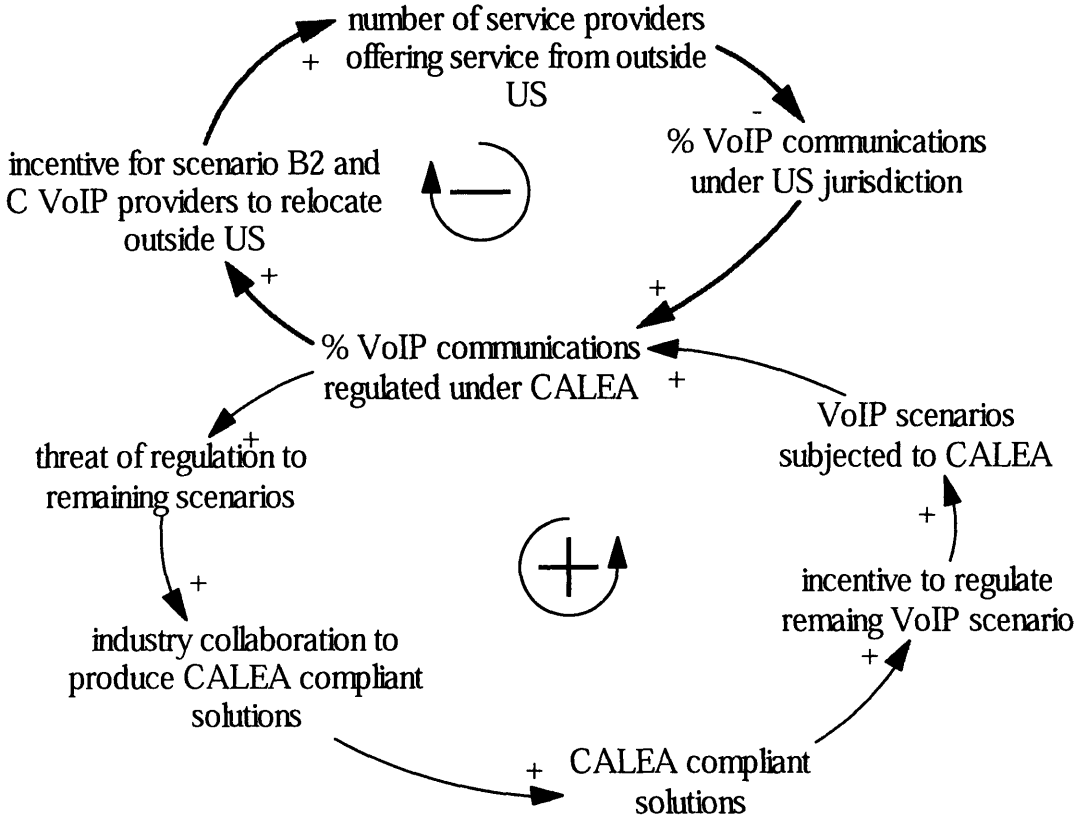


Figure 21 Reference modes and rough dynamic hypotheses for percentage of voice subjected to CALEA

Percentage of voice subjected to CALEA is the percentage of voice traffic that carried by the modes of voice communications currently subjected to CALEA. For example, as we stand today, only the telecommunication carriers are subjected to CALEA. Facility-based VoIP, VoIP over BB and P2P VoIP are not subjected to CALEA. Figure 21 show LEA's hope and fear for this parameter.

LEAs hope that the threat of CALEA would encourage industry players to collaborate and implement CALEA compliant technology. While initially, only some VoIP scenarios may be subjected CALEA, over time, there will be incentive to subject all scenarios to CALEA, as there will be technology available to enable that.

LEAs fear that since the layered architecture of VoIP allows for the service provider to locate their servers anywhere, globally; many service providers will offer services from outside US, thereby escaping the CALEA jurisdiction. Additionally, it is not clear how feasible, technically, is the dream of CALEA compliance for the packet-based voice. These factors, over time, may lead to only a small percentage of voice communications that are subjected to CALEA.

Variable 4: Percentage of Voice Communications that can be wiretapped

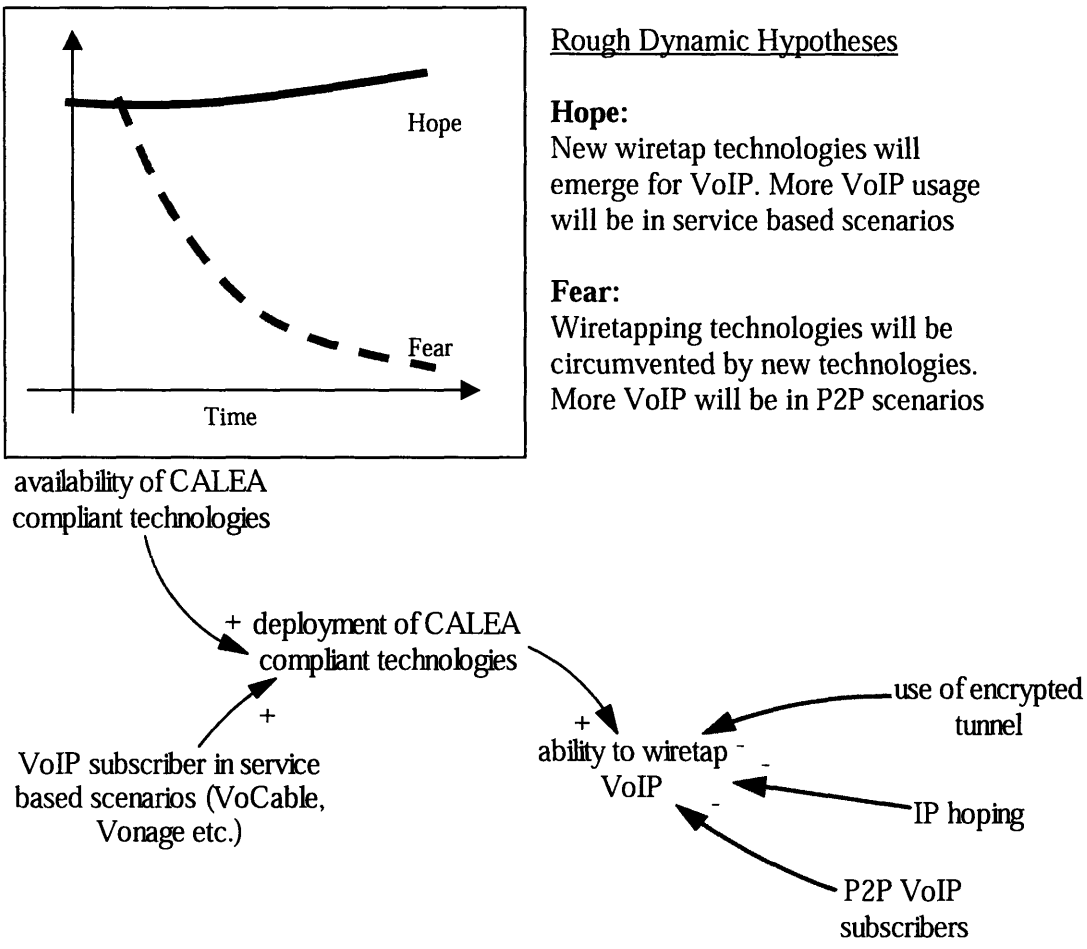


Figure 22 Reference modes and rough dynamic hypotheses for percentage of voice communications that can be wiretapped.

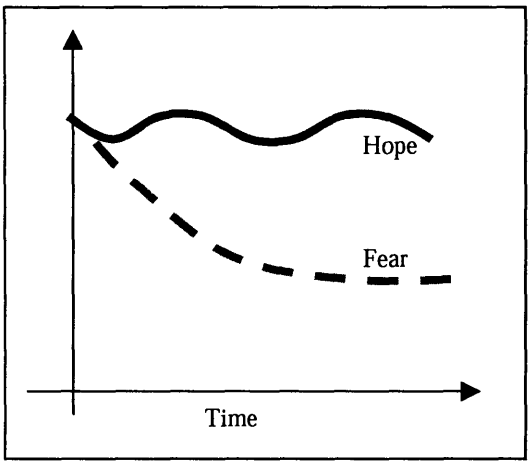
Percentage of voice communications that can be wiretapped is a measure of the percentage of voice communications for which wiretapping is technically feasible. Today, it is believed that to wiretap P2P VoIP is technically challenging. Figure 22 shows LEAs hope and fear for this parameter.

LEAs hope that more number of users will prefer VoIP service where there is a clear service provider, i.e. facility-based VoIP or VoIP over broadband. *The FCC calls these scenarios managed VoIP*[46]. The reason for this may be the service provider's brand recognition and perceived reliability. It is perceived that the managed VoIP scenarios it can be wiretapped with deployment of appropriate technology.

LEAs fear is that increasing number of users will migrate to P2P VoIP, or that with the advent of wiretapping techniques for packet-voice, there will be new technologies invented that circumvent the ability to wiretap. This will reduce the percentage of voice communications that can be wiretapped.

[46] FCC's CALEA NPRM. ET Docket No. 04-295, "we tentatively conclude that providers of VoIP services that Law Enforcement characterizes as "managed" or "mediated" are subject to CALEA as telecommunications carriers under the Substantial Replacement Provision. Law Enforcement describes managed or mediated VoIP services as those services that offer voice communications calling capability whereby the VoIP provider acts as a mediator to manage the communication between its end points and to provide call set up, connection, termination, and party identification features, often generating or modifying dialing, signaling, switching, addressing or routing functions for the user. Law Enforcement distinguishes managed communications from "non-managed" or "peer-to-peer" communications, which involve disintermediated communications that are set up and managed by the end user via its customer premises equipment or personal computer. In these non-managed, or disintermediated, communications, the VoIP provider has minimal or no involvement in the flow of packets during the communication, serving instead primarily as a directory that provides users' Internet web addresses to facilitate peer-to-peer communications."

Variable 5: Percentage Intercepts that can be decrypted



Rough Dynamic Hypotheses

Hope:
With the advent of new encryption scheme, ability to decrypt will lag; but then it will catch up, and the cycle continues (oscillations). Companies in privacy solutions will offer new solutions.

Fear:
New encryption methods be much difficult to decrypt.

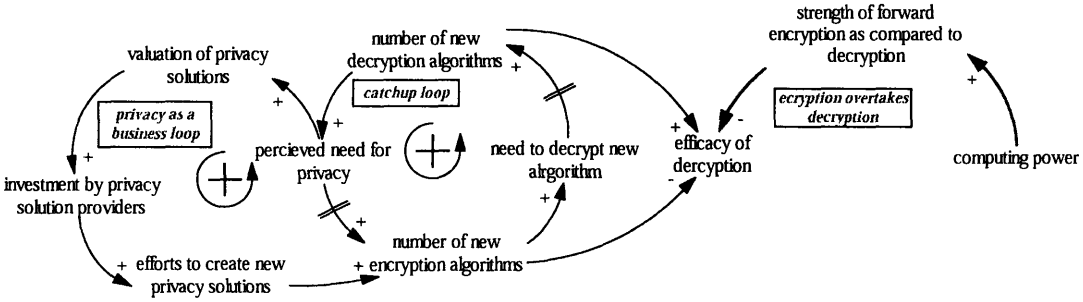


Figure 23 Reference modes and rough dynamic hypotheses for percentage intercepts that can be decrypted

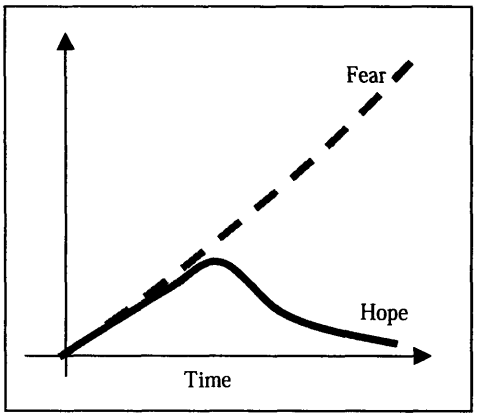
Percentage interrupts that can be decrypted is a measure of how much of the recorded information can be decrypted. Figure 23 shows the hope and fear of LEA for this parameter.

LEAs hope (or expect) that there will be an arms race between encryption and decryption techniques. When new encryption techniques will make the current methods of decryption obsolete, momentarily. After some time lag, new ways of decryption will be invented to catch up with the encryption methods. The same cycle will continue. The

ability to decrypt at a given point will determine how much of the wiretapped information can be decrypted.

LEAs fear that computing power will strengthen the ability to encrypt far ahead of the ability to decrypt. In such a case, it will not be possible to decrypt much of the information available from a wiretap.

Variable 6: Cost of CALEA Compliance



Rough Dynamic Hypotheses

Hope:
Industry will collaborate to find CALEA compliant solutions. Over time, the solutions will be available at low cost. Networks will be engineered to ease CALEA compliance.

Fear:
Perceived threat of Internet crime will lead to new security and privacy technologies, which will required new deployments for CALEA compliance.

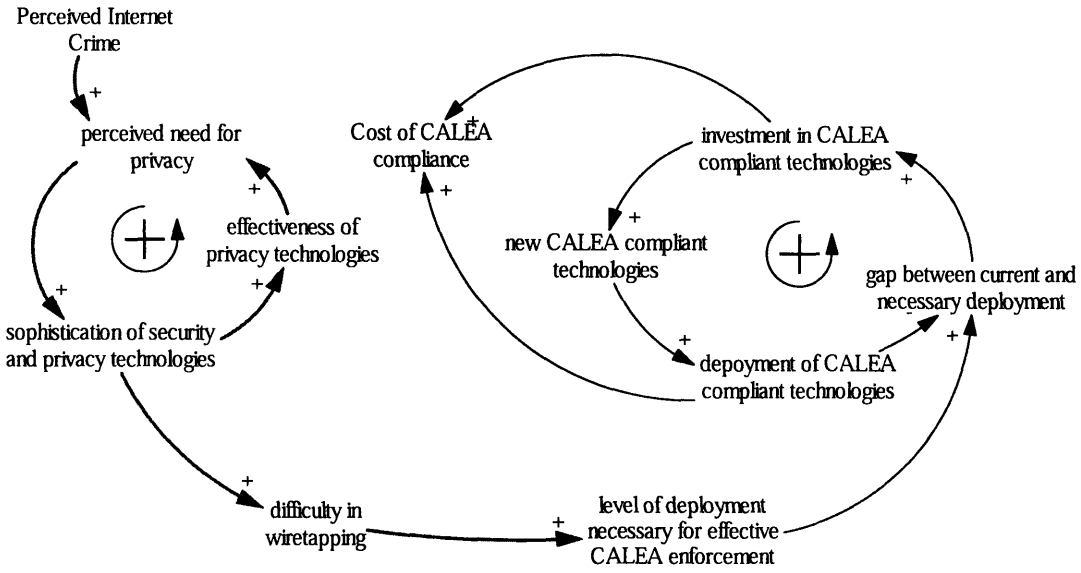


Figure 24 Reference modes and rough dynamic hypotheses for cost of CALEA compliance

Cost of CALEA compliance is the cost incurred by a service provider, and indirectly by the LEA, to comply with CALEA. Figure 24 shows LEA's hope and fear for this parameter.

