UNITED STATES PATENT AND TRADEMARK OFFICE
_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD
_____

AT&T Services, Inc.
Petitioner
v.

Digifonica (International) Limited
Patent Owner

Patent No. 8,542,815

_____

Inter Partes Review No. (To Be Assigned)

_____

DECLARATION OF JAMES BRESS IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW

UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.100 *et seq.*

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

1

Declaration of James Bress in Support of Petition for *Inter Partes* Review
of U.S. Patent No. 8,542,815

Table of Contents

2

Declaration of James Bress in Support of Petition for *Inter Partes* Review
of U.S. Patent No. 8,542,815

5

Declaration of James Bress in Support of Petition for *Inter Partes* Review
of U.S. Patent No. 8,542,815

I, James Bress, declares as follows:

I. INTRODUCTION

1.   I have been retained as a technical expert on behalf of petitioner
AT&T Services, Inc. in connection with the above-captioned inter partes review
("IPR") of U.S. Patent No. 8,542,815 ("the '815 Patent"). I understand that the
'815 Patent is currently assigned to Digifonica (International) Limited.

2.   I am familiar with the technology at issue in the period prior to
November 2, 2006, which is the filing date of the provisional application to which
the '815 Patent claims priority. I have not performed an analysis to determine
whether any of the claims of the '815 Patent should be entitled to this earlier
priority date. However, none of the opinions stated herein would change if any
claim were entitled to this earlier priority date.

3.   I have been asked to provide my technical opinion on concepts
discussed in the '815 Patent and the reference documents, as well as my technical
opinion on how these concepts relate to several '815 Patent claim limitations in the
context of the specification.

4.   I have been asked to consider how a person of ordinary skill in the art
would understand the claims of the '815 Patent and the applied reference

combinations. In reaching the opinions stated herein, I have considered the '815 Patent and the references discussed herein in the context of my own education, training, research, knowledge, and personal and professional experience.

5.   I am being compensated at my standard hourly rate of $350.00 per hour. My compensation is not dependent on the outcome of this IPR and in no way affects the substance of my statements in this declaration.

6.   I make this declaration based upon my own personal knowledge and, if called upon to testify, would testify competently to the matters contained herein. I may rely on handbooks, textbooks, technical literature, my own personal experience in the field, and other relevant materials and/or information to demonstrate the state of the art in the relevant period and the evolution of relevant technologies.

II.   SUMMARY OF OPINIONS

7.   After studying the '815 Patent, its file history, and the prior art, and considering the subject matter of the claims of the '815 Patent in light of the state of technical advancement in the area of IP telephony networks and telecommunications networks prior to the filing of the '815 Patent, I reached the conclusions discussed herein.

8.   In light of these general conclusions, and as explained in more detail throughout this Declaration, it is therefore my opinion that Claims 1, 7, 27–28, 34, 54, 72–74, 92–93, and 111 (the "Challenged Claims") of the '815 Patent are invalid as being obvious in the relevant time frame (prior to November 2006) in light of the knowledge of a person of ordinary skill in the art at that time and the teachings, suggestions, and motivations present in the prior art.

III.   BACKGROUND AND QUALIFICATIONS

9.   My qualifications are stated more fully in my curriculum vitae. (*See* EX1004.) As reflected in my curriculum vitae, and as explained in more detail below, I have experience with the technology described in the '815 Patent, including telecommunications network architectures, protocols, addressing, standards, Public Switched Telephone Networks (PSTN), Voice-over-IP (VoIP) telephony and networks, mobile networks, interworking between PSTN, VoIP, and mobile networks, the Session Initiation Protocol (SIP), the H.323 Protocol, the Transmission Control Protocol (TCP), the Internet Protocol (IP), call processing for both PSTN, VoIP, and mobile networks, network interfacing, network interconnection, gateways, call controllers, soft switches, etc. Here I provide a brief summary of my qualifications.

10.   I received a Bachelor of Science degree in electrical engineering from the University of North Carolina at Charlotte in 1985, and a Master of Science degree in electrical engineering from the California Institute of Technology in 1987. From 1982 to 1984, while still attending the University of North Carolina, I was an engineering technician at Process Systems, Inc., located in Charlotte, NC. My duties there included technical writing for field-located energy management equipment which was remotely accessible via modems and telephone lines, host system software and user manuals, as well as developing test equipment for the field-located equipment and host systems.

11.   In addition to my educational background, I have over 30 years of experience in the telecommunications industry. In 1985, after graduating from the University of North Carolina, I was employed by Bell Communications Research, Inc. (also known as Bellcore), located in Piscataway, NJ. I was an engineer and Member of the Technical Staff (MTS) at Bellcore with responsibility for numerous telecommunications systems operations and development projects. For these systems-related projects, I was responsible for development, integration, and testing including computers, network hardware, network interconnections, network signaling, network protocols, network equipment provisioning and configurations, database technologies, applications and software development, user interfaces,

10

client-server operations, test systems development, and telephony features development and prototyping.

12.   In 1995, I founded AST Technology Labs, Inc., located in Melbourne, Florida, where I am the President and Chief Technical Officer. AST's business is focused on telecommunications equipment and networks. My responsibilities at AST include the development of detailed system specifications, architectures, hardware, and software for custom telecommunications and telephony test systems including analog, digital, VoIP, and wireless. My responsibilities also include researching and analyzing the products that are tested at AST to enable system configurations, preparation for testing, troubleshooting hardware and software, and providing consulting to AST's customers.

13.   I have served on numerous standards setting committees of the Telecommunications Industry Association ("TIA") and have been a prime contributor, editor, and working group chairman for the development of many published ANSI (American National Standards Institute) / TIA telecommunications standards. I served continuously from 2000 to 2015 as chairman or vice chairman of the TIA TR41.3 engineering subcommittee for Performance and Accessibility for Communications Products. Starting in 2015 and to the present, I am the chairman of the parent engineering committee, TR41. I

also authored numerous system requirement publications and recommendations for Bellcore. Additionally, I am a named inventor on four issued US patents.

14.   My first assignment during my employment at Bellcore was in the software operations area. This area was focused on operations system software including PREMIS (PREMise Information System), SOAC (Service Order Analysis & Control), and LFACS (Loop Facility Assignment and Control System). These software systems integrated hardware (network access and switching equipment and computers) and software (database, reporting, network control, monitoring, management, and user interface) used for the operations systems used by Bellcore's owners (the Regional Bell Operating Companies (RBOCs) or "Baby Bells") in support of the Public Switched Telephone Network (PSTN). My experiences during this assignment included software installation and testing, network management, network equipment provisioning, database configuration and schema development, network connectivity troubleshooting, and software documentation.

15.   My next assignment at Bellcore was on a development team for the "Information Gateway" project. My responsibilities included data network design, network connectivity implementation, network equipment configurations and provisioning, and troubleshooting for the networked connectivity of computer

systems located in multiple states across the USA. Networking for this project

included PSTN and data network facilities and services and interworking between

the PSTN and data networks. The computer systems provided access to servers,

databases and terminal interface software from distributed network connected

workstations.   In addition to networking, I was also responsible for database

system design and distributed network access to compressed image files located on

a network connected server.   One of my many projects included analysis,

configurations, and troubleshooting of X.25 data network termination circuits, and

the related termination equipment, to enable numerous system demonstrations that

were set up in multiple locations across the USA.

16.   My work in Bellcore's "New Services Development" area included

designing and prototyping new services that were focused on the use of the

Advanced Intelligent Network (AIN) system features and components.   These

projects required an understanding of telecommunications systems network

architectures, signaling, protocols, standards, and features operations. One of my

projects in this area included interfacing to AIN components including Service

Control Points (SCP) and Signaling Transfer Points (STP) to implement a

telephone network control feature. I am the first named inventor on a patent for

one of the systems developed which was integrated with the AIN (U.S. Patent No.

5,570,420, "Customer premise equipment network integrator").

17.   Another assignment I had at Bellcore involving network signaling and

features was for the development of the Analog Display Services Interface (ADSI)

and the Caller ID on Call Waiting (CIDCW) feature that is now well known to

telephone users. My responsibilities included analyzing PSTN switching systems

architectures and capabilities, and feature related network triggers and service

logic. I was also responsible for developing prototype systems, including hardware

and software, for network signaling and features evaluation. Additionally, I was

responsible for developing Bellcore's Customer Premises Equipment (CPE) test

lab (including hardware, software, lab operations, and reporting) to support the

development of new telephony devices used with the ADSI and CIDCW features.

18.   I started designing network signal detection systems as a

troubleshooting assignment for the Bell Companies. At this time in the late 1980s,

most prison systems used primarily coin telephones, which were owned and

operated by the Bell Companies, to provide telephony services to inmates. Inmates

had discovered that they could defraud the telephone system by playing certain

music into the telephone transmitter (microphone), which would cause the Bell

Company Central Office (CO) accounting and billing systems to errantly record

14

sometimes hundreds of dollars of credit due to falsely detecting coin-drop-confirmation tones. After this problem was solved, the knowledge I gained was used to develop Bellcore's prototype CPE Alerting Signal (CAS) detector that was a key component of what became the widely popular Caller ID on Call Waiting (CIDCW) telephony feature. This work led to the issuing of U.S. Patent No. 5,519,774 "Method and system for detecting at a selected station an alerting signal in the presence of speech" for which I am a named inventor.