LEAs hope that initially, as CALEA compliant technology is deployed, the compliance costs will go up. However, beyond a point the deployment will be nearly

sufficient, hence the costs of CALEA compliant will only be the operational cost of performing a wiretap, and not the capital investment required for new deployment.

LEAs fear that perceived threat of Internet crime will lead to newer security and privacy technologies. The average user will use more sophisticated techniques to be more secure and protect their privacy. This will lead to higher and higher costs of CALEA compliance.

CALEA CAUSAL LOOPS

Simplified Version

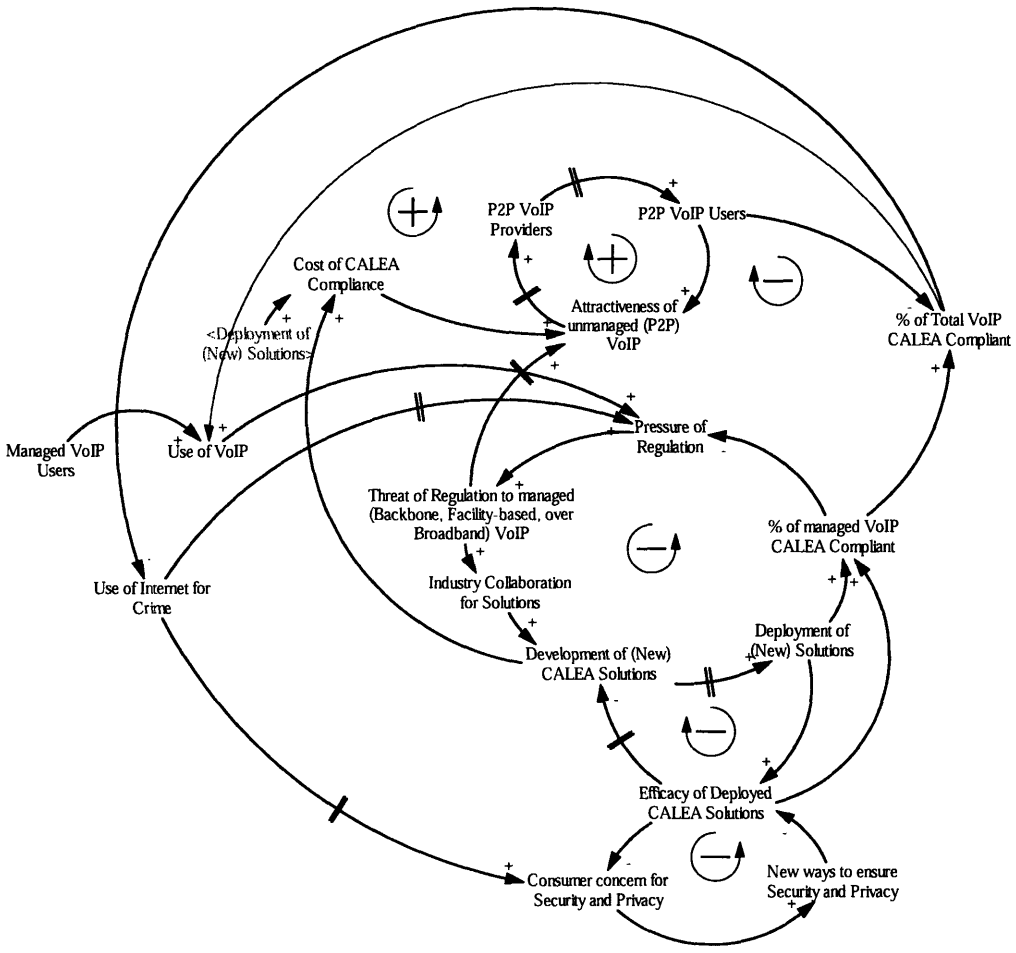


Figure 25 CALEA Causal Loops: Simplified Version

Figure 25 and Figure 26 show the basic and complete causal loop diagrams for CALEA, respectively. These are constructed by combining the causal loops related to each of the reference modes discussed above. In the process of creating the causal loop diagrams,

many redundant variables are dropped. Having discussed individual dynamic hypotheses for the six variables, the causal loops in Figure 25 and Figure 26 are self-explanatory. In the next section, we will develop the CALEA stock and flow model.

Complete Version

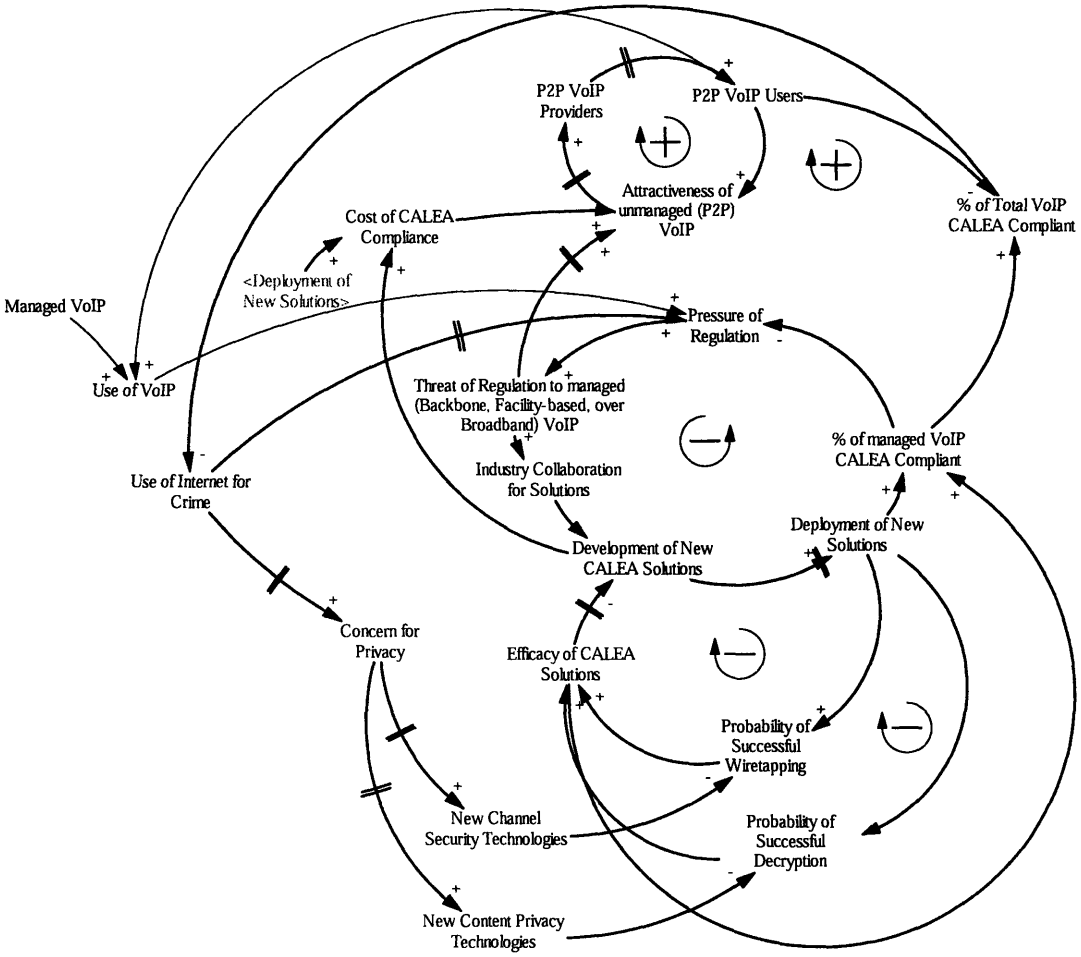


Figure 26 CALEA Causal Loops: Complete Version

CALEA - STOCK AND FLOW MODEL

In this section we will develop a sock and flow model for further analysis. We will first describe various parts of the model and the related assumptions. We will then discuss parameter initialization with the help of various data sources.

Model Construction and Assumptions

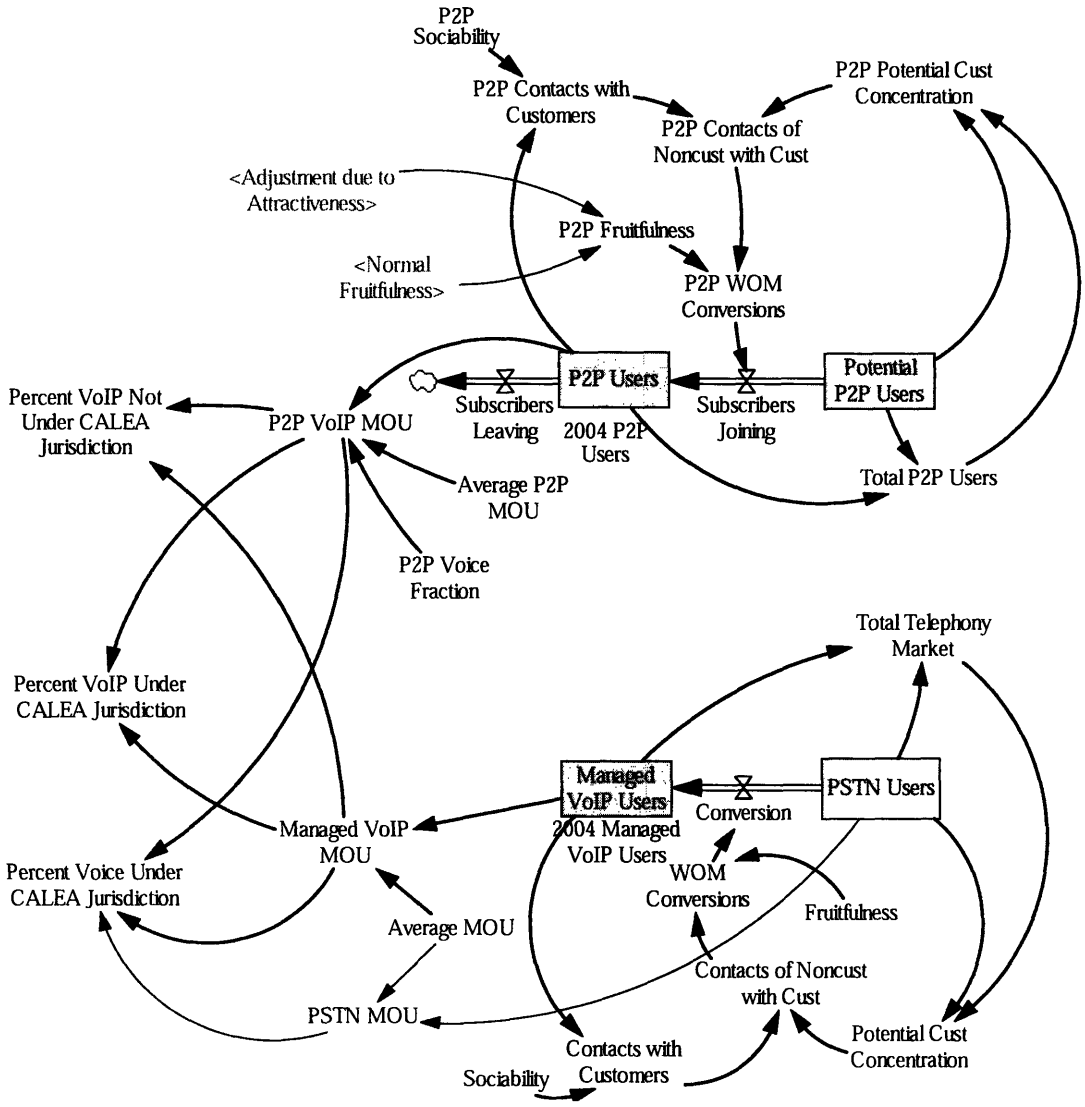


Figure 27 CALEA stock-flow model: VoIP Diffusion

Figure 27 show the VoIP diffusion of "managed" (i.e. VoIP in the backbone, facility-based VoIP and VoIP over Broadband) or "mediated" VoIP services, as well as the peer-to-peer VoIP services.

Following are the assumptions made here:

1. Currently PSTN users convert to Managed VoIP users.
2. P2P uses may substitute some of their total voice MOU with P2P VoIP, but do not entirely give up their PSTN or managed-VoIP service.
3. Only a fraction of total P2P traffic is voice.
4. Managed VoIP services will be subjected to CALEA, while P2P will not[47].
5. Total telephony market is the number of connections; whereas, potential P2P users are larger than the total telephony market, as there may be multiple users per household.

Conversion of PSTN users to managed VoIP users, or the potential P2P users to P2P users, occurs as a result of the word of mouth (WOM) conversion. WOM itself depends upon the sociability, i.e., how often a user comes in contact with a non-user, and the fruitfulness of that contact, i.e. how many contacts result in an actual conversion. To keep the model simple, factors that impact sociability or fruitfulness over time are not mentioned here. For example, it is conceivable that the fruitfulness may be affected by other factors such as technology attractiveness. Technology attractiveness is in turn impacted by factors such as reliability, quality, cost etc. However, exactness of VoIP diffusion is not the goal of this model. The goal here is to observe the impact of VoIP

[47] This assumption is already supported by the recent CALEA order. See www.fcc.gov for the official announcement.

diffusion on CALEA compliance.

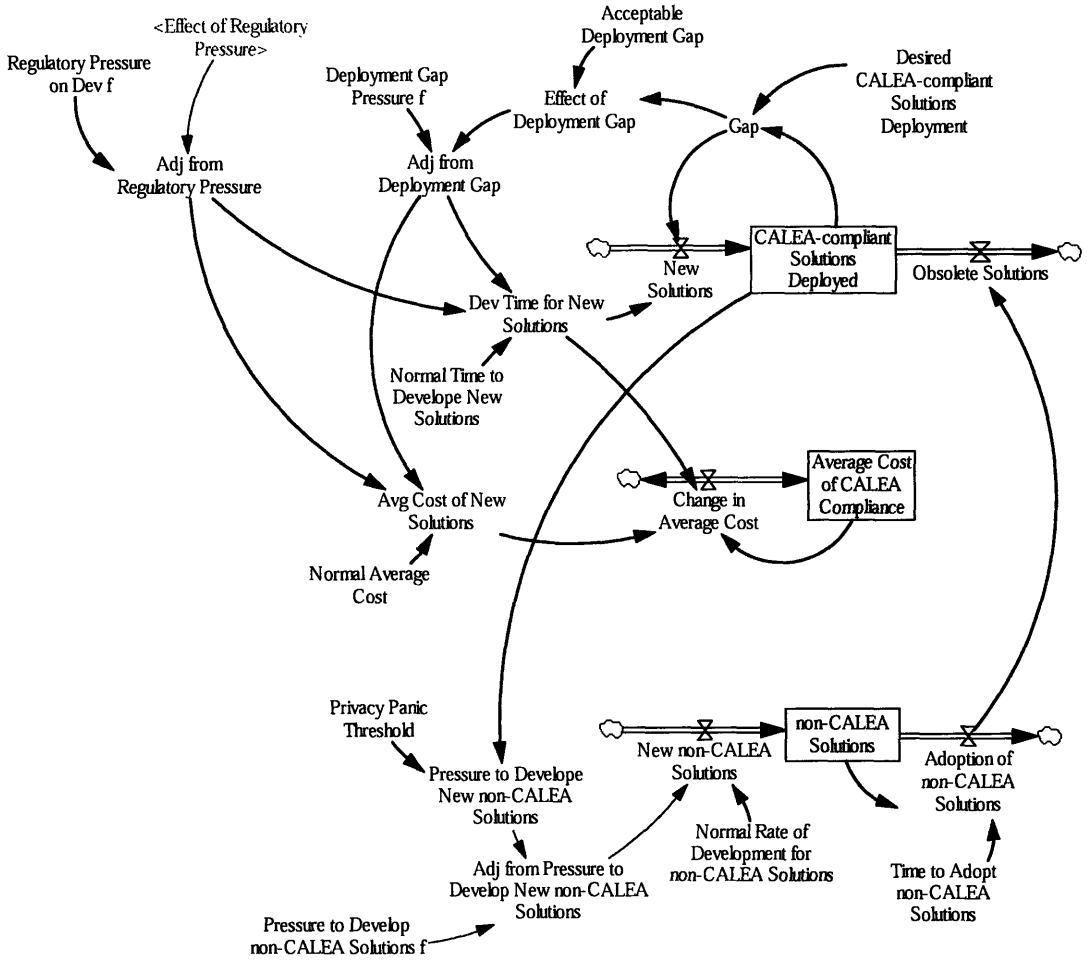


Figure 28 CALEA stock-flow model: CALEA compliance

Figure 28 shows the section of the stock-flow model that deals with development and deployment of CALEA-compliant solutions and its associated costs. It also depicts the arms race between the CALEA-compliant solutions and the non-CALEA solutions.

Following are the assumptions made here:

1. The LEAs have a threshold (an anchor) percentage of voice communications that they would like to be able to wiretap. For example, they may want the

ability to wiretap 90% of all voice communications. If the actual wiretapping capability falls below this threshold, there will be pressure to develop new CALEA-compliant solutions.

2. Average cost of CALEA compliance depends resources used for development.
3. When there is pressure to develop solutions faster, more resources will be required and hence higher will be the cost of compliance.
4. Hackers and other users of managed-VoIP service have a privacy panic threshold. When they feel their privacy is invaded by the ability to wiretap, they may develop new non-CALEA compliant solutions.

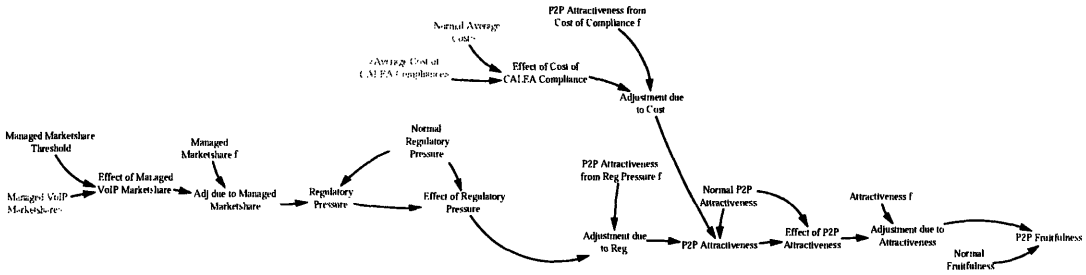


Figure 29 CALEA stock-flow model: Impact of CALEA on P2P VoIP

Figure 29 shows the part of the stock-flow model that depicts the impact of CALEA on the P2P VoIP diffusion. The assumption here is:

1. Cost of CALEA compliance and regulator pressure on managed VoIP services will provide more incentive for offering P2P VoIP.

It is important to note that this assumption needs some more thinking. There is no clear business model in the P2P VoIP market. No P2P VoIP offering is making money, unless they provide PSTN interconnection. However, providing PSTN interconnection makes the service a managed or mediated one, and hence regulated. However, it is conceivable that threat of regulation and the need to develop or pay for CALEA compliance may promote P2P use among trusted namespaces (communities).

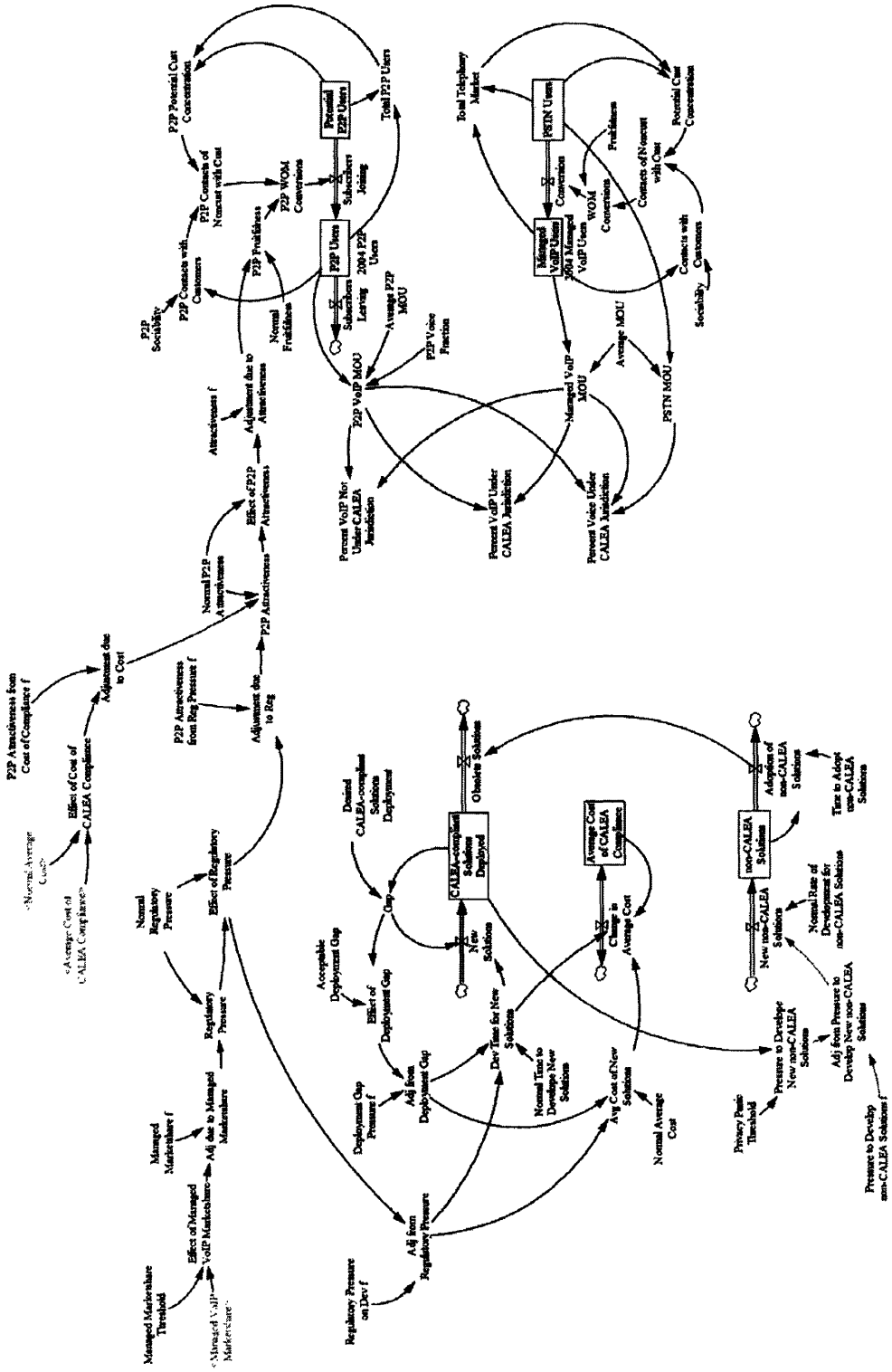


Figure 30 Complete CALEA stock-flow model

Figure 30 shows the complete stock-flow model for CALEA. We will now discuss the initialization of parameters and the relevant information sources.

Parameter Values and Ranges

Variable	Value	Unit	Range	Rationale	Source
PSTN Users	1.77E+08	Subscribers	N/A	Number of PSTN Lines in 2004 (US only)	[24])
2004 Managed VoIP Users	1.00E+06	Subscribers	0 - 6.00E+06	Number of Subscirbers for Residential VoIP Service at the end of 2004 (US only)	[25])
Potential P2P Users	2.00E+08	Subscribers	N/A	Potential P2P (Voice and Data) uses (US only)	Approximated to a little higher than the number of residential telephony subscribers, as there may be more than one P2P account holder at home. Alternatively, set to approximately 60% of the US population.
2004 P2P Usres	1.00E+06	Subscribers	0 - 40.00E+06	Number of P2P users in the US at the end of 2004	Set to a conservatively low number, considering 40 million broadband subscribers today.
Sociability	6	contact/(month*subscriber)	0 - 50	Number of contacts a managed VoIP service subscriber has with a non-subscriber every month	Set to achieve IDC's forecast of 27 million managed VoIP service subscribers by 2009.
Fruitfulness	0.01	subscriber/contact	0 - 1	Number of contacts it takes to convert a non-subscriber to a subscriber of managed VoIP service (The value is set to inverse of this. So, in this case, 0.01 means it takes 100 contacts to convert 1 subscriber)	Set to achieve IDC's forecast of 27 million managed VoIP service subscribers by 2009.
P2P Sociability	Sociability	contact/(month*subscriber)	0 - 50	Number of contacts a P2P user has with a non-P2P user every month	Sociability is assumed to be the same as derived before.
P2P Fruitfulness	Fruitfulness	subscriber/contact	0 - 1	Number of contacts it takes to convert a non-P2P user to a P2P user	Fruitfulness is assumed to be the same as derived before.
Average MOU	121	minutes/(month*subscriber)	0 - 200	Agerage minutes of use per month for a residential telephony customer.	Ageraged from the the average usage from 1995 to 2003.

Variable	Value	Unit	Range	Rationale	Source
Average P2P MOU	100	minutes/(month*subscriber)	0 - 200	Agerage minutes of use per month for a P2P customer.	Approximation
P2P Voice Fraction	0.1	dimensionless	0 - 1	Fraction of P2P traffic that is voice	Voice P2P approximated to 10% of the total P2P traffic.
Desired CALEA-compliant Solutions Deployment	100	solutions	0 - 100	Equivalent of the percentage of voice communications that the LEA desires to wiretap	
Acceptable Deployment Gap	10	solutions	0 - 100	Percentage of voice communications that the LEA can live without wiretapping	Approximation
Normal Time to Develop New Solutions	6	months	1 - 30	Set to 1/3 of time all of the CALEA solutions are expected to take. The value is set to 1/3 of 18 months, the time FCC expects the industry to take in achieving CALEA compliance. This entity is modeled as a smooth, and a smooth takes 3 time periods to reach 95% of its final value.	
Privacy Panic Threshold	50	solutions	0 - 100	Equivalent of the percentage chance that a hacker or criminal's voice communications will be successfully wiretapped that will make them worried.	Approximation
Normal Rate of Development for non-CALEA Solutions	6	solutions/month	1 - 30		Approximation
Time to Adopt non-CALEA Solutions	Normal Time to Develop New Solutions	months	1 - 30	Hackers take the same time the industry takes in delpoying solutions.	
Normal Average Cost	1	Dollar/solution	0 - 5	Cost of developing and deploying solution for wiretapping a single percentage of managed VoIP communications	Used as a reference

Variable	Value	Unit	Range	Rationale	Source
Managed Marketshare Threshold	0.1	dimensionless	0 - 1	Managed VoIP market share beyond which LEA/FCC will have a pressure to regulate managed VoIP service	Used for analysis
Normal Regulatory Pressure	1	unitRegPressure	0 - 3	Normal level of pressure to regulate managed VoIP service.	Used as a reference
Normal P2P Attractiveness	1	unitAttractiveness	0 - 3	Normal level of P2P attractiveness	Used as a reference
Subscrivers Leaving	0	subscribers	N/A	Normal P2P users leaving P2P	Currently assumed that no P2P users ceases to use it.

Table 6. Parameter Selection for CALEA Model

Chapter 6

MODEL ANALYSIS AND POLICY LESSONS FOR CALEA

In this chapter we will discuss results of the model analysis and the policy lessons resulting from it.

MODEL BEHAVIOR

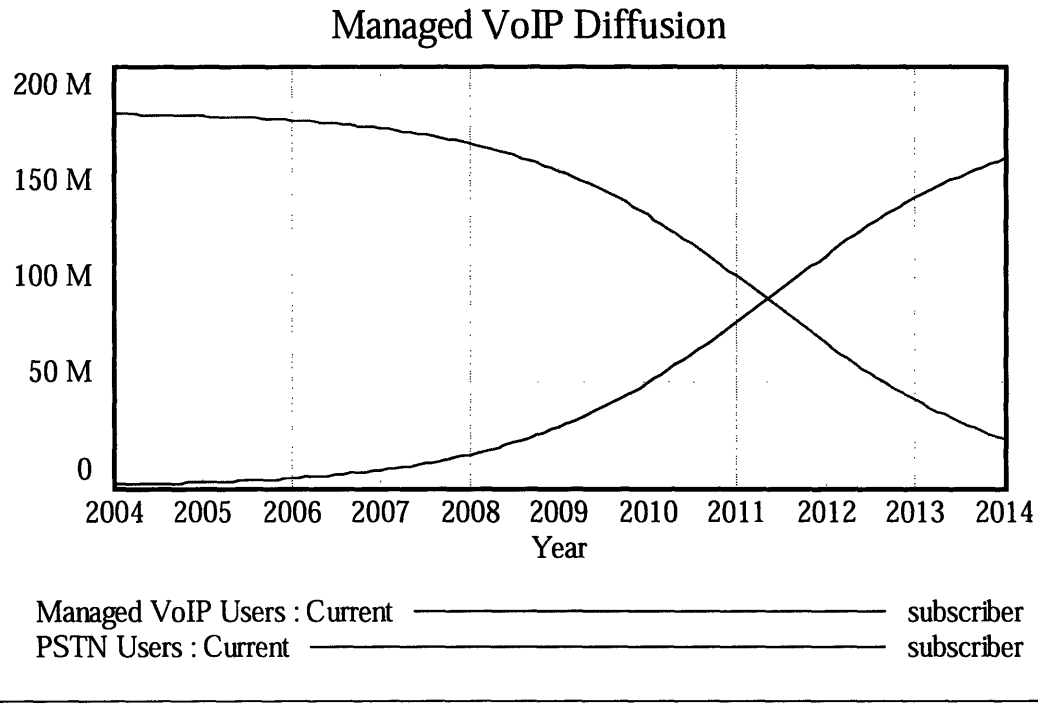


Figure 31 Managed VoIP Diffusion

Figure 31 shows the conversion of PSTN users into Managed VoIP (i.e. facility-based VoIP or VoIP over Broadband classes). The model parameters are set to the values in Table 6. According to this model, the crossover point between PSTN and Managed VoIP Service users is between year 2011 and 2012.