19. I am the first named inventor on U.S. Patent No. 7,076,031 "System and Method for Telephone Signal Collection and Analysis." The impetus for this patent was the development of the TSA-6000® telephone signal recording and analysis system. This project culminated into the manufacture and sale of TSA-6000® systems starting in 2002. I was the chief architect for the design of this system and I continue to serve as the technical lead for this project and product. The TSA-6000® system was designed using the concept of functional units that can be combined in any physical implementation including the functions of 1) signal data capture and recording; 2) analysis of the captured signaling data to identify pre-defined telephone signals and events occurring in the recorded signals, as well as identifying the states, or modes of the telephone line; and 3) a user-friendly graphical interface for viewing signals and analysis data, and also for

system configurations such as changing the parameters used during the analysis operations. The software of the TSA-6000® was developed using C language and runs on a Windows®-based computer. The software has been revised over the years for multiple reasons including to add new pre-defined signal types or classifications, and to modify and enhance the signal analysis algorithms.

20. While employed at AST Technology Labs (AST), I have been responsible for the development of a "Call Generator" system for Telcordia Systems (formerly Bellcore). The Call Generator system included PSTN and data network interfaces integrated with a network based controller system. My development responsibilities for the controller system included hardware integration, software development including network control, remote configuration, database, and user interfaces. The system was designed to demonstrate Telcordia's larger system goal of handling "one million calls per minute" for emergency management. The system was installed at Telcordia and used for demonstrations by Telcordia management and sales teams.

21. In my position as chairman of the TIA-TR41.3 subcommittee and TIA-TR41 committee for the performance of communications products, I have been responsible for contributions to, and the development and publication of, several PSTN and VoIP related performance standards for telephony and gateway

equipment including the ANSI/TIA-470 series, ANSI/TIA-4953, the ANSI/TIA-920 series, ANSI/TIA-1083, and ANSI/TIA-1063. In addition to my leadership role for standards development at TIA, I include as part of my responsibilities to be informed, and to maintain a level of expertise, regarding other standard's bodies' analog, VoIP, and mobile related standards including those published by the IEEE (Institute of Electrical and Electronics Engineers), the ETSI (European Telecommunications Standards Institute), the ITU (International Telecommunication Union), 3GPP (Third Generation Partnership Project), and others.

22.   In 2007, I started a project at AST for Microsoft for the development of detailed performance and testing specifications, and the development of custom testing capabilities, for Microsoft's "Response Point" VoIP-PBX system. The detailed specifications covered each of the Response Point VoIP-PBX system components including telephony devices (handset, headset, and speakerphone), voice gateways (FXO/PSTN to VoIP and FXS/ATA-Analog to VoIP), and the system base controller (including SIP proxy and registrar servers, and voicemail server).   In addition to developing the detailed performance and testing requirements, developing custom test capabilities, and performing testing on the

Response Point systems, I also provided troubleshooting for and consulting to Microsoft's customer's.

23. Regarding the testing of IP and mobile related devices and equipment, my responsibilities at AST include the development of IP-based test systems for evaluating the performance of VoIP equipment, including telephones (Ethernet and USB connected), computer connected devices (USB to computer's Ethernet LAN), Ethernet connected voice gateways, and wireless (cellular) handsets. I am responsible for the set-up, configuration and operation of mobile and VoIP related test systems used to evaluate the audio and acoustic, network interface, and feature implementation performance of mobile handsets and VoIP endpoints and gateways. Included with the test systems developed and used is the integration of network-based servers including SIP proxies and registrars.

24. I am the chief architect and design engineer for the development of one of AST's in-house test systems used for evaluating the performance of VoIP endpoints and gateway products. These endpoint products, and the test systems developed, employ the SIP (Session Initiation Protocol) and the SDP (Session Description Protocol) for establishing call connections, and the RTP (Real Time Protocol) for the transmission of media (e.g., packets of digitized voice) after session establishment. During the on-going development of these systems, I have

gained experience in the operation and implementation of the stack of protocols which are used to implement VoIP features and services. This includes developing software enabled features for controlling and manipulating SIP signaling parameters, SDP session and device related parameters, and RTP parameters. In addition to controlling the content of the messages used by these protocols, the test systems I have developed control the timing of offer / answer negotiations which is the primary method used to establish sessions between endpoints (e.g., two VoIP telephones), or between endpoints and servers (e.g., a voicemail server) and gateways using SIP, SDP, and RTP protocols. I was responsible for implementing these systems which required the development of user interfaces, configuration / provisioning features, custom IP protocol level control software, and the integration of network-based servers including SIP proxies and registrars.

25.   I am a named inventor on US Patent No. 9,020,621 "Network Based Media Enhancement Function Based on an Identifier" which was based on the systems and concepts developed for a start-up company for whom I was a consultant. My responsibilities included research and development of system designs and architectures for PSTN and IP-based IMS (Internet-protocol Multimedia Subsystems) servers and services. The systems developed provided services to users connecting to an IMS network via PSTN or SIP/SDP enabled

devices to access application servers located within an IMS network. The

application servers provided the ability to enhance the audio of a PSTN, VoIP, or

mobile telephone call by being inserted into the media path and modifying the

audio to match a user's needs based on the user's hearing impairment parameters.

As such, the application server performed the role of a media gateway with added

features to provide the audio enhancements.

26. My Curriculum Vitae, included as Exhibit 1004, outlines my duties at

Bellcore, AST, and as a consultant, includes further details about my education and

professional career, and lists my patents and publications. I have extensive

expertise in all of the 32 telecommunications, systems, and computer related areas

listed on page 2 of my Curriculum Vitae. *See* EX1004 at p. 2. My Curriculum

Vitae also lists my prior litigation consulting over the past twelve years. *See id*. at

pp. 13–23.

IV.   MATERIALS CONSIDERED

27. I have considered information from various sources in forming my

opinions attached as Appendices to this Declaration. Besides drawing from over

three decades of research and development work in telecommunications networks,

including IP telephone networks, I also have reviewed the '815 Patent, the

prosecution file history of the '815 Patent, and the other documents and references

as cited herein, including those identified in the following table:

Exhibit No.	Document
1001	U.S. Patent No. 8,542,815
1002	Prosecution File History of the '815 Patent
1005	U.S. Patent No. 6,240,449 ("*Nadeau*")
1006	U.S. Patent No. 6,594,254 ("*Kelly*")
1007	U.S. Patent No. 7,715,413 ("*Vaziri*")

V. UNDERSTANDING OF THE LAW

28.   I have applied the following legal principles provided to me by

counsel in arriving at the opinions set forth in this report.   My opinions are

informed by my understanding of the relevant law. I understand that a patentability

analysis is conducted on a claim-by-claim basis and that there are several possible

reasons that a patent claim may be found to be unpatentable.

29.   I understand that earlier publications and patents may act to render a

patent claim unpatentable as obvious.

A.   Legal Standard for Prior Art

30.   I understand that a patent or other publication must first qualify as

prior art before it can be used to invalidate a patent claim.

31.   I understand that a U.S. or foreign patent qualifies as prior art to an

asserted patent if the date of issuance of the patent is prior to the invention of the

asserted patent. I further understand that a printed publication, such as a book or an article published in a magazine or trade publication, qualifies as prior art to an asserted patent if the date of publication is prior to the invention of the asserted patent.

32.   I understand that a U.S. or foreign patent qualifies as prior art to an asserted patent if the date of issuance of the patent is more than one year before the filing date of the asserted patent. I further understand that a printed publication, such as a book or an article published in a magazine or trade publication, constitutes prior art to an asserted patent if the publication occurs more than one year before the filing date of the asserted patent.

33.   I understand that a U.S. patent qualifies as prior art to the asserted patent if the application for that patent was filed in the United States before the invention of the asserted patent.

34.   I understand that to qualify as prior art, a reference must contain an enabling disclosure that allows one of ordinary skill to practice the claims without undue experimentation.

35.   I understand that documents and materials that qualify as prior art can be used to render a patent claim unpatentable as anticipated or as obvious.

B.   Legal Standard for Obviousness

36.   I have been instructed by counsel on the law regarding obviousness, and understand that even if a patent is not anticipated, it is still unpatentable if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person of ordinary skill in the pertinent art.

37.   I understand that a person of ordinary skill in the art provides a reference point from which the prior art and claimed invention should be viewed. This reference point prevents a person of ordinary skill from using one's insight or hindsight in deciding whether a claim is obvious.

38.   I also understand that an obviousness determination includes the consideration of various factors such as (1) the scope and content of the prior art, (2) the differences between the prior art and the Asserted Claims, (3) the level of ordinary skill in the pertinent art, and (4) the existence of secondary considerations such as commercial success, long-felt but unresolved needs, failure of others, etc.

39.   I am informed that secondary indicia of non-obviousness may include (1) a long felt but unmet need in the prior art that was satisfied by the invention of the patent; (2) commercial success or lack of commercial success of processes covered by the patent; (3) unexpected results achieved by the invention; (4) praise

of the invention by others skilled in the art; (5) taking of licenses under the patent

by others; and (6) deliberate copying of the invention. I also understand that there

must be a relationship between any such secondary indicia and the invention. I

further understand that contemporaneous and independent invention by others is a

secondary consideration supporting an obviousness determination.

40.   I understand that an obviousness evaluation can be based on a

combination of multiple prior art references. I understand that the prior art

references themselves may provide a suggestion, motivation, or reason to combine,

but other times the nexus linking two or more prior art references is simple

common sense. I further understand that obviousness analysis recognizes that

market demand, rather than scientific literature, often drives innovation, and that a

motivation to combine references may be supplied by the direction of the

marketplace.

41.   I understand that if a technique has been used to improve one device,

and a person of ordinary skill in the art would recognize that it would improve

similar devices in the same way, using the technique is obvious unless its actual

application is beyond his or her skill.

42.   I also understand that practical and common sense considerations

should guide a proper obviousness analysis, because familiar items may have

obvious uses beyond their primary purposes. I further understand that a person of

ordinary skill in the art looking to overcome a problem will often be able to fit the

teachings of multiple publications together like pieces of a puzzle, although the

prior art need not be like two puzzle pieces that must fit perfectly together. I

understand that an obviousness analysis therefore takes into account the inferences

and creative steps that a person of ordinary skill in the art would employ under the

circumstances.