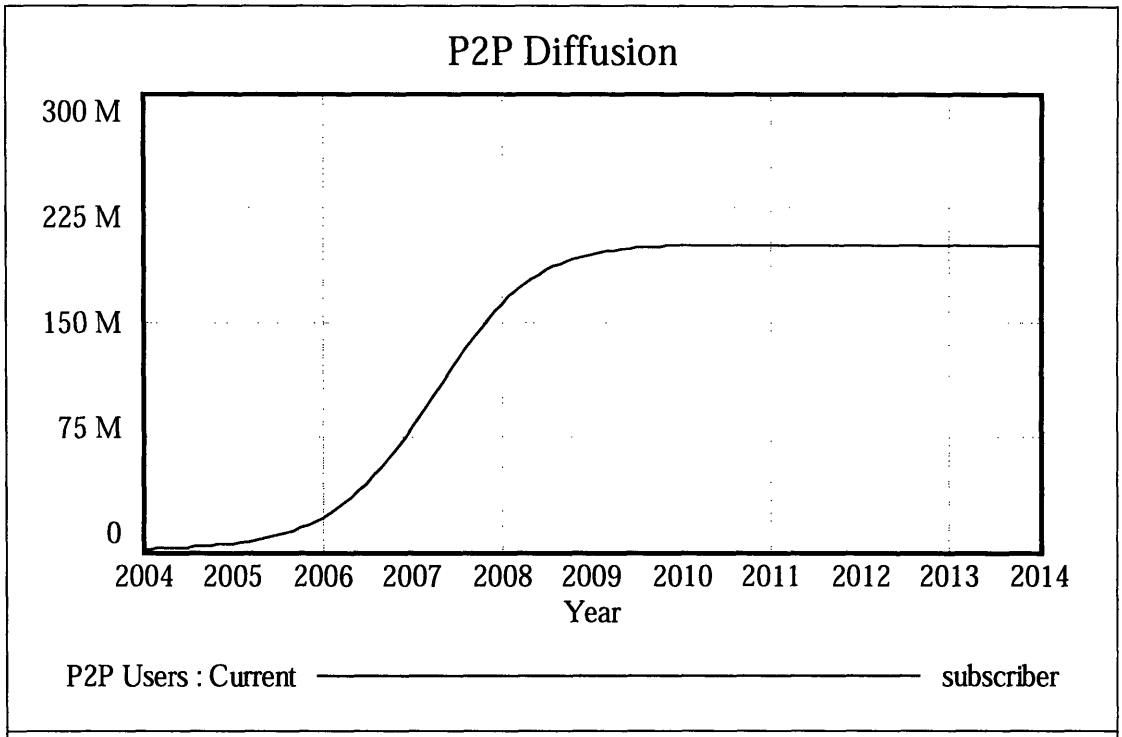


Figure 32 P2P Diffusion

Figure 32 shows diffusion of P2P users. Here, the sociability and fruitfulness of P2P users is assumed to be the same as that of managed VoIP users. Comparing Figure 32 with Figure 31 shows that diffusion of P2P users is quicker than that of managed VoIP users. This is an artifact of the way P2P Fruitfulness is modeled. P2P Fruitfulness impacted by P2P Attractiveness, which is in turn affected positively by the raising cost of CALEA compliance in managed VoIP.

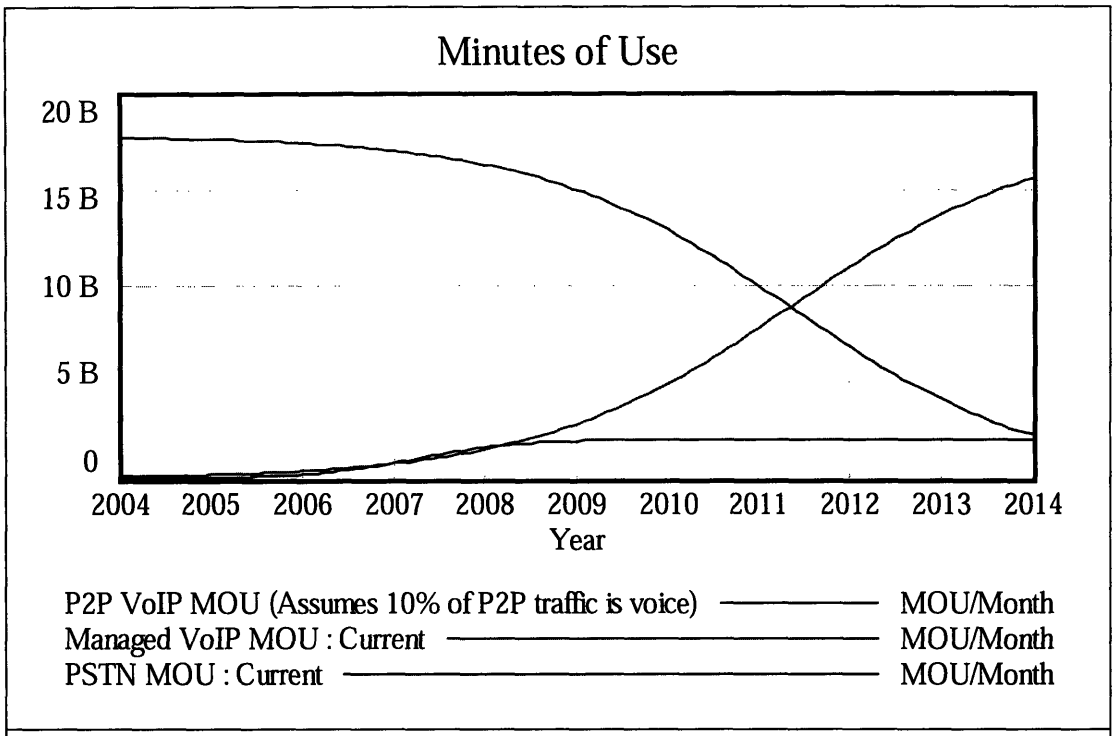


Figure 33 Minutes of Use

Figure 33 shows the minutes of use (MOU) for PSTN, managed VoIP and P2P VoIP. P2P VoIP MOU is only a fraction of the total VoIP (i.e. managed VoIP + P2P VoIP) because P2P Voice Fraction is set to 0.1 (10%) of the total P2P traffic for this model.

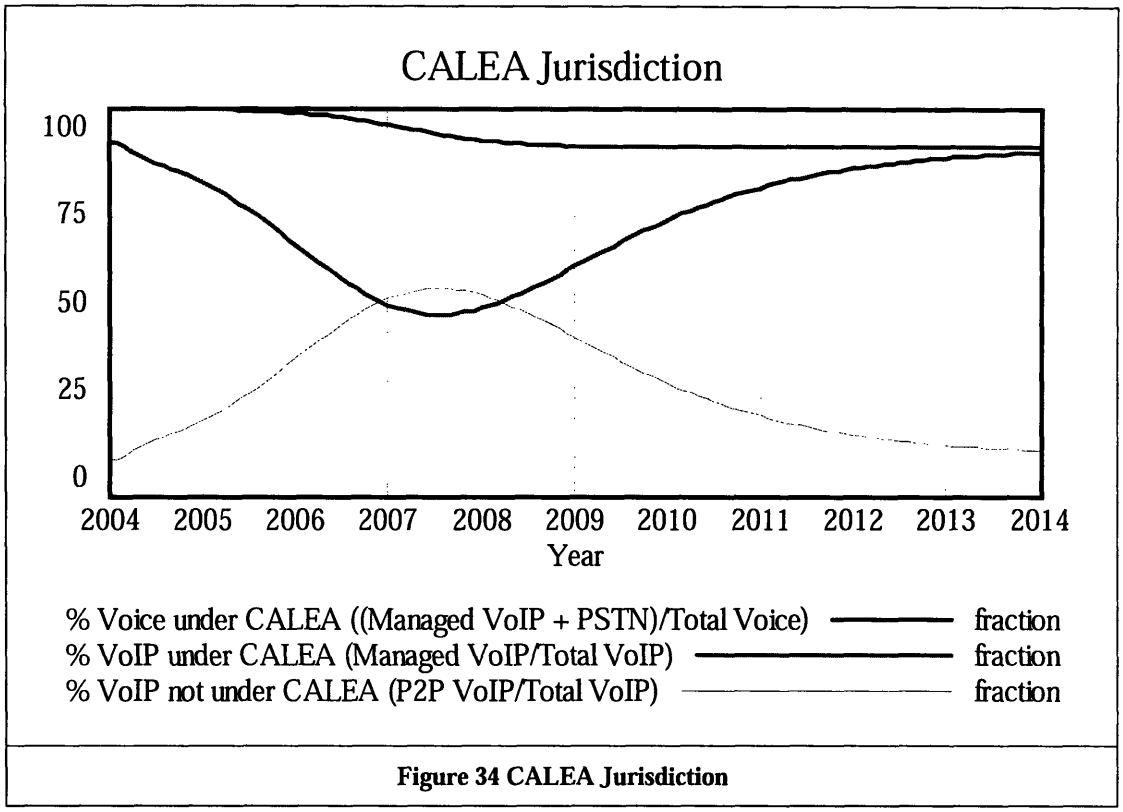


Figure 34 CALEA Jurisdiction

Figure 34 shows curves related to CALEA jurisdiction. % Voice under CALEA includes the PSTN plus managed VoIP fraction of the total voice MOU. The FCC's recent order[48] declared that, "certain broadband and interconnected voice over Internet Protocol (VoIP) services must be prepared to accommodate law enforcement wiretaps." In our VoIP

[48] The FCC's new release of August 05, 2005, titled "FCC Requires Certain Broadband and VoIP Providers to Accommodate Wiretaps Order Strikes Balance Between Law Enforcement, Innovation" declared that Washington, D.C. – Responding to a petition from the Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Agency, the Commission determined that providers of certain broadband and interconnected voice over Internet Protocol (VoIP) services must be prepared to accommodate law enforcement wiretaps, the Federal Communications Commission ruled today.

The Commission found that these services can essentially replace conventional telecommunications services currently subject to wiretap rules, including circuit-switched voice service and dial-up Internet access. As replacements, the new services are covered by the Communications Assistance for Law Enforcement Act, or CALEA, which requires the Commission to preserve the ability of law enforcement agencies to conduct court-ordered wiretaps in the face of technological change.

classification, discussed in Chapter 2, this translates to two classes of VoIP, facility-based VoIP and VoIP over Broadband, which we collectively call managed VoIP (using this term from VoIP NPRM).

Figure 35 shows what causes the CALEA jurisdiction curves in Figure 34 to behave as such. Figure 35 (a) shows the causal trace of % Voice under CALEA. Total voice traffic constitutes PSTN, managed VoIP and P2P VoIP. With the P2P VoIP diffusion, which is the part left out by the recent CALEA order, the fraction of total voice under CALEA jurisdiction declines.

Figure 35 (b) shows what causes the % VoIP under CALEA to behave as such. Total VoIP traffic constitutes managed VoIP plus P2P VoIP. % VoIP under CALEA jurisdiction declines with the increase in P2P VoIP MOU. As the P2P VoIP MOU plateaus, and managed VoIP MOU continues to rise, the %VoIP under CALEA goes back up. The % VoIP not under CALEA behaves exactly in the opposite manner, as shown in Figure 34.