43.   I understand that a particular combination may be proven obvious by

showing that it was obvious to try the combination. For example, when there is a

design need or market pressure to solve a problem and there are a finite number of

identified, predictable solutions, a person of ordinary skill has good reason to

pursue the known options within his or her technical grasp because the result is

likely the product not of innovation but of ordinary skill and common sense.

44.   I understand that the combination of familiar elements according to

known methods may be proven obvious when it does no more than yield

predictable results. When a work is available in one field of endeavor, design

incentives and other market forces can prompt variations of it, either in the same

field or a different one. If a person of ordinary skill can implement a predictable

variation, obviousness likely bars its patentability.

45.   It is further my understanding that a proper obviousness analysis

focuses on what was known or obvious to a person of ordinary skill in the art, not

just the patentee. Accordingly, I understand that any need or problem known in

the field of endeavor at the time of invention and addressed by the patent can

provide a reason for combining the elements in the manner claimed.

46.   I understand that a claim can be obvious in light of a single reference,

without the need to combine references, if the elements of the claim that are not

found explicitly or inherently in the reference can be supplied by the common

sense of one of ordinary skill in the art.

47.   I understand that a person of ordinary skill could have combined two

pieces of prior art or substituted one prior art element for another if the substitution

can be made with predictable results, even if the swapped-in element is different

from the swapped-out element. In other words, the prior art need not be like two

puzzle pieces that must fit together perfectly. The relevant question is whether

prior art techniques are interoperable with respect to one another, such that a

person of ordinary skill would view them as a design choice, or whether a person

of ordinary skill could apply prior art techniques into a new combined system.

48.   In sum, my understanding is that prior art teachings are properly

combined where a person of ordinary skill in the art having the understanding and

knowledge reflected in the prior art and motivated by the general problem facing

the inventor, would have been led to make the combination of elements recited in

the claims. Under this analysis, the prior art references themselves, or any need or

problem known in the field of endeavor at the time of the invention, can provide a

reason for combining the elements of multiple prior art references in the claimed

manner.

49.   I have been informed and understand that the obviousness analysis

requires a comparison of the properly construed claim language to the prior art on

a limitation-by-limitation basis.

50.   I have written this report with the understanding that in an *inter partes*

review obviousness must be shown by a preponderance evidence.

C.   Legal Standard for Claim Construction

51.   I understand that a patentee may express a claim element as a means

for performing a specified function without reciting in the claim the structure for

performing the recited function, and such claims are construed to cover the

corresponding structure described in the specification and equivalents of that

disclosed structure.   Furthermore, I understand that when the specification

discloses structure that includes a general purpose computer, microprocessor, or

logic, the corresponding structure must also include an algorithm for performing the function.

VI. LEVEL OF SKILL OF ONE OF ORDINARY SKILL IN THE ART

52.   I have been informed by counsel that the claims of a patent are judged from the perspective of a hypothetical construct involving "a person of ordinary skill in the art" at the time the claimed invention of the patent was made. The "art" is the field of technology to which the patent is related. I understand that the purpose of using the view point of a person of ordinary skill in the art is for objectivity.

53.   In my opinion, a person of ordinary skill must generally have the capability of understanding the general computer systems and principles that are applicable to the pertinent art. I understand that the factors to be considered in determining the level of ordinary skill in the art to be: (1) the educational level of active workers in the field, including the named inventors of the patent; (2) the type of problems encountered in the art; (3) prior art solutions to those problems; (4) the rapidity with which innovations are made; and (5) the sophistication of the technology in the art.

54. I understand that the application that resulted in the '815 Patent was filed on March 1, 2010. I also understand that the earliest possible priority date that the '815 Patent can claim is November 2, 2006.[1]

55. In my opinion, a person of ordinary skill in the art pertaining to the '815 Patent at the relevant time would have been someone with at least a Bachelor's Degree in electrical engineering, or in a related field, with at least 2–4 years of industry experience in designing or developing packet-based and circuit-switched telecommunication systems. Alternatively, a person of ordinary skill in the relevant timeframe could have been someone lacking formal technical education but having practical experience that would be equivalent to such education. Each of the factors that I outlined above supports this formulation.

56. Based on my education and experience in the field of electrical engineering, telecommunications, and computer science set forth above and in my

---

[1] I am not offering an opinion that the '815 Patent should be entitled to this earlier priority date. As I stated earlier, I have not been asked, and I have not performed an analysis to determine whether any of the claims of the '815 Patent should be entitled to this earlier priority date. My statement simply asserts that, based on the filing information on the face of the patent, the earliest possible priority date that the '815 Patent can claim is November 2, 2006.

curriculum vitae, I believe I am qualified to provide opinions about how one of ordinary skill in the art at the relevant time would have interpreted and understood the '815 Patent and the prior art discussed herein. Although my qualifications and experience exceed those of a person of ordinary skill in the art, both in 2006 and today, I have nevertheless applied the perspective of a person of ordinary skill in the art in rendering my opinions below.

VII.   BRIEF OVERVIEW OF THE '815 PATENT

57.   The '815 Patent has a filing date of March 1, 2010 and claims priority, through a PCT application, to a provisional application filed on November 2, 2006.

A.   Admitted Prior Art in the Background

58.   The '815 Patent relates to routing voice-over-IP ("VoIP") calls, a type of call that was well-known at the time of the '815 Patent. (*See* EX1001 at 1:11–13.) The Background section of the '815 Patent admits that it was well-known at the time of the '815 Patent to use IP telephones to establish VoIP calls over packet switched IP networks like the Internet or private networks of large organizations. (*See id*. at 1:15–21.) These calls could be routed to their destinations over these IP networks using well-known protocols such as the Session Initiation Protocol ("SIP"). (*See id*. at 1:22–23, 1:40–43.)

59. The Background section also admits that it was well-known at the time of the '815 Patent that these calls could be routed to their destinations over switched circuit networks like the public switched telephone network ("PSTN"). (*See id*. at 1:29–39.)

60. The '815 Patent also admits that it was well-known at the time of the '815 Patent that it may be more appropriate to route a call over the PSTN rather than the Internet or private corporate networks depending on various criteria (e.g., reliability, cost, availability, etc.). (*See id*. at 1:29–46.)

B. The Purported Invention of the '815 Patent

61. The purported invention is a call routing controller that selects a routing network for a VoIP call by performing two functions: (1) determining what type of network should be used to route a VoIP call based on a caller profile and (2) producing a routing message to route the call to the determined network.

62. The call routing controller is provided in a system that includes IP telephones, a call controller, and a database. (*See id*. at Figure 1.) In the example of Figure 1, an IP telephone in Vancouver has the IP address 192.168.0.20 and a number 2001 1050 8667 and an IP telephone in Calgary has the number 2001 1050 2222. (*See id*. at Figure 1.)
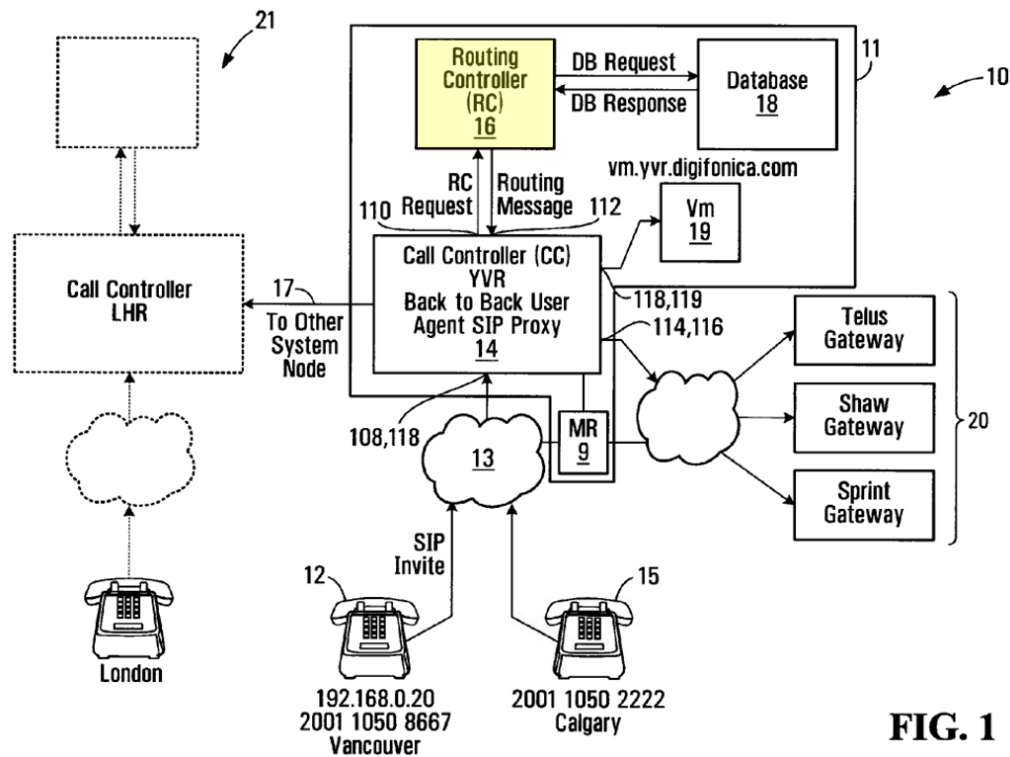
FIG. 1