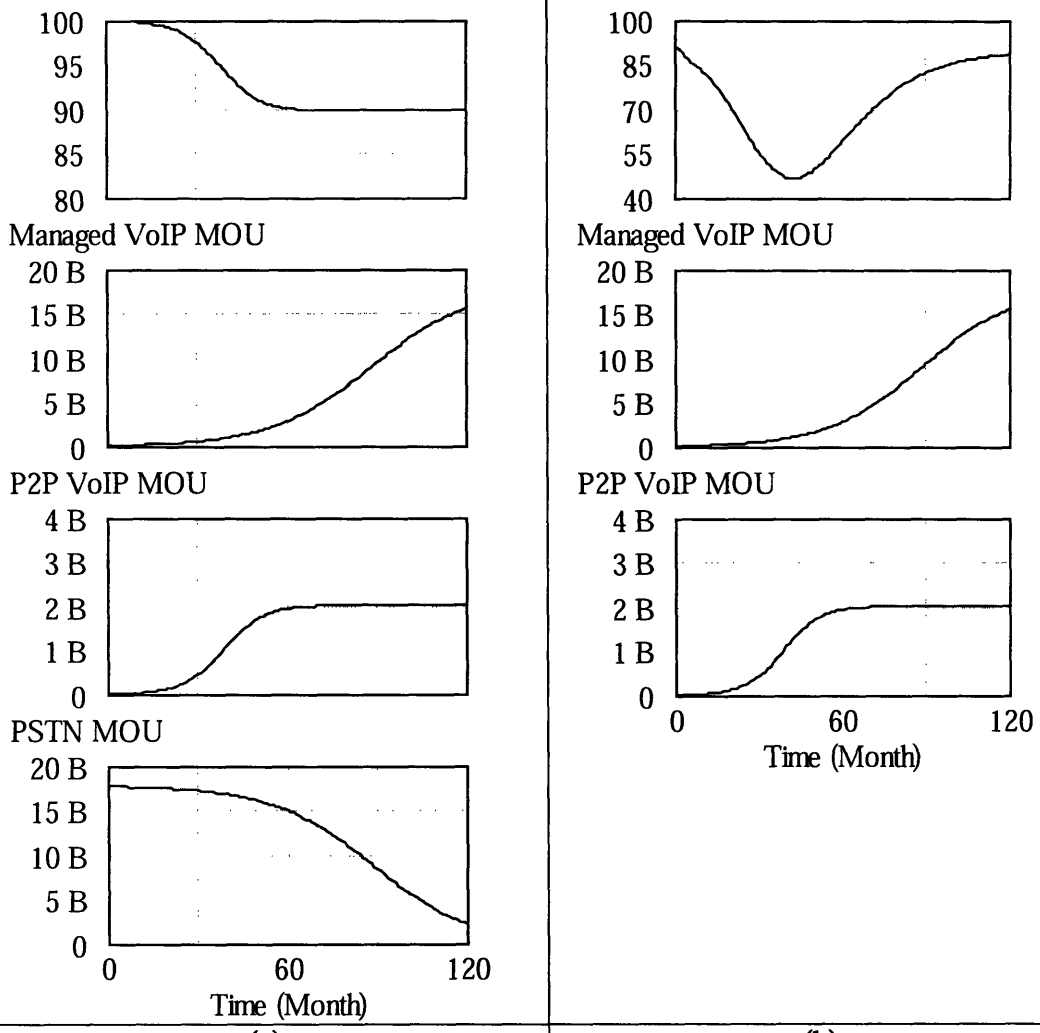
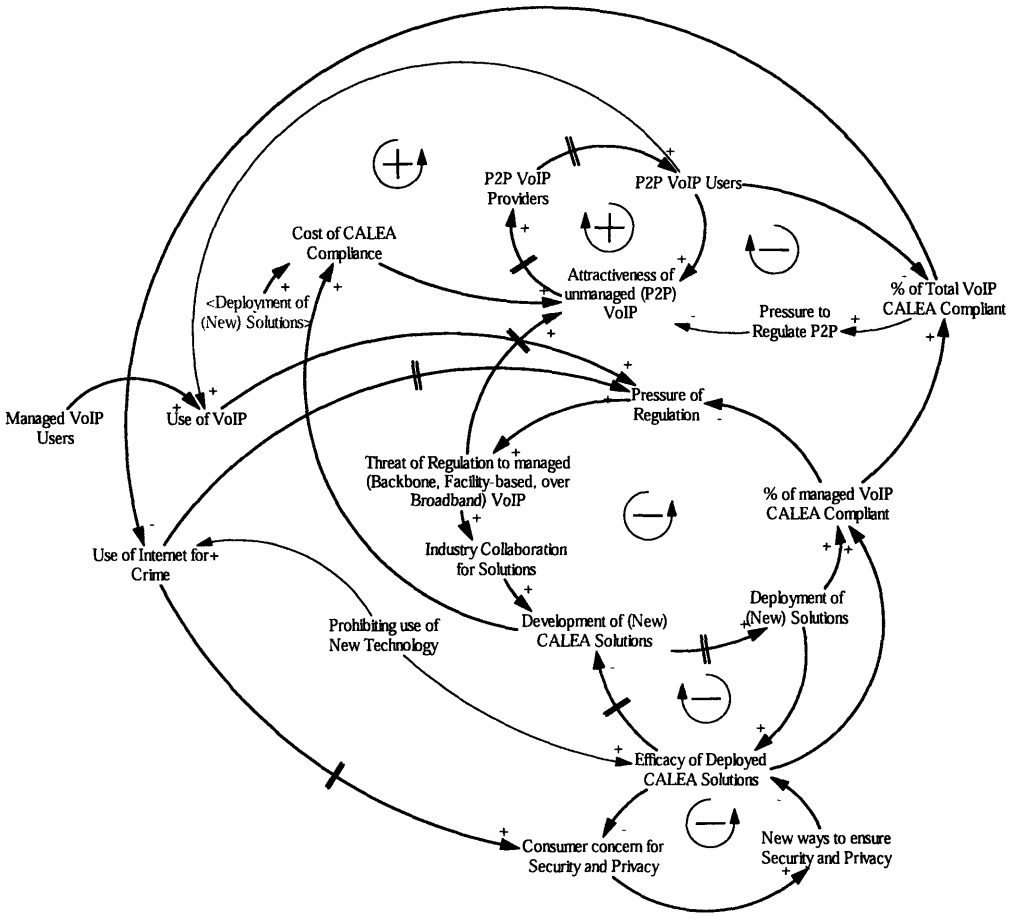


Figure 35 CALEA Jurisdiction causal trace

SENSITIVITY ANALYSIS AND POLICY LESSONS



1. **Considering P2P a non-issue for CALEA is exactly what might make it an issue.**
2. **If P2P aspires to become a telephony substitute, it will invite the threat of regulation**
3. ***Arms race between CALEA-compliant and non-compliant technologies may raise the cost of compliance.***
4. **Prohibiting use of certain encryption techniques may help the LEA to keep their ability to wiretap intact, but it also deprives consumers of the privacy the prohibited schemes would have offered.**

Figure 36 CALEA Causal Loops with Policy Insights

Figure 36 shows the basic causal loop diagram with major insights. The insights emerge through the process of arriving at the model, and through the subsequent sensitivity analysis.

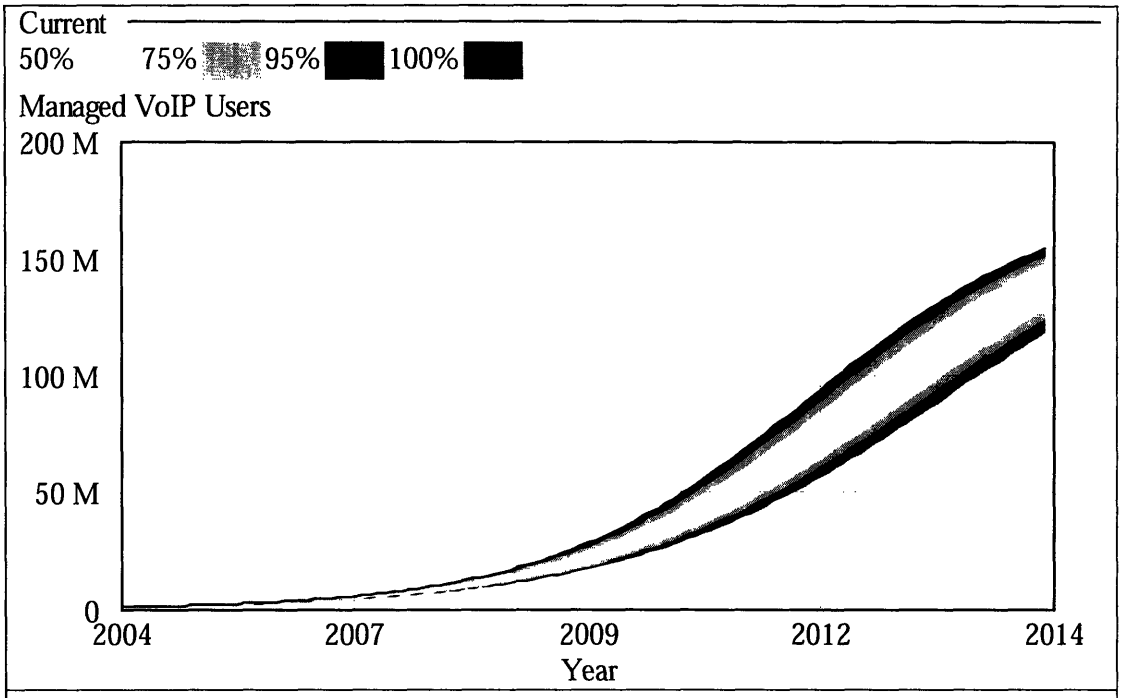


Figure 37 Sensitivity Analysis: Sensitivity of Managed VoIP Users to varying Sociability

Figure 37 shows the sensitivity of managed VoIP diffusion when varying the sociability. The sociability is varied to match the upper and lower bound of the analyst prediction. The upper bound – with Sociability = 6 and Fruitfulness = 0.01 – matches the number of managed VoIP users = 27 million by 2009, as predicted by the International Data Corp [26]. Whereas, the lower bound – with Sociability = 5 – matches the number of managed VoIP users = 17 million, as predicted by the Yankee Group [27]. The sensitivity graph of managed VoIP users shows bounds with different confidence intervals within which the diffusion occurs.

Policy Lesson 1: Considering P2P a non-issue for CALEA is exactly what might make it an issue.

In CALEA NPRM[49], the LEA indicated and the FCC tentatively concluded that the P2P or non-managed VoIP should not be subject to CALEA. Although, for variety of reasons P2P may be exempted from CALEA at this point, such an exemption expedites the need for regulating P2P VoIP under CALEA. Currently, P2P VoIP may be exempt from CALEA as its share of total voice traffic is very small, it is technically harder to wiretap P2P traffic, and there is a tension between regulation and innovativeness.

Diffusion of P2P VoIP reduces the % voice communications under CALEA jurisdiction. If variance similar to managed VoIP is introduced in P2P, by setting P2P Sociability = Sociability = 5 – 6 contacts/(month * subscriber), and the P2P Voice Fraction is varies between 5% and 20% of the total P2P traffic, the P2P VoIP diffusion can have a considerable impact on CALEA jurisdiction.

Figure 38 how sensitive is CALEA jurisdiction to the P2P VoIP diffusion. Figure 38(a) shows that with the aforementioned variance in P2P diffusion, % voice under CALEA jurisdiction can be as low as 82%. In other words, 18% of voice traffic would be legally exempt from wiretapping.

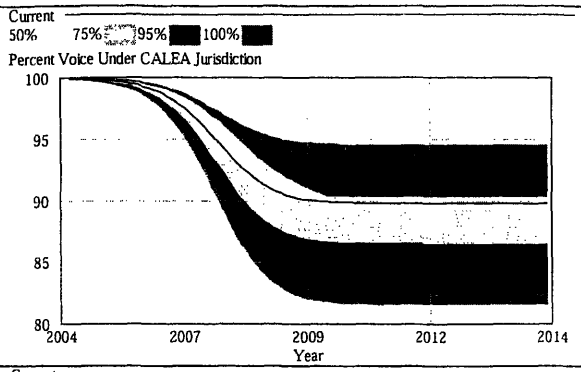
Figure 38(b) and (c) show how % VoIP under CALEA jurisdiction is impacted. As high as 70% of VoIP traffic may be outside of the CALEA jurisdiction at one point, given the diffusion rates assumed in the model.

Finally, Figure 38(d) shows how P2P VoIP diffusion, and the resulting pressure to increase CALEA compliance may drive the cost of CALEA compliance higher.

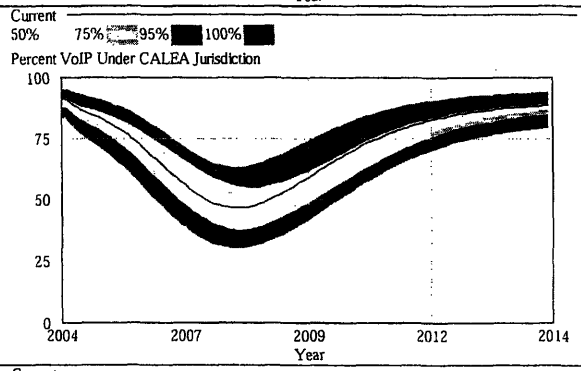
---

[49] FCC's CALEA NPRM. ET Docket No. 04-295, item 54, 55 and 57

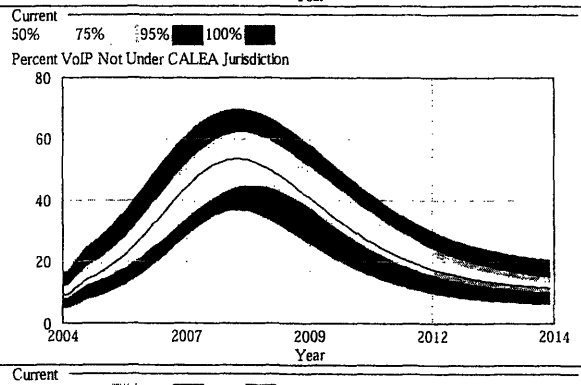
(a)



(b)



(c)



(d)

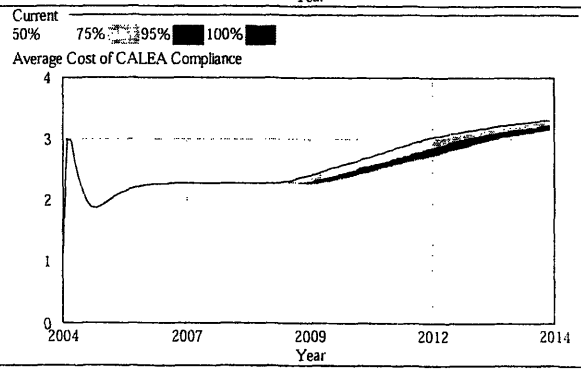


Figure 38 Sensitivity Analysis: Sensitivity of CALEA Jurisdiction and Compliance Cost to varying P2P and Managed VoIP Diffusion

Policy Lesson 2: If P2P aspires to be a telephony substitute, it will invite the threat of social regulation.

P2P VoIP experience has shown that there are no clear business models in this space. The only way any P2P VoIP provider has ever made money is to provide PSTN interconnection. Interconnection with PSTN or substitution of PSTN traffic, however, is a way to invite regulation. Today, under current statutory environment, the language and definitions permit regulation of a voice service that interconnects with PSTN, thereby satisfying the three prongs of the Substantial Replacement Provision with respect to VoIP services.[50] Additionally, if substantial amount of telephony traffic is substituted with P2P voice, it will invite social regulation such as CALEA and 911. The innovative freedom of the P2P technology would be kept unaffected only if the technology providers use innovative ways and solutions to remain viable and do not aspire to be telephony substitutes.

Policy Lesson 3: Arms race between CALEA-compliant and non-compliant technologies may raise the cost of compliance.