63.   The call routing controller itself is implemented using well-known computer components such as memories, processors, and I/O ports. (*See id.* at Figure 7.) These components operate in a conventional manner to perform the two functions of the call routing controller.
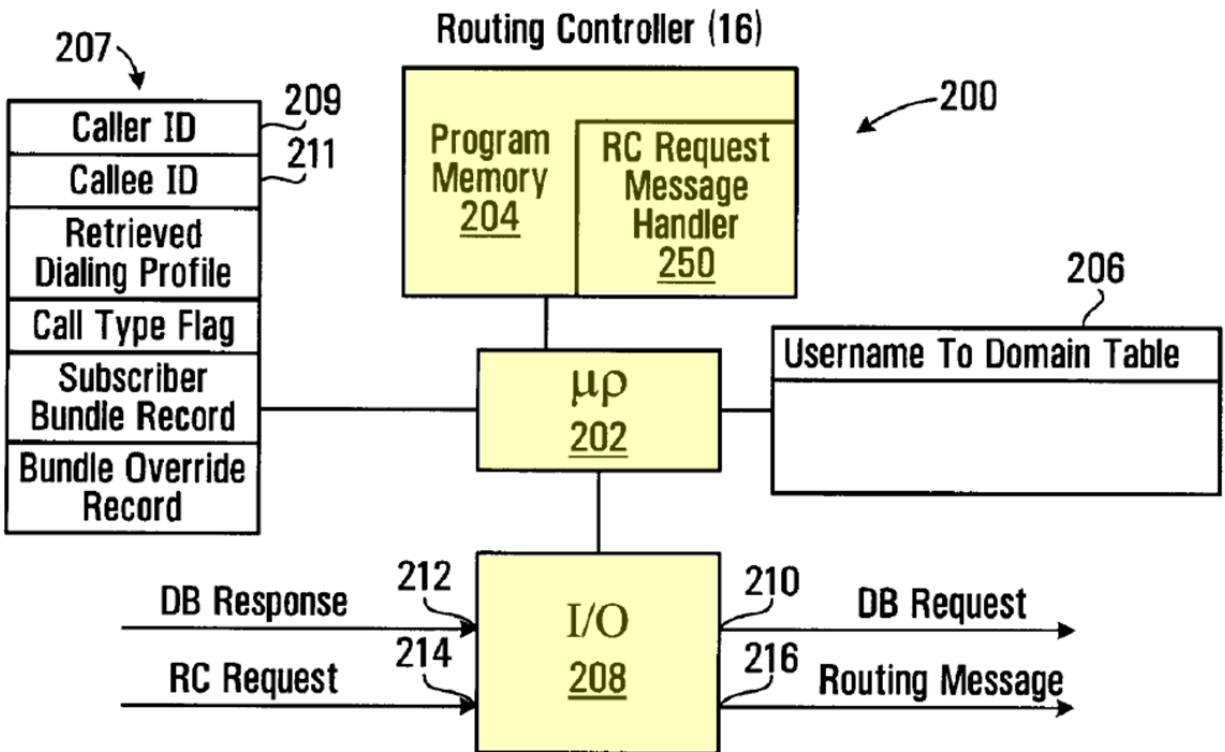
64. First, the call routing controller determines the type of network, such as a public network like the PSTN or a private network like an IP network, that should be used to route a call. The call routing controller receives from a caller a request to establish a call, which includes identifiers of the caller and the callee. (*Id*. at 1:54–56.) For example, the request can be a well-known message like a SIP Invite message that includes the identifiers of the caller and the callee. (*See id*. at Figure 3.) In the example of Figures 1 and 3, if the IP telephone in Vancouver calls the IP telephone in Calgary, the call routing controller receives a SIP Invite message that includes a number for the calling telephone (2001 1050 8667), a

33

number for the callee telephone (2001 1050 2222), and an IP address of the calling

telephone (192.168.0.20). (*See id*. at Figures 1 and 3.)

SIP Invite Message

60 ⁓ Caller   2001 1050 8667
62 ⁓ Callee   2001 1050 2222
64 ⁓ Digest Parameters   XXXXXXX
65 ⁓ Call ID   FF10@ 192.168.0.20
67 ⁓ IP Address   192.168.0.20
69 ⁓ Caller UDP Port   1

FIG. 3

65.   Based on the caller identifier, the routing controller locates a caller

profile that includes caller attributes. (*Id*. at 2:1–7.) An example caller profile for

the example Vancouver caller is shown in Figure 10 below. The profile includes a

username field that shows the number of the caller (2001 1050 8667). (*See id*. at

Figure 10.) The profile also includes calling attributes, such as international

dialing digits and national dialing digits. (*See id*. at Figure 10.)

Dialing Profile for Caller (Vancouver Subscriber)
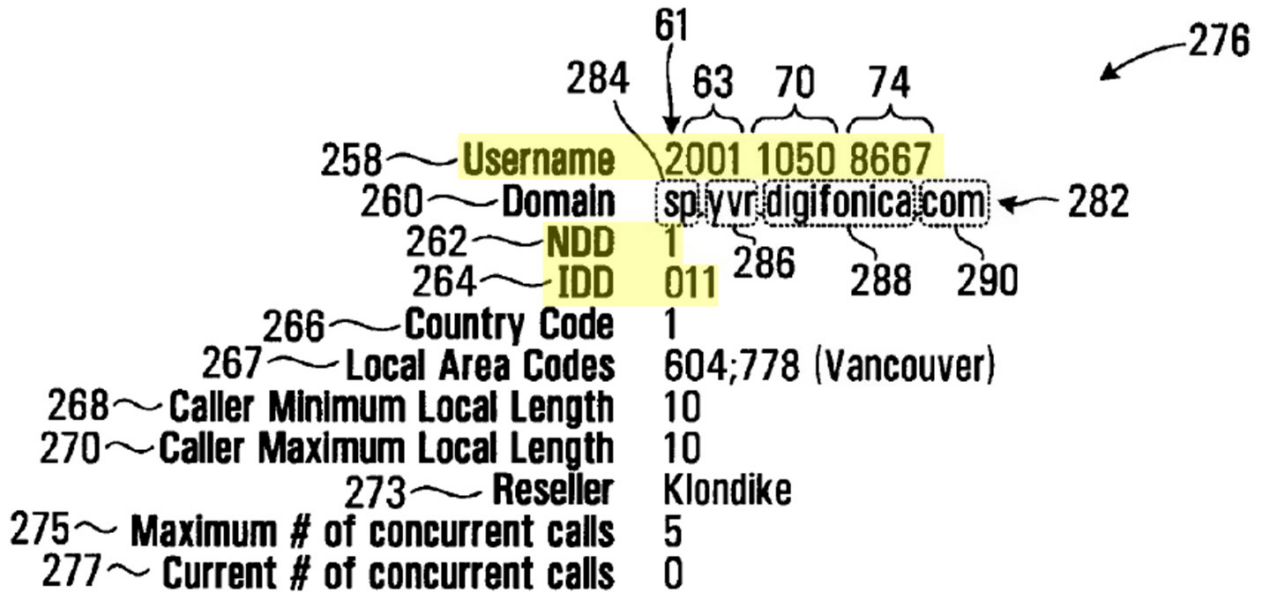
66.   The routing controller then compares the callee identifier with these attributes to determine a match. (*Id.* at 2:8–25.)   For example, the routing controller can match the NDD and IDD in the dialed telephone number with the NDD and IDD in the caller profile. An example flowchart is provided in Figure 8B, shown below, that includes steps that show example matches.
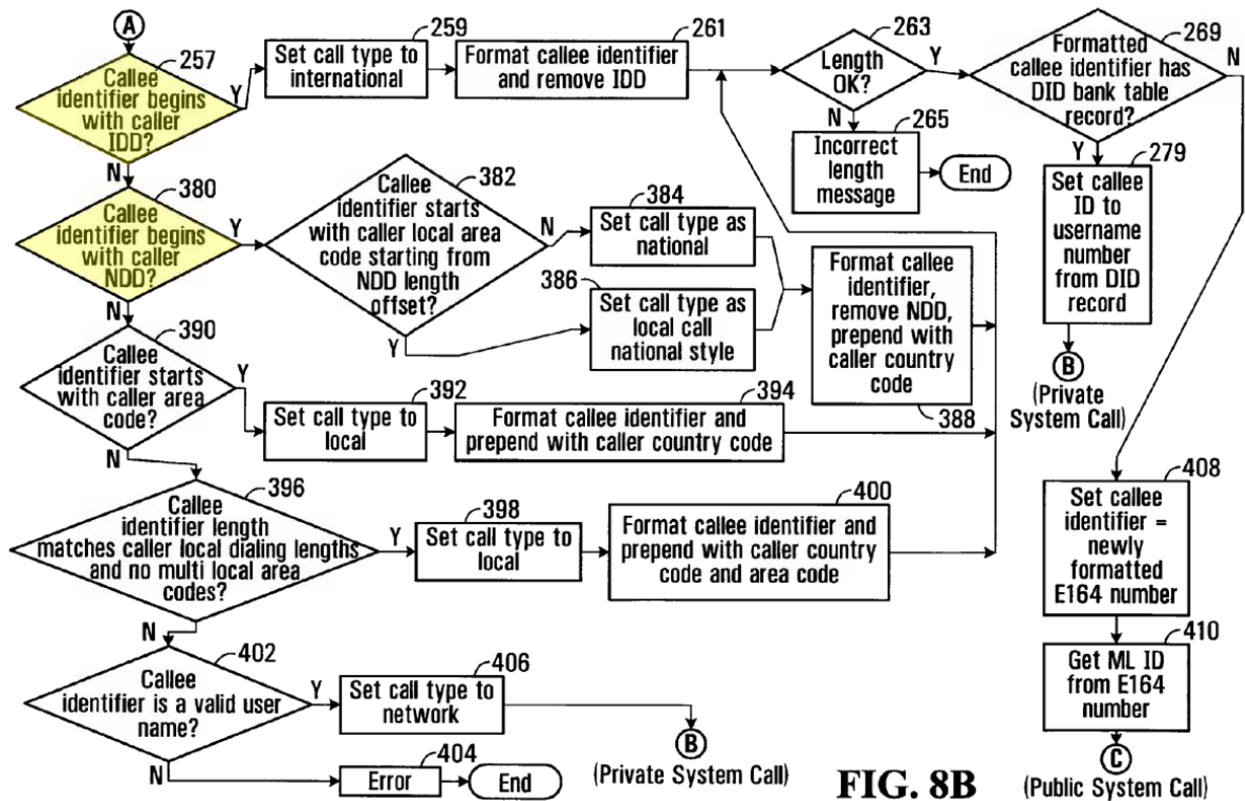
FIG. 8B

67. After a match is determined, the routing controller determines whether

the match meets public network classification criteria or private network

classification criteria. (*Id*. at Abstract.) For example, the routing controller can

first format the dialed telephone number and then determine whether the formatted

telephone number has a direct in dial ("DID") bank table record. (*See id*. at Figure

8B.) An example DID bank table record for the example Calgary callee is shown

below. The record includes two telephone numbers for the callee, a private

telephone number (2001 1050 2222) and a public E.164 telephone number (1 604

867 5309). (*See id*. at Figure 8B.)