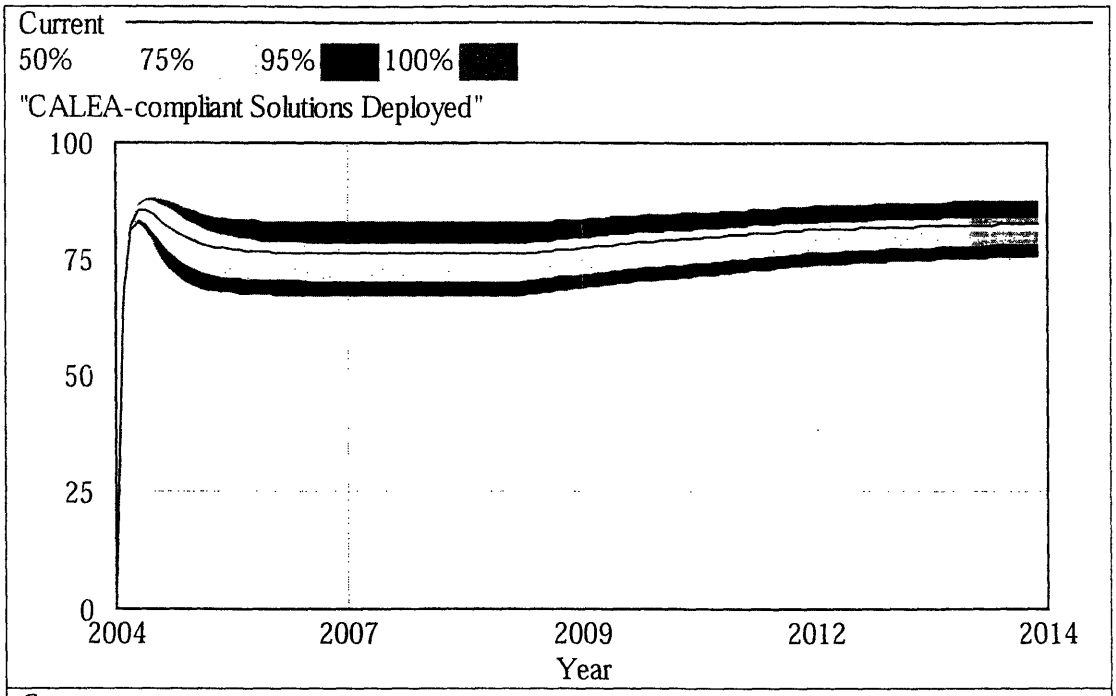
As the carriers deploy CALEA compliant technologies, various factors will lead to the use of non-compliant technologies. First, CALEA compliance may lag the technological progress in security and privacy technologies. Second, increase in concern for privacy may lead to proprietary privacy solutions. Finally, hackers and Internet-criminals may try to outsmart CALEA-compliant technologies. This arms race can raise the cost of CALEA compliance.

---

[50]FCC's CALEA NPRM. ET Docket No. 04-295, [s]ervice providers provide "subscribers the ability to originate, terminate or direct communications" in a manner "that allows the customer to obtain access to a publicly switched network." *See House Report*, 1994 U.S.C.C.A.N at 3504 (Section-by-Section Analysis).

Figure 39 shows the sensitivity of CALEA compliance to the varying development and deployment rate of non-CALEA solutions. Here, the variables "Normal Rate of Development for non-CALEA Solutions" and "Time to Adopt non-CALEA Solutions" is varied between half and two times their normal value. Normal Rate of Development for non-CALEA Solutions is varied from 3 to 12 solutions/month. Time to Adopt non-CALEA Solutions is varied from 3 to 12 months/solution.

Figure 39 shows that variance in development and deployment of non-CALEA solutions impacts the cost of CALEA compliance. The cost of compliance can rise as high as 4.5 times the normal cost.



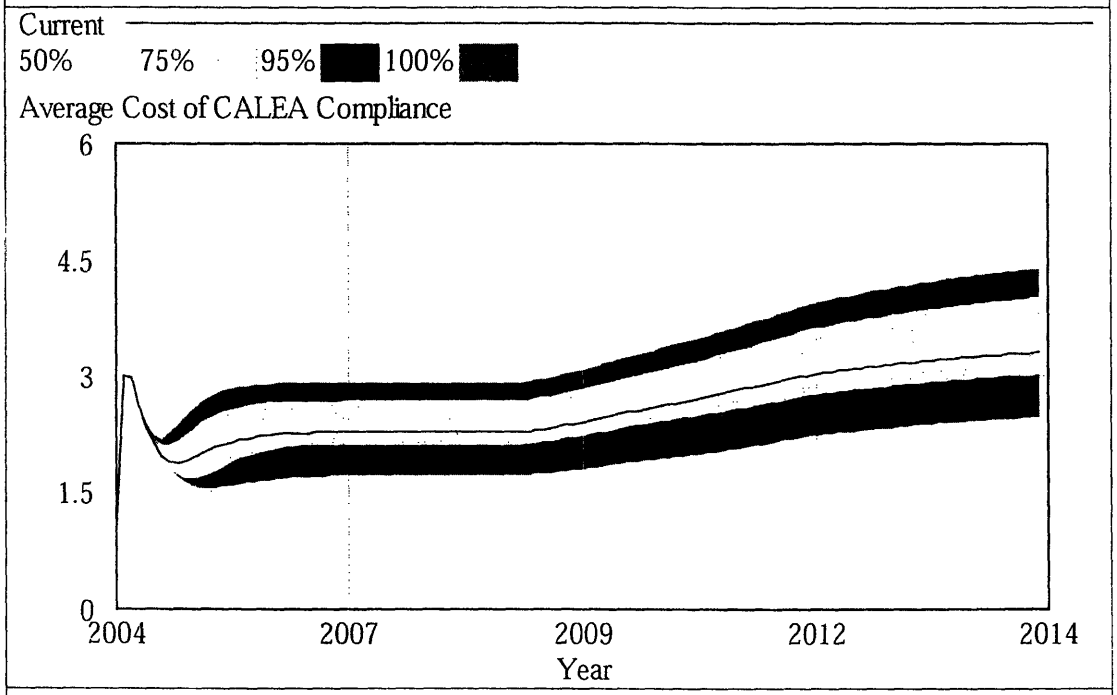


Figure 39 Sensitivity Analysis: Sensitivity of CALEA Deployment and Compliance Cost to varying Development and Deployment Rate of Non-CALEA Solutions

Policy Lesson 4: Prohibiting use of certain encryption techniques may help the LEA to keep their ability to wiretap intact, but it also deprives customers of the privacy the prohibited schemes would have offered, and thereby helps the Internet-crime.

If the use of new encryption scheme causes the CALEA compliance to lag behind, the tendency may be to prohibit the use of new encryption scheme until technology to wiretap it is developed. Use of stronger encryption schemes without the government approval has a history of inviting political wrath. Banning the use of an encryption scheme, if only for a short time, may not be the best option. Internet-criminals could be interested in two aspects of wiretapping: they may want to avoid being wiretapped by the LEA; they may want to wiretap conversations to commit crime similar to the ones that currently happen through tapping phone conversations. Banning the use of an encryption scheme helps the LEA by giving them the grace period to develop a mechanism to wiretap, but in the meanwhile it deprives customers of the privacy the use of the banned scheme would have offered, and helps criminal by leaving customers vulnerable to being wiretapped as a result of old encryption schemes.

REFERENCES

1. Maresca, M., Z. Nicola, and P. Baglietoo, *Internet Protocol Support for Telephony.* Proceedings of IEEE, 2004. **92**(9): p. 1463:1477.
2. (ITU-T), I.T.S.S., *Packet-based multimedia communications systems version 5.* 2003, International Telecommunication Union: Geneva, Switzerland.
3. Thom, G.A., *H.323: The Multimedia Communications Standard for Local Area Networks.* Ieee Communications Magazine, 1996. **34**(12): p. 52-56.
4. Greene, N., M. Ramalho, and B. Rosen, *RFC 2805: Media Gateway Control Protocol Architecture and Requirements.* 2000, IETF.
5. Rosenberg, J., et al., *RFC 3261: SIP: Session Initiation Protocol.* 2002, IETF.
6. Blatherwick, P., R. Bell, and P. Holland, *RFC 3054: Megaco IP Phone Media Gateway Application Profile.* 2001, IETF.
7. Nocentini, S. and M. Siviero, *Innovative class 5: A challenge for incumbent network operators.* Journal of the Communications Network, 2002. **1**: p. 52-55.
8. Lovell, D., *Cisco IP Telephony.* 2001, Indianapolis, IN: Cisco Press.
9. Markopoulou, A.P., F.A. Tobagi, and M.J. Karam, *Assessing the quality of voice communications over Internet backbones.* Ieee-Acm Transactions on Networking, 2003. **11**(5): p. 747-760.
10. (ITU-T), I.T.U., *ITU-T Recommendation H.323: Packet-based multimedia communications systems*, in *International Telecommunication Union.* 1997, ITU-T: Geneva, Switzerland.
11. Handley, M. and V. Jacobson, *RFC 2327: SDP: Session Description Protocol.* 1998, IETF.
12. Arango, M. and C. Huitema, *Simple gateway control protocol (SGCP) Version 1.0.* 1998.
13. Cuervo, F., et al., *RFC 3015: Megaco Protocol Version 1.0.* 2000, IETF.
14. (CableLabs), C.T.L., *PacketCable Network-Based Call Signaling Protocol Specification.* 1999.
15. Schulzrinne, H. and J. Rosenberg, *Internet telephony: architecture and protocols - an IETF perspective.* Computer Networks-the International Journal of Computer and Telecommunications Networking, 1999. **31**(3): p. 237-255.
16. (ITU-T), I.T.U., *ITU-T Recommendation G.114: One-way transmission time*, in *International Telecommunication Union.* 1996, ITU-T: Geneva, Switzerland.
17. (CCITT), C.C.I.T.T., *CCITT Recommendation G.131: Stability and Echo*, in *Comite Consultatif International Telephonique Telegraphique.* 1988, CCITT: Geneva, Switzerland.
18. Braden, R., D. Clark, and S. Shenker, *RFC 1633: Integrated Services in the Internet Architecture: An overview.* 1994, IETF.
19. Braden, R., et al., *RFC 2205: Resource Reservation Protocol (RSVP) version 1 functional specification.* 1997, IETF.
20. Goode, B., *Voice over Internet protocol (VoIP).* Proceedings of the Ieee, 2002. **90**(9): p. 1495-1517.
21. (NAS), N.A.o.S., *Realizing the Information Future: The Internet and Beyond.* 1994, CSTB Publications. p. 340.

22. Saltzer, J., D. Reed, and D. Clark, *End-to-end arguments in system design.* ACM Transactions of Computer Systems. **2**(4): p. 277-288.
23. Sterman, J., *Business dynamics: systems thinking and modeling for a complex world.* c2000, Boston: Irwin/McGraw-Hill.
24. (FCC), F.C.C., *Local Telephone Competition: Status as of December 31, 2004.* 2004.
25. (FCC), F.C.C., *High Speed Services for Internet Access: Status as of December 31, 2004.* 2004.
26. (IDC), I.D.C., *Challenges with 911 to slow VoIP Adoption,* in *Customer Relationship Management.* 2005. p. 14.
27. (Yankee), Y.G., *Discovering VoIP Profitability,* in *America's Network.* 2005. p. 22.

Appendix A: Abbreviations

ACD	Automatic call distributor.
ALG	Application level gateway.
ATM	Asynchronous transfer mode, a cell- switched communications technology.
BGP-4	Border gateway protocol 4, an interdomain routing protocol.
BRI	Basic rate interface (ATM interface, usually 144 kb/s).
Codec	Coder/decoder.
CR-LDP	Constrained route label distribution protocol.
DiffServ	Differentiated services.
DHCP	Dynamic host configuration protocol.
DNS	Domain Name System
DSL	Digital subscriber line.
DTMF	Dual tone multiple frequency.
E.164	An ITU-T standard for telephone numbering plan
ENIM	IETF standard for mapping telephone numbering on DNS
EF	Expedited forwarding.
FTP	File transfer protocol.
FXO	Foreign Exchange Office.
H.323	An ITU-T standard protocol suite for real-time communications over a packet network.
H.225	An ITU-T call signaling protocol (part of the H.323 suite).
H.235	An ITU-T security protocol (part of the H.323 suite).
H.245	An ITU-T capability exchange protocol (part of the H.323 suite).
HTTP	Hypertext transfer protocol.
IANA	Internet assigned numbers authority.
IETF	Internet engineering task force.
IntServ	Integrated services Internet.
ITAD	Internet telephony administrative domain.
ITSP	Internet telephony service provider.
ITU	International Telecommunications Union.
IP	Internet protocol.
IS-IS	Intermediate system-to-intermediate system, an interior routing protocol.
LAN	Local area network.
LDP	Label distribution protocol.
LS	Location server.

LSP	Label switched path.
LSR	Label switching router.
Megaco/H.248	An advanced media gateway control protocol standardized jointly by the IETF and the ITU-T.
MG	Media gateway.
MGCP	Media gateway control protocol.
MOS	Mean opinion score.
MPLS	Multiprotocol label switching.
MPLS-TE	MPLS with traffic engineering.
NAT	Network address translation.
OSPF	Open shortest path first, an interior routing protocol.
PBX	Private branch exchange, usually used on business premises to switch telephone calls.
PHB	Per hop behavior.
PRI	Primary rate interface (ATM interface, usually 1.544 kb/s or 2.048 Mb/s).
PSTN	Public switched telephone network.
RAS	Registration, admission and status. RAS channels are used in H.323 gatekeeper communications.
RFC	Request for comment, an approved IETF document.
RSVP	ReSerVation setup protocol.
RSVP-TE	RSVP with traffic engineering extensions.
RTP	Real-time transport protocol.
RTCP	Real-time control protocol.
RTSP	Real-time streaming protocol.
QoS	Quality of service.
SDP	Session description protocol.
SG	Signaling gateway.
SIP	Session initiation protocol.
SS7	Signaling system 7.
SCTP	Stream control transmission protocol.
SOHO	Small office/ home office.
TCP	Transmission control protocol.
TLS	Transport layer security.
TDM	Time-division multiplexing.
TRIP	Telephony routing over IP.
URI	Uniform resource identifier.
URL	Uniform resource locator.
UDP	User datagram protocol.

VAD	Voice activity detection.
VoIP	Voice over Internet protocol.