36
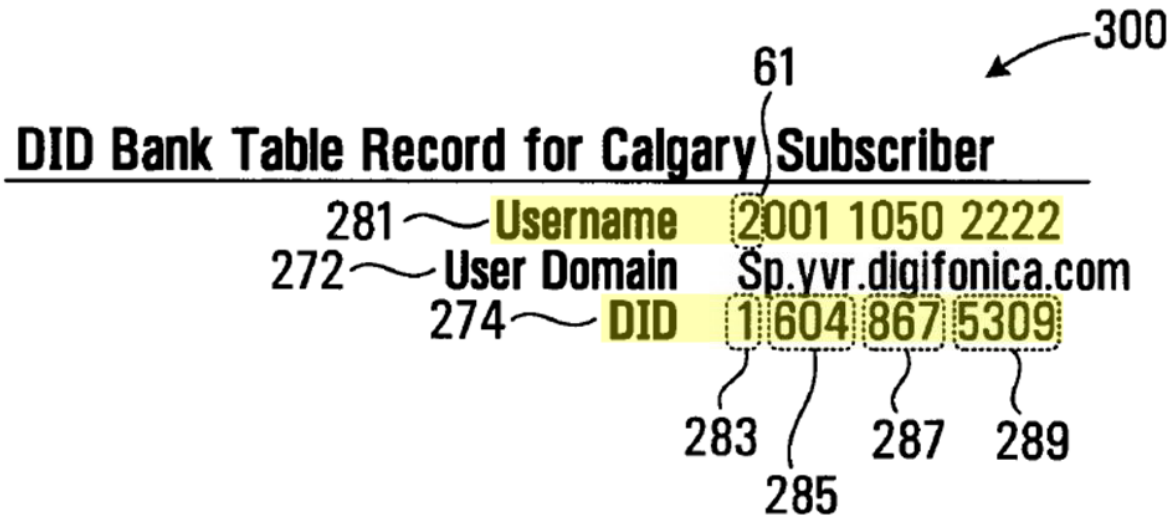
FIG. 14

68.   If the formatted number has a DID bank table record, such as the example with the Calgary callee, then the call can be classified as a private network call and can be routed over a private network, like an IP network. (*See id.* at 1:15–21, 14:24–34.)   The routing controller then determines that the private telephone number of the callee (e.g., 2001 1050 2222) should be used. (*See id.* at Figure 8B.)   Example formatting and classification steps are shown below using the example of Figure 8B.
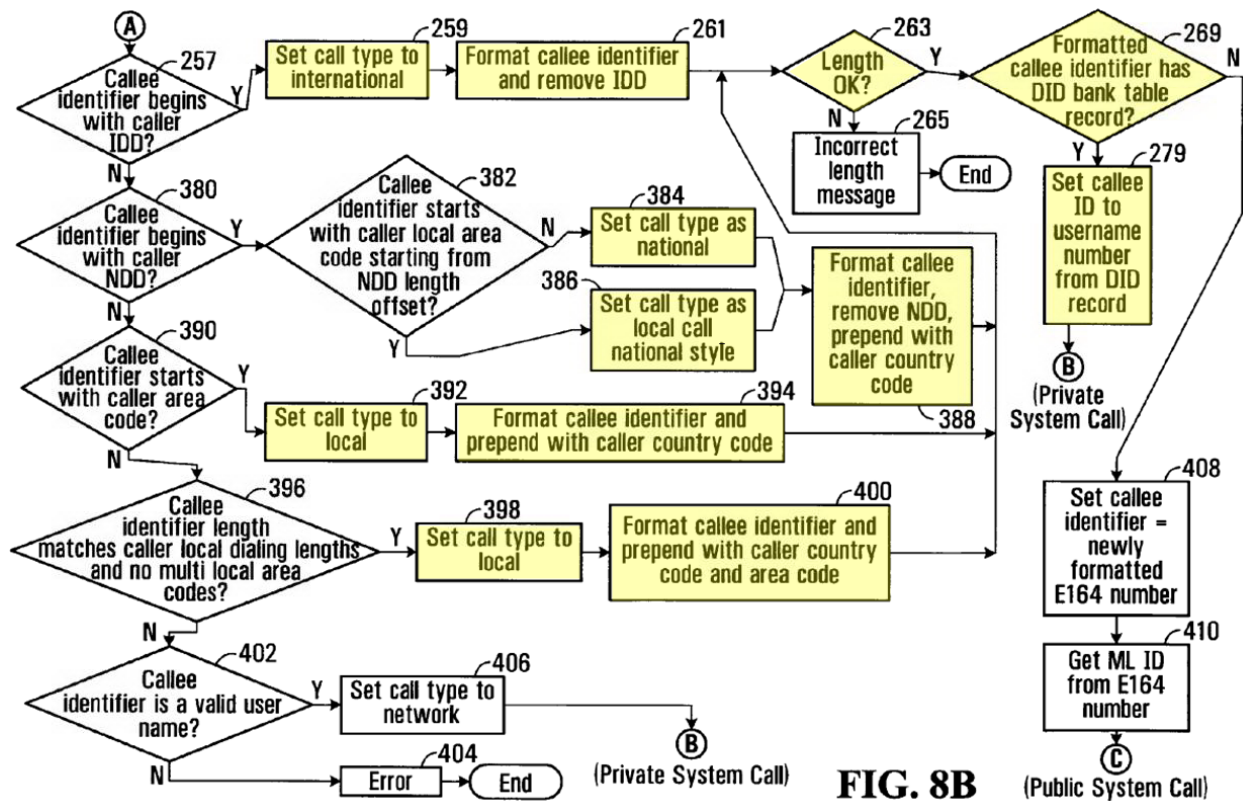
FIG. 8B

69.　　If the formatted telephone number does not have a DID bank table record, then the call can be classified as a public network call and can be routed over a public network like the PSTN. (*See id.* at 1:22–27, 14:24–34.) The routing controller then determines to use the newly formatted E.164 number as the callee identifier and begins determining a supplier to the public telephone network to carry the call. (*See id.* at Figure 8B.) Example formatting and classification steps are shown below using the example of Figure 8B.
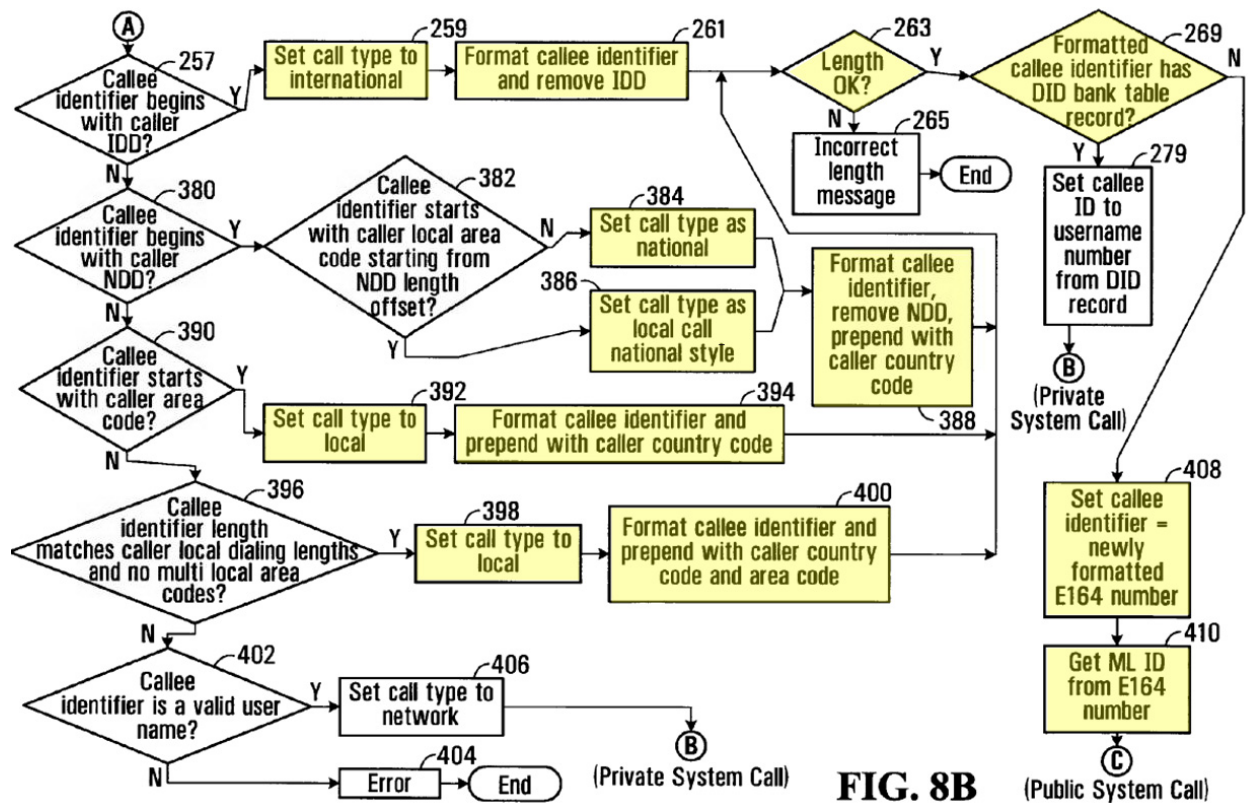
FIG. 8B

70.   Second, after the call has been classified, the call routing controller produces network routing messages to route the call to the appropriate network. An example network routing message format is shown in Figure 15 below. The message includes a telephone number for the callee (public or private depending on the call classification) and a domain name or IP address for routing. (*See id*. at Figure 15.)

─352

Routing Message Format

354	Supplier Prefix (optional)	Code identifying supplier traffic
356	Delimiter (optional)	Symbol separating fields
358	Callee	PSTN compatible number or Digifonica number
360	Route	Domain name or IP address
362	Time to Live(TTL)	In seconds
364	Other	TBD
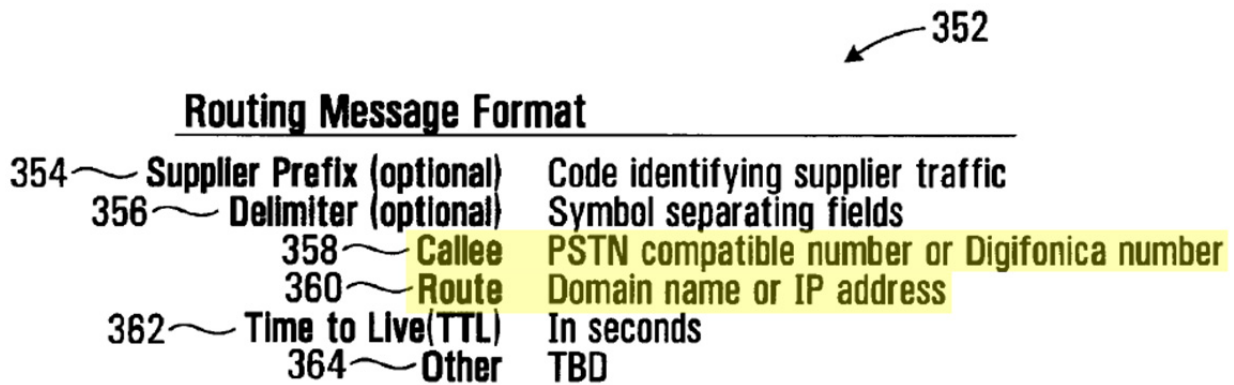
FIG. 15

71.   If the call is classified as a public network call, the routing controller produces a public network routing message that identifies a gateway to the public network. (*Id.*) An example public network routing message is shown in Figure 25 below. The message includes entries for each supplier that can carry the call. Each entry has an identifier for the supplier (e.g., 4973), the callee's E.164 number (e.g., 0116048675309), an IP address for the supplier's gateway (e.g., 72.64.39.58), a time to live (e.g., 3600), and a timeout (e.g., 20). (*Id.* at Figure 25.)

Routing Message Buffer for Gateway Call

```
4973#0116048675309@72.64.39.58;ttl=3600;to=20 ──570
4974#0116048675309@73.65.40.59;ttl=3600;to=30 ──572
4975#0116048675309@74.66.41.60;ttl=3600;to=40 ──574
```

FIG. 25

72.   If the call is classified as a private network call, the routing controller

produces a private network routing message that identifies an address on the

private network. (*Id.*) An example private network routing message is shown in

Figure 16 below. The message includes a telephone number for the callee (e.g.,

440110624444), a domain name (e.g., sp.lhr.digifonica.com), and a time to live

(e.g., 9999). (*See id.* at Figure 16.)

Example of Routing Message – Different Node

440110624444@sp.lhr.digifonica.com;ttl=9999

359   361   363

366
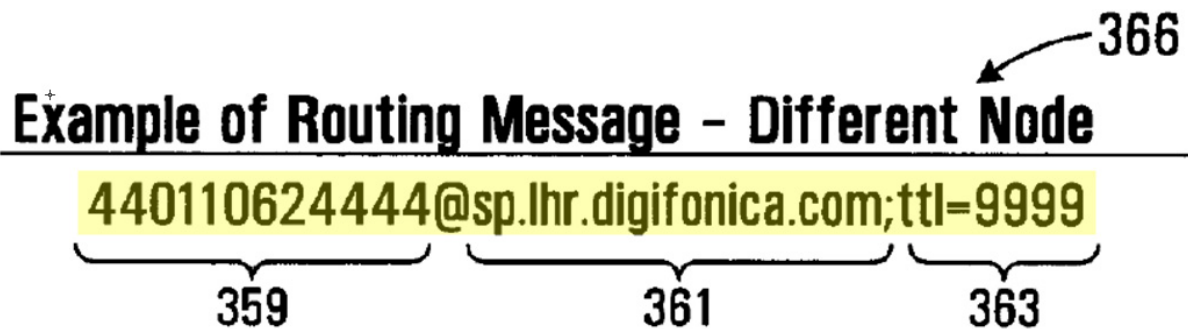
FIG. 16

73.   The call routing controller then sends the routing message (whether

public or private) to the call controller to route the call to the appropriate network.

(*See id.* at 21:13–16, 24: 65–67, 26:40–41.)

C.   The Challenged Claims

74.   The Challenged Claims are set forth below:

1. [1Pre] A process for operating a call routing controller to facilitate communication between callers and callees in a system comprising a plurality of nodes with which callers and callees are associated, the process comprising:

[1a] in response to initiation of a call by a calling subscriber, receiving a caller identifier and a callee identifier;

[1b] locating a caller dialing profile comprising a username associated with the caller and a plurality of calling attributes associated with the caller;

[1c] determining a match when at least one of said calling attributes matches at least a portion of said callee identifier;

[1d] classifying the call as a public network call when said match meets public network classification criteria and classifying the call as a private network call when said match meets private network classification criteria;

[1e] when the call is classified as a private network call, producing a private network routing message for receipt by a call controller, said private network routing message identifying an address, on the private network, associated with the callee;

[1f] when the call is classified as a public network call, producing a public network routing message for receipt by the call controller, said public network routing message identifying a gateway to the public network.

7. The process of claim 1 further comprising formatting said callee identifier into a pre-defined digit format to produce a re-formatted callee identifier.

27. [27Pre] A non-transitory computer readable medium encoded with codes for directing a processor to execute a method of operating a call routing controller to facilitate communication between callers and callees in a system comprising a plurality of nodes with which callers and callees are associated, the method comprising:

[27a] in response to initiation of a call by a calling subscriber, receiving a caller identifier and a callee identifier;

[27b] locating a caller dialing profile comprising a username associated with the caller and a plurality of calling attributes associated with the caller;

[27c] determining a match when at least one of said calling attributes matches at least a portion of said callee identifier;

[27d] classifying the call as a public network call when said match meets public network classification criteria and classifying the call as a private network call when said match meets private network classification criteria;

[27e] when the call is classified as a private network call, producing a private network routing message for receipt by a call controller, said private network routing message identifying an address, on the private network, associated with the callee; and

[27f] when the call is classified as a public network call, producing a public network routing message for receipt by a call controller, said public network routing message identifying a gateway to the public network.

28. [28Pre] A call routing apparatus for facilitating communications between callers and callees in a system comprising a plurality of nodes with which callers and callees are associated, the apparatus comprising:

[28a] receiving means for receiving a caller identifier and a callee identifier, in response to initiation of a call by a calling subscriber;

[28b] means for locating a caller dialing profile comprising a username associated with the caller and a plurality of calling attributes associated with the caller;

[28c] means for determining a match when at least one of said calling attributes matches at least a portion of said callee identifier;

[28d]   means for classifying the call as a public network call when said match meets public network classification criteria;

[28e]   means for classifying the call as a private network call when said match meets private network classification criteria;

[28f]   means for producing a private network routing message for receipt by a call controller, when the call is classified as a private network call, said private network routing message identifying an address, on the private network, associated with the callee; and

[28g]   means for producing a public network routing message for receipt by a call controller, when the call is classified as a public network call, said public network routing message identifying a gateway to the public network.

34. The apparatus of claim 28 further comprising formatting means for formatting said callee identifier into a pre-defined digit format to produce a re-formatted callee identifier.

54. [54Pre]   A process for operating a call routing controller to establish a call between a caller and a callee in a communication system, the process comprising:

[54a]   in response to initiation of a call by a calling subscriber, locating a caller dialing profile comprising a plurality of calling attributes associated with the caller; and

[54b]   when at least one of said calling attributes and at least a portion of a callee identifier associated with the callee match and when the match meets a private network classification criterion, producing a private network routing message for receipt by a call controller, said private network routing message identifying an address, on a private network, the address being associated with the callee; and

[54c]   when at least one of said calling attributes and said at least said portion of said callee identifier associated with the callee match and when the match meets a public network classification criterion, producing a public network routing

message for receipt by a call controller, said public network routing message identifying a gateway to a public network.

72. The process of claim 54 further comprising causing the private network routing message or the public network routing message to be communicated to a call controller to effect routing of the call.

73. A non-transitory computer readable medium encoded with codes for directing a processor to execute the method of claim 54.