Appendix B: VoIP Timeline

Date	Description	Comments
03/05/95	VocalTec's announces VocalChat for free PC_to-PC long-distance	VocalChat from VocalTec (201-768-9400) lets you use a local area network of connected computers as an intercom system by allowing you to send your voice over the network."Internet Phone," a software program, makes it possible to send your "real time" voice over the Internet. And since unlimited Internet service is about $ 20 a month that's unlimited voice telephone calls to anywhere for about $ 20 a month (on regular internet provider service from AOL, ATT etc.). Internet Phone requires Windows 3.1 or higher, at least a 486/33 Mhz system and a Winsock 1.1 compatible SLIP or PPP 14.4K modem or better Internet connection.
11/13/95	Free World Dialup made the first successful internet phonecall from Tokyo to Jakarta on 10/17/95	Vowing to make voice and video communication over the Internet as easy to use and accessible as the telephone, Lucent Technologies Inc. introduced a business venture yesterday and several products intended to bring Internet communication into the mainstream.
11/13/95	10,000 VocalTec downloads in the first week (March)	First version was simplex
01/16/96	About a dozen new phone products for PCs have appeared on the Internet over the past 12 months, such as Internet Phone, Digiphone, Internet Global Phone, CU-SeeMe, and for Macs, Maven, Internet Phone, e-Phone (formerly NetPhone), PGPfone and CU-SeeMe.	About a dozen new phone products for PCs have appeared on the Internet over the past 12 months.
03/01/96	Internet Telephony anxiety increases	attraction is cheap long distance. Prof Joseph Farrell, chief economist at the Federal Communications Commission (FCC), the body which regulates US telecoms and broadcasting, told a London conference that there should be no restrictions on Net telephony. It would help to drive down the charges long-distance operators pay to connect into local networks, and so reduce the cost of long-distance calls.
03/17/96	IP Voice Forum taps G.723.1 audio codec	
07/19/96	Major backing for H.323	
09/11/96	Internet Telephony vendors request interoperability standard	
09/18/96	Lucent plans to make internet phones	
02/03/97	IP Telephony Gateway (although not termed so) introduced by Delta Three in Israel. No PC required for Internet Telephony.	
02/03/97	Long distance companies announce IP in backbone	MCI will use Vault Architecture with IP telephony gateways
04/07/97	Early IP Telephony Gateways	Lucent announces IP Telephony Gateway for cable and internet

05/12/97	Early IP-to-POTS standardization efforts	The European Telecommunications Standards Institute (ETSI) is creating a special project to set standards for allowing Internet-protocol-based voice services to work with analog and digital fixed telephones and with digital-cellular mobile phones. Project Tiphon (Telecommunications and Internet Protocol Harmonization over Networks) is being established on the recommendation of ETSI members Alcatel, Belgacom, Ericsson, Koninklije PTT Nederland (KPN), Lucent Technologies, Nokia, Siemens and Telia. KPN and Telia are the leading phone-service providers in the Netherlands and Sweden, respectively; Belgacom is the nationally owned Belgian service provider.
05/19/97	Intel and Mircosoft announce H.323 tool kit	will help voice and video development
07/07/97	Early bans on Internet Service	Czech Republic, Hungary, Iceland and Portugal have banned Internet Telephony
07/14/97	Internet Fax, an important precursor to Internet Telephony?	UUNet introduced the most extensive internet faxing infrastructure. Forrester believes this is important.
07/28/97	Internet Telephony finds a niche in international market	
08/04/97	Studies predict strong internet telephony growth	
08/18/97	Early efforts to standardize phone number to IP translation	VoIP forum is working on it
09/03/97	VoIP past hobbyist phase	
10/27/97	Cisco Routers get VoIP	Cisco Systems last week introduced a voice-over-Internet protocol module for the 3600 line of routers.
11/13/97	600,000 VocalTec downloads by October 1995	Mostly euphoria by techno-geeks
12/08/97	Early IP Interoperability efforts	
06/01/98	Age of Aliances - AT&T and TCI, MCI-IBM-Cisco	
07/20/98	*Gateway-Gatekeeper Age begins*	Ericsson announces a gatekeeper
10/01/98	IP Telephony hype continues	
11/16/98	IP phones design issues begin to surface	
11/23/98	Cable telephony returns to industry shows	
11/23/98	IPS7 standards proposed	
04/26/99	First VoIP over Cable appears	IXC Communications on Cisco Gateways and Phones
07/26/99	Softswitch gains steam	
08/16/99	VoIP vendors announce Open Source Linux based products	Motorola and Lineo
11/22/99	Comcast claims successful VoIP over cable	
12/13/99	ISP's enter IP telephony	iBasis
01/24/00	Early QoS concerns	
04/03/00	SIP gains fans	
07/20/00	Early VoIP over wireless collaboration	AT&T and Nokia
10/16/00	Interoperabilty considered key	
12/11/00	VoIP over Cable faces QoS issues	

05/07/01	early "echo" conserns	
11/26/01	VoIP making a comeback in Cable industry	
04/01/02	Ban on VoIP operators in some countries -- hurried move to protect revenues from International Calls	
04/01/02	Network Management Product focus for VoIP	
04/09/02	AT&T Links Global VoIP Services	
04/09/02	AT&T Links Global VoIP Services, Expanding On-Net Connectivity and Hop-Off Capability	inter-networking between IP, frame relay and ATM, VoIP at speeds upto T-3
05/01/02	2002 was the year for packet based cable infrastructure. Lab and field triels.	VoIP for Cable always made sense, regardless of the regulations. It was a revenue that did not exist. Every MSO has VoIP plans.
05/01/02	Scalability and QoS concerns	Canadian Cable Industry complained about scalability and latency (QoS) issues with VoIP. Called for Industry wide approach.
06/01/02	Security and QoS concerns	A number of problems must be solved first involving firewalls, NAT (network address translation) devices, GAG (call admission control), SDRs (session detail records) and QoS.
06/01/02	ROI concerns	Economic downturn pushed cost reduction to the top of the agenda
06/20/02	6% of voice traffic in Europe is end-to-end VoIP	Margaret Hopkins, Analysys Research
09/19/02	Cost of IP Phone concerns	Cost of IP Phone is much higher than regular phones
09/23/02	Security concerns at forefront of design	Three Reasons: 1) Unlike ordinary phones, VoIP phones do not reqire wire tap to breach security, 2) IP phone has an IP address and an internet aware processor, 3) VoIP has the same security vulnerability as any data network
10/03/02	VoIP training certificates rolled out	Nortel, Avaya roll out VoIP training certificates
10/08/02	NAT and Firewall Issues	NAT and Firewalls introduce delay
10/08/02	In 2001 Latin America used 1 Billion minutes of use (MOU) of VoIP	Deregulation is helping VoIP in Latin America
11/01/02	Firewall issues Continue	RTP uses any port, hance needing a IPSec tunnel. A working group within the IETF is developing a protocol known as the Middlebox Communication Architecture and Framework (MIDCOM for short) to enable devices to pre-process multimedia traffic before firewall encounters it to better integrate with traditional firewalls.
11/25/02	Numbering Conflicts	Two Interest Groups: 1) VoIP is impacting the current numbering scheme, 2) Current numbering plan is impacting VoIP. The body managing this is North American Numbering Council (NANC)
01/01/03	Voce over WiFi	Voice over 802.11e will resulat in additional cost savings
01/14/03	Japanese VoIP leads the world?	According to Yutaka Asai, President of IP Solutions Company at Oki Electric, "The Japanese VoIP market currently leads the world, with the IP telephony subscribers numbering over three million. In November 2002, the government launched phone-number allocation for IP telephony, a world first. As a leader in the Japanese VoIP market, we offer potential business partners our wealth of cumulative experience and know-how."
02/10/03	VoIP hidden costs concerns	IP PBX replacing Circuit-Switched PBX have several hidden costs: 1) they optional pricing for standard PBX features such as E911, with site license charges, 2) Backbone needs to be 100Mbps or Gigabit Ethernet, 3) Routers supporting QoS, 4) QoS net management tools, 5) Additional servers for redundancy, failover, availability, 6) Training

02/18/03	Today,85% of router based systems are not ready for VoIP deployment	Said Gartner. No QoS support.
02/24/03	VoIP for Cable looks viable	Cable companies must target broadband users first. They must bundle voice, video and data, and price it lower than phone line and the internet charges.
03/18/03	International VoIP Council launched	Worldwide "voice" for VoIP within the business, consumer and technology communities, and be the international organization representing all elements of IP telecommunications. Founded by CommuniTech President and CEO, Neal Shact. Members include: bConvergent, Deltathree, DiamondWare, Dialpad, Gordon & Glickson, Hitnet, Interactive Intelligence, Kancharla, Net6, PBX.net, Pingtel, Swissvoice, Sylantro and members of the International Softswitch Consortium.
03/31/03	AT&T Advances Voice Over Internet Services With Cisco Systems' IP PBX Solution	
04/01/03	Security continues to be a concern	Firewalls not build to handle VoIP traffic. Security continues to be a deal breaker.
05/01/03	Scalability concerns continue	Scalability concerns continue for cable operators
05/26/03	VoIP-based services were $13 billion in 2002	Insight Research.
09/01/03	VoIP picking up	Beginning of the 2nd wave?
09/01/03	10% of global calls are VoIP	Michael Haney, a senior analyst in the Securities and Investment Practice at Celent Communications,
09/01/03	VoIP service revenue $1 billion in 2003	Michael Haney, a senior analyst in the Securities and Investment Practice at Celent Communications,
09/24/03	20 Million Broadband Connections in the US	
12/02/03	FCC Invites the VoIP Forum	
12/09/03	Voice Packets hit the chip level	AudioCodes Ltd. has developed a four-channel voice-compression processor set for handling Voice Over Internet Protocol (VOIP).
06/30/04	Rumblings of ISP eying Internet Telephony	

Appendix C: List of all CALEA Variables

CALEA Variables
Number of Pen-Register Trace Required
Number of lawful-intercepts Required
Number of wire-tap decryption success
Number of wire-tap decryption failure
Number of wire-tap decrypted by service providers
Number of wiretaps decrypted by LEA
Number of encryption algorithms available
Number of decryption algorithms available
Effectiveness of decryption
Number of VoIP providers with Pen-Register Trace capability
Number of VoIP providers with lawful intercept capability
% of Voice Communications that can be wire-tapped
% of voice traffic that is VoIP
% of voice traffic with Scenario A providers
% of voice traffic with Scenario B1 providers
% of voice traffic with Scenario B2 providers
% of voice traffic with Scenario C providers
% of voice traffic with Scenario D providers
% Homes with Broadband
% of businesses with Broadband
ARPU of Residential User
ARPU of Business User
Cost of CALEA Compliance
Scenario A Cost of CALEA Compliance
Scenario B1 Cost of CALEA Compliance
Scenario B2 Cost of CALEA Compliance
Scenario C Cost of CALEA Compliance
Scenario D Cost of CALEA Compliance
% of Voice Communication subjected to CALEA
Number of Scenario A subscribers
Number of Scenario B1 subscribers
Number of Scenario B2 subscribers
Number of Scenario C subscribers
Number of Scenario D subscribers
Number of Scenario A service providers
Number of Scenario B1 service providers
Number of Scenario B2 service providers
Number of Scenario C applicaiton providers
Number of Scenario D service providers

Number of VoIP Equipment Vendors
Number of VoIP Feature (Application) Vendors
Number of VoIP CPE Vendors
Number of VoIP Service Providers
Number of free VoIP application providers
VoIP Quality of Service
Cost of providing service in Scenario A
Cost of providing service in Scenario B1
Cost of providing service in Scenario B2
Cost of providing service in Scenario C
Cost of providing service in Scenario D
Willingness to make VoIP wiretap-able
Actual Wiretap-ability
Percieved Wiretap-ability
Actual Difficulty of Wiretapping
Percieved Difficulty of Wiretapping
Cost of technologies for wiretapping
Availability of technologies for wiretapping
Customers using encryption
Service Providers using encryption
Need for security
Need for privacy
Cost of maintaining privacy
Scenario A - Cost of maintaining privacy
Scenario B1 - Cost of maintaining privacy
Scenario B2 - Cost of maintaining privacy
Scenario C - Cost of maintaining privacy
Scenario D - Cost of maintaining privacy
Number of US based service providers
Number of non-US service providers

Appendix D: CALEA Model Equations

(01) "2004 Managed VoIP Users"=
1e+006
Units: subscriber [0,6e+006]

Used by:(38)Managed VoIP Users -

(02) "2004 P2P Users"=
1e+006
Units: subscriber [0,4e+007]

Used by:(57)P2P Users -

(03) Acceptable Deployment Gap=
10
Units: solutions [0,100]

Used by:(26)Effect of Deployment Gap -

(04) Adj due to Managed Marketshare=
Managed Marketshare f (Effect of Managed VoIP Marketshare)
Units: dmnl

(27)Effect of Managed VoIP Marketshare -
(34)Managed Marketshare f -
Used by:(71)Regulatory Pressure -

(05) Adj from Deployment Gap=
Deployment Gap Pressure f (Effect of Deployment Gap)
Units: dmnl

(26)Effect of Deployment Gap -
(22)Deployment Gap Pressure f -
Used by:(16)Avg Cost of New Solutions -
(24)Dev Time for New Solutions -

(06) "Adj from Pressure to Develop New non-CALEA Solutions"=
"Pressure to Develop non-CALEA Solutions f" ("Pressure to Develope New non-CALEA Solutions"
)
Units: dmnl

(67)Pressure to Develope New non-CALEA Solutions -
(66)Pressure to Develop non-CALEA Solutions f -
Used by:(39)New non-CALEA Solutions -

(07) Adj from Regulatory Pressure=
Regulatory Pressure on Dev f (Effect of Regulatory Pressure)
Units: dmnl

(29)Effect of Regulatory Pressure -
(72)Regulatory Pressure on Dev f -
Used by:(16)Avg Cost of New Solutions -
(24)Dev Time for New Solutions -

(08) Adjustment due to Attractiveness=
Attractiveness f (Effect of P2P Attractiveness)
Units: dmnl

(28)Effect of P2P Attractiveness -
(12)Attractiveness f -
Used by:(54)P2P Fruitfulness -

(09) Adjustment due to Cost=
P2P Attractiveness from Cost of Compliance f (Effect of Cost of CALEA Compliance
)
Units: dmnl

(25)Effect of Cost of CALEA Compliance -
(50)P2P Attractiveness from Cost of Compliance f -
Used by:(49)P2P Attractiveness -

(10) Adjustment due to Reg=
P2P Attractiveness from Reg Pressure f (Effect of Regulatory Pressure)
Units: dmnl

(29)Effect of Regulatory Pressure -
(51)P2P Attractiveness from Reg Pressure f -
Used by:(49)P2P Attractiveness -

(11) "Adoption of non-CALEA Solutions"=
"non-CALEA Solutions"/"Time to Adopt non-CALEA Solutions"
Units: solutions/Month

(41)non-CALEA Solutions -
(78)Time to Adopt non-CALEA Solutions -
Used by:(41)non-CALEA Solutions -
(48)Obsolete Solutions -

(12) Attractiveness f(
[(0,0)-(10,10)],(0,1),(1,1),(2,2),(4,4),(10,10))
Units: dmnl

Used by:(08)Adjustment due to Attractiveness -

(13) Average Cost of CALEA Compliance= INTEG (
Change in Average Cost,
Normal Average Cost)
Units: Dollar/solution

(18)Change in Average Cost -
(42)Normal Average Cost -
Used by:(18)Change in Average Cost -
(25)Effect of Cost of CALEA Compliance -

(14) Average MOU=
100
Units: MOU/subscriber/Month [0,200]

Used by:(37)Managed VoIP MOU -

(69)PSTN MOU -

(15) Average P2P MOU=
100
Units: MOU/(subscriber*Month) [0,200]

Used by:(59)P2P VoIP MOU -

(16) Avg Cost of New Solutions=
Normal Average Cost * Adj from Deployment Gap * Adj from Regulatory Pressure
Units: Dollar/solution

(05)Adj from Deployment Gap -
(07)Adj from Regulatory Pressure -
(42)Normal Average Cost -
Used by:(18)Change in Average Cost -