74. [74Pre] A call routing controller apparatus for establishing a call between a caller and a callee in a communication system, the apparatus comprising:

[74a] a processor operably configured to:

[74b] access a database of caller dialing profiles wherein each dialing profile associates a plurality of calling attributes with a respective subscriber, to locate a dialing profile associated with the caller, in response to initiation of a call by a calling subscriber; and

[74c] produce a private network routing message for receipt by a call controller, said private network routing message identifying an address, on a private network, through which the call is to be routed, when at least one of said calling attributes and at least a portion of a callee identifier associated with the callee match and when the match meets a private network classification criterion, the address being associated with the callee; and

[74d] produce a public network routing message for receipt by a call controller, said public network routing message identifying a gateway to a public network, when at least one of said calling attributes and said at least said portion of said callee identifier associated with the callee match and when the match meets a public network classification criterion.

92. The apparatus of claim 74 wherein said processor is further operably configured to cause the private network routing message or

the public network routing message to be communicated to a call controller to effect routing of the call.

93. [93Pre] A call routing controller apparatus for establishing a call between a caller and a callee in a communication system, the apparatus comprising:

[93a] means for accessing a database of caller dialing profiles wherein each dialing profile associates a plurality of calling attributes with a respective subscriber, to locate a dialing profile associated with the caller, in response to initiation of a call by a calling subscriber; and

[93b] means for producing a private network routing message for receipt by a call controller, said private network routing message identifying an address, on a private network, through which the call is to be routed, when at least one of said calling attributes and at least a portion of a callee identifier associated with the callee match and when the match meets a private network classification criterion, the address being associated with the callee; and

[93c] means for producing a public network routing message for receipt by a call controller, said public network routing message identifying a gateway to a public network when at least one of said calling attributes and said at least said portion of said callee identifier associated with the callee match and when the match meets a public network classification criterion.

111. The apparatus of claim 93 further comprising means for causing the private network routing message or the public network routing message to be communicated to a call controller to effect routing of the call.

VIII. STATE OF THE ART

75.   Networks that provide telecommunications services are based on signaling protocols to establish connections from a calling (originating) party to a called (terminating) party. Protocols define the methods and processes used by

network equipment to route and control calls, often across multiple networks. Two

well-known networks are the Public Switched Telephone Network (PSTN) and the

Internet. Originally, the PSTN was used primarily for voice communications and

the Internet for data. Over the past several decades, services and capabilities for

both the PSTN and the Internet have expanded beyond these origins.

"Telecommunications Essentials", by Lillian Goleniewski, copyright 2002,

Chapter 5 "The PSTN", at pages 113-150 and Chapter 11, "Next-Generation

Network Services", at pages 329-368.

76.   A few basic terms regarding the PSTN are provided here to provide

clarity. Access to the PSTN (e.g., a telephone line) is generally provided by a

"class 5 switch" located in a "central office" (CO). Based on the "called party

telephone number" provided by the "calling party" telephone the class 5 switch

will route the call request to 1) another telephone line on the same class 5 switch,

2) another class 5 switch, or 3) to a "class 4 switch" (or to multiple class 4

switches) before being routed to the class 5 switch that provides access to the

"called party" telephone. Class 4 switches are associated with long distance or

"inter-exchange carrier" (IXC) services. The network and protocols used in the

PSTN to route calls is called "Signaling System #7" (SS7). The SS7 network and

protocols provide, inter alia, the means to route, establish, control, and disconnect

calls within the PSTN. "Telecommunications Essentials", by Lillian Goleniewski,

copyright 2002, Chapter 5, "The PSTN" at pages 113-150.

77.   The ITU E.164 standard, established the format for telephone

numbers ("addresses") that are used by the interconnected PSTNs around the

world. The use of E.164 telephone numbers is the basis for enabling network

protocols, and associated equipment, to route an originating telephone call request,

through multiple switches and network equipment, to the destination (terminating)

endpoint (e.g., a telephone). Users of the PSTN must provide an E.164 compatible

number to the network to initiate a telephone call.   International

Telecommunication Union (ITU) E.164 standard, "The international public

telecommunication numbering plan" (1997), Section 2, "Scope", at page 1, and

Section 4.1 "number", at page 2. See also "Telecommunications Essentials", by

Lillian Goleniewski, copyright 2002, Chapter 5, "The PSTN.", at page 121.

Following is Figure 1 from the E.164 standard.
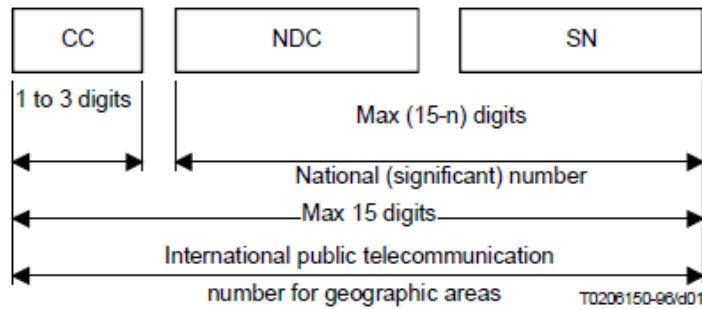
CC   Country Code for geographic areas
NDC   National Destination Code (optional)
SN   Subscriber Number
n   Number of digits in the country code

NOTE – National and international prefixes are not part of the international public telecommunication number for geographic areas.

Figure 1/E.164 – International public telecommunication number structure for geographic areas

ITU-T E.164 (1997), Section 6.2.1, at page 6.

78.   When a call is made within a country (i.e., it is not an international call) then only the digits shown in E.164 Figure 1 as "National (significant) number" are required. National numbering plans can be unique in different countries with a variety of possible formats used even within one country. For example, in North America many people will be familiar with 7-digit dialing, 10-digit dialing, and 11-digit dialing. The specific format required at a given location may depend on the local area code, and other factors. Calls made within a country may require a "National Destination Code" (also referred to as "National Dialing Digit" (NDD)) to precede the digits of the telephone number. This is a '1' when

49

addressing a call within North America. Only if a call is destined for outside the country (i.e., an international call) is the country code required, and in this case, the NDC would be omitted. Additionally, when an international call is addressed, the country code will be preceded by the "International Prefix" (also known as the "International Dialing Digit (IDD)) which may be one or more digits that are specific to each country. The International Prefix allows the switching system to determine the call is an international call and the digits after the International Prefix are the country code. Telcordia Technologies Special Report, SR-2275, Issue 4, October 2000 entitled "Telcordia Notes on the Networks", Section 3.7, **"**Dialing Procedures", at pages 3-8 to 3-12, and Section 3.10 "International Direct Distance Dialing", at pages 3-13 to 3-14. E.164 telephone numbers and their application for call routing would be well-known to a person of normal skill in the art starting at least in the 1990's.

79.   When a call is connected in the PSTN, the information (e.g., voice media) that is transmitted to and from the calling and called parties is transmitted over "circuit-switched" data paths. PSTN circuit-switched transmission is also referred to as "time-division multiplexing" (TDM). "Telecommunications Essentials", by Lillian Goleniewski, copyright 2002, Chapter 4, "Establishing Communications Channels", at pages 99-100. See also Telcordia SR-2275, Issue

4, October 2000, Section 18.1 "Introduction to Next Generation Networks", at page 18-1. A person of normal skill in the art, starting at least in the 1990's, would understand PSTN related circuit-switched connections, access, SS7 protocols, call routing, call control, switching, and transmission.

80.   The PSTN routes call requests from one endpoint on the PSTN (e.g., a calling party's telephone) to any other endpoint connected to the PSTN (e.g., a called party's telephone). Softswitch Architecture for VoIP (Frankin D. Ohrtman, Jr., copyright 2003), Chapter 2 "The Public Switched Telephone Network (PSTN)", at pages 11-13.   The PSTN is described as a "public" network because the telecommunications services provided are available to the public and connections can be routed between any two endpoints associated with a service and connected to the PSTN. See the United States Telecommunications Act of 1996. This end-to-end call routing is possible due to the interconnection of multiple PSTN networks at the local, regional, national, and international level. ITU-T E.164 (1997), Section 4.4 at page 3, Section 4.17 at page 4, and Annex A at page 13. A person of normal skill in the art, starting at least in the 1990's ,would understand the public access requirements of the PSTN in the United States and the ability to connect calls from any international PSTN subscriber to another.

81. The Advanced Intelligent Network (AIN) has been a deployment architecture for the PSTN starting in the 1990s. The AIN is based on a network of service switching points (SSP), signal transfer points (STP), and service control points (SCP) which communicate using SS7 protocols. A basic example is when a calling party uses a telephone to signal a called party telephone number to the CO class 5 switch (an SSP), the SSP may transmit SS7 routing request messages (including the calling party and called party telephone numbers) through a network of STPs, to an SCP. The SCP may return (via SS7 signaling) a routing message including information for the SSP to use to route the call. Softswitch Architecture for VoIP (Frankin D. Ohrtman, Jr., copyright 2003), Chapter 2 "The Public Switched Telephone Network (PSTN)", at pages 27-30. A person of normal skill in the art, starting at least in the 1990's, would understand the components and concepts of the AIN and the AIN related features in the PSTN for producing and using call routing messages.

82. Routing a PSTN call request is based on the called party telephone number and the calling party telephone number. For example, the switching equipment in the PSTN (e.g., a class 5 switch) which serves the calling party, possibly in concert with other network entities (e.g., an SCP), uses the called party telephone number to determine which trunk or line through which to route a call.

Likewise, the PSTN may use the calling party number and/or the called party number to determine which interexchange (long distance) carrier's switch through which to route a call. Softswitch Architecture for VoIP (Frankin D. Ohrtman, Jr., copyright 2003), Chapter 2 "The Public Switched Telephone Network (PSTN)", at pages 27-30.