(17) "CALEA-compliant Solutions Deployed"= INTEG (
New Solutions-Obsolete Solutions,
0)
Units: solutions

(40)New Solutions -
(48)Obsolete Solutions -
Used by:(32)Gap -
(67)Pressure to Develope New non-CALEA Solutions -

(18) Change in Average Cost=
(Avg Cost of New Solutions - Average Cost of CALEA Compliance)/Dev Time for New Solutions
Units: Dollar/solution/Month

(13)Average Cost of CALEA Compliance -
(16)Avg Cost of New Solutions -
(24)Dev Time for New Solutions -
Used by:(13)Average Cost of CALEA Compliance -

(19) Contacts of Noncust with Cust=
Contacts with Customers * Potential Cust Concentration
Units: contact/Month

(20)Contacts with Customers -
(64)Potential Cust Concentration -
Used by:(81)WOM Conversions -

(20) Contacts with Customers=
Managed VoIP Users * Sociability
Units: contact/Month

(38)Managed VoIP Users -
(74)Sociability -
Used by:(19)Contacts of Noncust with Cust -

(21) Conversion=
WOM Conversions
Units: subscriber/Month

(81)WOM Conversions -
Used by:(38)Managed VoIP Users -
(70)PSTN Users -

(22) Deployment Gap Pressure f(
[(0,0)-(20,10)],(0,1),(0.5,1),(0.917431,1.05263),(1.5,1.5),(2,2),(3.79205
,3.24561),(6,4),(8,4),(10,4))
Units: dmnl

Used by:(05)Adj from Deployment Gap -

(23) "Desired CALEA-compliant Solutions Deployment"=
100
Units: solutions [0,100]

Used by:(32)Gap -

(24) Dev Time for New Solutions=
Normal Time to Develope New Solutions * (1/Adj from Deployment Gap)* (1/
Adj from Regulatory Pressure)
Units: Month

(05)Adj from Deployment Gap -
(07)Adj from Regulatory Pressure -
(47)Normal Time to Develope New Solutions -
Used by:(18)Change in Average Cost -
(40)New Solutions -

(25) Effect of Cost of CALEA Compliance=
Average Cost of CALEA Compliance/Normal Average Cost
Units: dmnl

(13)Average Cost of CALEA Compliance -
(42)Normal Average Cost -
Used by:(09)Adjustment due to Cost -

(26) Effect of Deployment Gap=
Gap/Acceptable Deployment Gap
Units: dmnl

(03)Acceptable Deployment Gap -
(32)Gap -
Used by:(05)Adj from Deployment Gap -

(27) Effect of Managed VoIP Marketshare=
Managed VoIP Marketshare/Managed Marketshare Threshold
Units: dmnl

(35)Managed Marketshare Threshold -
(36)Managed VoIP Marketshare -
Used by:(04)Adj due to Managed Marketshare -

(28) Effect of P2P Attractiveness=
P2P Attractiveness / Normal P2P Attractiveness
Units: dmnl

(44)Normal P2P Attractiveness -
(49)P2P Attractiveness -
Used by:(08)Adjustment due to Attractiveness -

(29) Effect of Regulatory Pressure=
Regulatory Pressure/Normal RegulatoryPressure
Units: dmnl

(46)Normal RegulatoryPressure -
(71)Regulatory Pressure -
Used by:(07)Adj from Regulatory Pressure -
(10)Adjustment due to Reg -

(30) FINAL TIME = 1200
Units: Month

(31) Fruitfulness=
0.01
Units: subscriber/contact [0,1]

Used by:(81)WOM Conversions -

(32) Gap=
"Desired CALEA-compliant Solutions Deployment" - "CALEA-compliant Solutions Deployed"
Units: solutions

(17)CALEA-compliant Solutions Deployed -
(23)Desired CALEA-compliant Solutions Deployment -
Used by:(26)Effect of Deployment Gap -
(40)New Solutions -

(33) INITIAL TIME = 0
Units: Month

Used by:(00)Time - Internally defined simulation time.

(34) Managed Marketshare f(
[(0,0)-(20,20)],(0,1),(1,1),(2,1.2),(5,1.6),(10,2),(20,2))
Units: dmnl

Used by:(04)Adj due to Managed Marketshare -

(35) Managed Marketshare Threshold=
0.1
Units: fraction [0,1]

Used by:(27)Effect of Managed VoIP Marketshare -

(36) Managed VoIP Marketshare=
Managed VoIP MOU/(Managed VoIP MOU + PSTN MOU)
Units: fraction

(37)Managed VoIP MOU -

(69)PSTN MOU -
Used by:(27)Effect of Managed VoIP Marketshare -

(37) Managed VoIP MOU=
Managed VoIP Users * Average MOU
Units: MOU/Month

(38)Managed VoIP Users -
(14)Average MOU -
Used by:(36)Managed VoIP Marketshare -
(61)Percent Voice Under CALEA Jurisdiction -
(62)Percent VoIP Not Under CALEA Jurisdiction -
(63)Percent VoIP Under CALEA Jurisdiction -

(38) Managed VoIP Users= INTEG (
Conversion,
"2004 Managed VoIP Users")
Units: subscriber

(01)2004 Managed VoIP Users -
(21)Conversion -
Used by:(20)Contacts with Customers -
(37)Managed VoIP MOU -
(80)Total Telephony Market -

(39) "New non-CALEA Solutions"=
"Normal Rate of Development for non-CALEA Solutions" * "Adj from Pressure to Develop New non-CALEA Solutions"
Units: solutions/Month

(06)Adj from Pressure to Develop New non-CALEA Solutions -
(45)Normal Rate of Development for non-CALEA Solutions -
Used by:(41)non-CALEA Solutions -

(40) New Solutions=
Gap / Dev Time for New Solutions
Units: solutions/Month

(24)Dev Time for New Solutions -
(32)Gap -
Used by:(17)CALEA-compliant Solutions Deployed -

(41) "non-CALEA Solutions"= INTEG (
+"New non-CALEA Solutions"-"Adoption of non-CALEA Solutions",
0)
Units: solutions

(11)Adoption of non-CALEA Solutions -
(39)New non-CALEA Solutions -
Used by:(11)Adoption of non-CALEA Solutions -

(42) Normal Average Cost=
1
Units: Dollar/solution [0,5]

Used by:(13)Average Cost of CALEA Compliance -

(16)Avg Cost of New Solutions -
(25)Effect of Cost of CALEA Compliance -

(43) Normal Fruitfulness=
0.01
Units: subscriber/contact [0,1]

Used by:(54)P2P Fruitfulness -

(44) Normal P2P Attractiveness=
1
Units: unitAttractiveness [0,3]

Used by:(28)Effect of P2P Attractiveness -
(49)P2P Attractiveness -

(45) "Normal Rate of Development for non-CALEA Solutions"=
6
Units: solutions/Month [1,30]

Used by:(39)New non-CALEA Solutions -

(46) Normal RegulatoryPressure=
1
Units: unitRegPressure [0,3]

Used by:(29)Effect of Regulatory Pressure -
(71)Regulatory Pressure -

(47) Normal Time to Develope New Solutions=
6
Units: Month [0,30]

Used by:(24)Dev Time for New Solutions -

(48) Obsolete Solutions=
"Adoption of non-CALEA Solutions"
Units: solutions/Month

(11)Adoption of non-CALEA Solutions -
Used by:(17)CALEA-compliant Solutions Deployed -

(49) P2P Attractiveness=
Normal P2P Attractiveness * Adjustment due to Reg * Adjustment due to Cost
Units: unitAttractiveness

(09)Adjustment due to Cost -
(10)Adjustment due to Reg -
(44)Normal P2P Attractiveness -
Used by:(28)Effect of P2P Attractiveness -

(50) P2P Attractiveness from Cost of Compliance f(
[(0,0)-(10,10)],(0,1),(1,1),(2,2),(4,4),(10,10))
Units: dmnl

Used by:(09)Adjustment due to Cost -

(51) P2P Attractiveness from Reg Pressure f(
[(0,0)-(10,10)],(0,1),(0.458716,0.964912),(1.00917,1.09649),(1.5,1.5),(2,2),(4,4),(10,10))
Units: dmnl

Used by:(10)Adjustment due to Reg -

(52) P2P Contacts of Noncust with Cust=
P2P Contacts with Customers * P2P Potential Cust Concentration
Units: contact/Month

(53)P2P Contacts with Customers -
(55)P2P Potential Cust Concentration -
Used by:(60)P2P WOM Conversions -

(53) P2P Contacts with Customers=
P2P Users * P2P Sociability
Units: contact/Month

(57)P2P Users -
(56)P2P Sociability -
Used by:(52)P2P Contacts of Noncust with Cust -

(54) P2P Fruitfulness=
Normal Fruitfulness * Adjustment due to Attractiveness
Units: subscriber/contact

(08)Adjustment due to Attractiveness -
(43)Normal Fruitfulness -
Used by:(60)P2P WOM Conversions -

(55) P2P Potential Cust Concentration=
Potential P2P Users/Total P2P Users
Units: dmnl

(65)Potential P2P Users -
(79)Total P2P Users -
Used by:(52)P2P Contacts of Noncust with Cust -

(56) P2P Sociability=
6
Units: contact/subscriber/Month [0,50]

Used by:(53)P2P Contacts with Customers -

(57) P2P Users= INTEG (
Subscribers Joining-Subscribers Leaving,
"2004 P2P Users")
Units: subscriber

(02)2004 P2P Users -
(75)Subscribers Joining -
(76)Subscribers Leaving -
Used by:(53)P2P Contacts with Customers -
(59)P2P VoIP MOU -

(79)Total P2P Users -

(58) P2P Voice Fraction=
0.1
Units: fraction [0,1]

Used by:(59)P2P VoIP MOU -

(59) P2P VoIP MOU=
P2P Users * Average P2P MOU * P2P Voice Fraction
Units: MOU/Month

(57)P2P Users -
(15)Average P2P MOU -
(58)P2P Voice Fraction -
Used by:(61)Percent Voice Under CALEA Jurisdiction -
(62)Percent VoIP Not Under CALEA Jurisdiction -
(63)Percent VoIP Under CALEA Jurisdiction -

(60) P2P WOM Conversions=
P2P Contacts of Noncust with Cust * P2P Fruitfulness
Units: subscriber/Month

(52)P2P Contacts of Noncust with Cust -
(54)P2P Fruitfulness -
Used by:(75)Subscribers Joining -

(61) Percent Voice Under CALEA Jurisdiction=
(Managed VoIP MOU + PSTN MOU) / (Managed VoIP MOU + P2P VoIP MOU + PSTN MOU)
Units: fraction

(37)Managed VoIP MOU -
(59)P2P VoIP MOU -
(69)PSTN MOU -

(62) Percent VoIP Not Under CALEA Jurisdiction=
P2P VoIP MOU / (P2P VoIP MOU + Managed VoIP MOU)
Units: fraction

(37)Managed VoIP MOU -
(59)P2P VoIP MOU -

(63) Percent VoIP Under CALEA Jurisdiction=
Managed VoIP MOU / (P2P VoIP MOU + Managed VoIP MOU)
Units: fraction

(37)Managed VoIP MOU -
(59)P2P VoIP MOU -

(64) Potential Cust Concentration=
PSTN Users/Total Telephony Market
Units: dmnl

(70)PSTN Users -
(80)Total Telephony Market -

Used by:(19)Contacts of Noncust with Cust -

(65) Potential P2P Users= INTEG (
-Subscribers Joining,
2e+008)
Units: subscriber

(75)Subscribers Joining -
Used by:(55)P2P Potential Cust Concentration -
(79)Total P2P Users -

(66) "Pressure to Develop non-CALEA Solutions f"(
[(0,0)-(10,10)],(0,1),(0.5,1),(1,1),(1.5,1.5),(1.95719,1.84211),(2.5,2),(
3,2),(4,2))
Units: dmnl

Used by:(06)Adj from Pressure to Develop New non-CALEA Solutions -

(67) "Pressure to Develope New non-CALEA Solutions"=
"CALEA-compliant Solutions Deployed"/Privacy Panic Threshold
Units: dmnl

(17)CALEA-compliant Solutions Deployed -
(68)Privacy Panic Threshold -
Used by:(06)Adj from Pressure to Develop New non-CALEA Solutions -

(68) Privacy Panic Threshold=
50
Units: solutions [0,100]

Used by:(67)Pressure to Develope New non-CALEA Solutions -

(69) PSTN MOU=
PSTN Users * Average MOU
Units: MOU/Month

(70)PSTN Users -
(14)Average MOU -
Used by:(36)Managed VoIP Marketshare -
(61)Percent Voice Under CALEA Jurisdiction -

(70) PSTN Users= INTEG (
-Conversion,
1.77e+008)
Units: subscriber

(21)Conversion -
Used by:(64)Potential Cust Concentration -
(69)PSTN MOU -
(80)Total Telephony Market -

(71) Regulatory Pressure=
Normal RegulatoryPressure * Adj due to Managed Marketshare
Units: unitRegPressure

(04)Adj due to Managed Marketshare -

(46)Normal RegulatoryPressure -
Used by:(29)Effect of Regulatory Pressure -

(72) Regulatory Pressure on Dev f(
[(0,0)-(10,10)],(0,1),(1,1),(1.5,1.5),(2,2),(3,2.2),(4,2.2))
Units: dmnl

Used by:(07)Adj from Regulatory Pressure -

(73) SAVEPER =
TIME STEP
Units: Month [0,?]

(77)TIME STEP - The time step for the simulation.

(74) Sociability=
6
Units: contact/subscriber/Month [0,50]

Used by:(20)Contacts with Customers -

(75) Subscribers Joining=
P2P WOM Conversions
Units: subscriber/Month

(60)P2P WOM Conversions -
Used by:(57)P2P Users -
(65)Potential P2P Users -

(76) Subscribers Leaving=
0
Units: subscriber/Month

Used by:(57)P2P Users -

(77) TIME STEP = 1
Units: Month [0,?]

Used by:(73)SAVEPER - The frequency with which output is stored.

(78) "Time to Adopt non-CALEA Solutions"=
6
Units: Month [1,30]

Used by:(11)Adoption of non-CALEA Solutions -

(79) Total P2P Users=
Potential P2P Users + P2P Users
Units: subscriber

(57)P2P Users -
(65)Potential P2P Users -
Used by:(55)P2P Potential Cust Concentration -

(80) Total Tele Managed VoIP Users + PSTN Users
Units: subscriber

(38)Managed VoIP Users -
(70)PSTN Users -
Used by:(64)Potential Cust Concentration -

(81) WOM Conversions=
Contacts of Noncust with Cust * Fruitfulness
Units: subscriber/Month

(19)Contacts of Noncust with Cust -
(31)Fruitfulness -
Used by:(21)Conversion -