83.   With the introduction of SCPs in the 1990s came the ability for the PSTN to store and maintain service / user profiles associated with each telephone number. Access to a user profile for editing or updates requires a user identifier (such as the telephone number associated with the account) and possibly a PIN (Personal Identification Number). These user profiles may be used to enable services, for example speed dialing, or selective call routing. See "Perspectives on the AIN Architecture," Berman, Roger K., and Brewster, John H., IEEE Communications Magazine, Feb. 1992, pp. 27-32. Additionally, US 7,907,714 patent to Baniak, et al, entitled "Profile management system including user interface for accessing and maintaining profile data of user subscribed telephony services" (published March 15, 2011, filed July 21, 2006, priority date April 3, 1997) describes methods for accessing and modifying SCP based user profiles. A person of normal skill in the art, starting at least in the late 1990's would understand SCP based user profiles, and associated call routing control features.

84.   The 3GPP (Third Generation Partnership Project) began developing

the next generation of telecommunications standards and requirements called the

IP Multimedia Subsystem (IMS) in the 1990s.   The 3GPP published groups of

standards that make up the pre-IMS and IMS requirements in a series of "releases"

starting in 1999 (IMS release "99"), and IMS release 5 in 2002 which is considered

to be the first full IMS release.   IMS release 5 was intended "to be a standardized

access-independent IP-based architecture that interworks with existing voice and

data networks for both fixed (e.g., PSTN, ISDN, Internet) and mobile users (e.g.,

GSM, CDMA)."   See "The IMS IP Multimedia Concepts and Services", Third

edition, Miikka Poikselka and Georg Mayer, published 2009, Chapter-1,

"Introduction", at pages 3-14.

85.   As described above, the PSTN AIN architecture includes SCPs within

which subscribers' user profiles may be maintained.   The evolution of the SCP

user profile to IMS includes user service profiles which are maintained in the

Home Subscriber Server (HSS) defined with the IMS.   User profiles can be used in

conjunction with IMS SIP Application Servers (AS) to control the routing of

outgoing (originating) and incoming (terminating) calls.   See the information

provided in "The IMS IP Multimedia Concepts and Services", Third edition,

Miikka Poikselka and Georg Mayer, published 2009 at pages 24-25 and 86-94,

regarding the IMS HSS, service profiles, Application Servers (AS) and the S-CSCF (Serving Call Session Control Function) related to originating (outgoing) and terminating (incoming) session routing control.

86.   The Internet is the interconnection of multiple packet-based data networks which communicate to initiate, route, establish, control, and end sessions using multiple layered protocols. The Internet routes data session set-up requests from one endpoint to another endpoint. The Internet uses the "Internet Protocol" (IP) to route packets of data through the network. The well-known "IP address" is assigned to endpoints connected to an IP network and is the basis for enabling IP protocols and associated equipment to route data packets from an originating endpoint, through multiple packet switches and other network elements, to the destination (terminating) endpoint.   See "Telecommunications Essentials", by Lillian Goleniewski, copyright 2002, Chapter 9, "The Internet: Infrastructure and Service Providers", at pages 244-267.

87.   The Internet is distinguished from the PSTN for providing voice services in multiple ways including 1) transmission of call media (voice data) over the Internet is via packet-switching also known as "datagrams" rather than the PSTN's circuit-switched, TDM based connections; 2) VoIP networks may include private networks (e.g., LANs) and public networks (e.g., the Internet). IP network

endpoints directly accessed by users (e.g., a computer terminal or a telephone) may be connected to a private network (e.g., a LAN) that may route a session over the public Internet to another endpoint which is connected to another private network. See Telecommunications Essentials", by Lillian Goleniewski, copyright 2002, Chapter 11, "Next Generation Network Services", at pages 329-368; 3) connection to, and use of, the PSTN is associated with national regulations, including requirements to provide universal service to the public, and national and international interconnection, whereas the Internet is generally considered to be a global network with little regulation regarding access, interconnection, or use. See the Telecommunications Act of 1996, and Softswitch Architecture for VoIP (Frankin D. Ohrtman, Jr., copyright 2003), Chapter 11 "Softswitch Economics", at pages 238-239.

88. The book entitled "Softswitch Architecture for VoIP" attributes the "invention" of VoIP to Republic Telcom of Boulder Colorado for their patent number 4,782,485 entitled "Multiplexed digital packet telephone system" (published November 1, 1988, filed November 9, 1987, and priority date August 23, 1985). Softswitch Architecture for VoIP (Frankin D. Ohrtman, Jr., copyright 2003), Chapter 4 "Voice over Internet Protocol", at page 68. A person of normal skill in the art, starting in the late 1990's, would have known about the use of the

packet-switched Internet and IP networks for voice communications and Voice

over Internet Protocol (VoIP).

89.   A few basic terms regarding the Internet and VoIP are provided here

to provide clarity. The use of private data networks and the Internet for the

connection of voice calls has been well-known as "VoIP" (Voice over Internet

Protocol) to those of normal skill in the art starting in the late 1990's. Access to

the Internet is generally provided by an "Internet Service Provider" (ISP) which

provides a connection to the global Internet network. The ISP connection is

usually made to a user's Local Area Network (private or enterprise LAN) which is

commonly an "Ethernet" network for the physical and link layers. "Dial-up"

connections using a computer, modem, and an analog telephone line are another

type of Internet access provided by ISPs. The ISPs, private LANs, and public

Internet use the "Internet Protocol" (IP), including well-known "IP addresses"

which are used to route data packets from one endpoint on a network (e.g., a

calling party (originating) telephone) to another endpoint on an interconnected

network (e.g., a called party (terminating) telephone). IP networks are defined by

being based on the "IP Suite" of protocols which may also be referred to as

"TCP/IP". The VoIP related software that runs on an endpoint device (e.g., a

telephone or a computer) may be referred to as "client software' and/or a "user

agent." See "Telecommunications Essentials", by Lillian Goleniewski, copyright 2002, Chapter 9, "The Internet: Infrastructure and Service Providers", at pages 244-267. Also see Softswitch Architecture for VoIP (Frankin D. Ohrtman, Jr., copyright 2003), Chapter 5 "SIP: Alternative Softswitch Architecture", at pages 87-112.

90.   The messages transmitted to establish a connection between a calling party's VoIP telephone, the IP network, and a called party's VoIP telephone, and through a VoIP PSTN gateway to a PSTN telephone, comprise the protocols used to establish the required end to end connection. Telecommunications network protocols are generally described as being a "layered" architecture with the lowest layer being the "physical layer" (for example a modulated electrical signal). Each subsequent higher layer makes use of the features and capabilities of the layer below it to perform the intended function. For example, the well-known seven layer OSI (Open Systems Interconnection) model is used to describe a standardized "protocol stack" used for the communication functions in a telecommunications network. Telcordia SR-2275, Issue 4, October 2000, Section 18.2.2.1 "OSI Model", at pages 18-12 to 18-13.

91.   IP networks used for VoIP are described as a layered protocol architecture that are aligned to some degree with the OSI model. The following

58

figure shows the OSI model and how the layered protocol concepts relate to the IP

protocol suite.
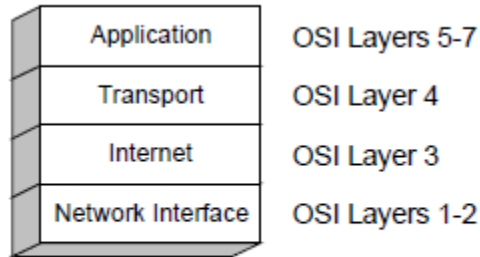
Figure 18-6. Protocol Layering in TCP/IP

The following figure illustrates how the principle of encapsulation described in the

OSI model relate to the protocol layers of the IP protocol suite.
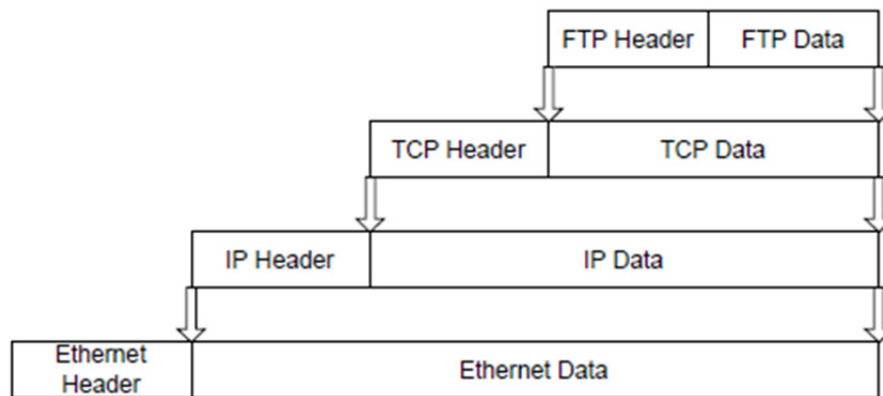
Figure 18-7. Encapsulation in the IP Protocol Suite

Telcordia SR-2275, Issue 4, October 2000, Section 18.2.2.2 "IP Protocol Suite", at

pages 18-13 to 18-14.

59

92. Referring to figure 18-6 from Telcordia SR-2275, the network interface layer comprises the physical hardware and electrical signals, and the data link protocols that are used between two physically connected endpoints. A data link protocol uses the physical layer to reliably convey bits of data (1s and 0s) across the physical channel. Every network device that supports the TCP/IP protocol suite must have a physical network interface (i.e., an I/O port) for transmitting and receiving IP data. A widely used I/O port for IP networks is the Ethernet physical interface. Telcordia SR-2275 in Fig 18-7 (supra) described the IP protocol suite network interface as "Ethernet." Telcordia SR-2275, Issue 4, October 2000, Section 18.2.2.2.1 "Network Interface", at pages 18-14 to 18-15. An Ethernet I/O port is typically provided using a well-known RJ-45 connector using also well-known cat-5 or cat-6 cabling. Telecommunications Essentials", by Lillian Goleniewski, copyright 2002, Chapter 8, "Local Area Networking", at page 221.

51. RFC 1122 defines:

Physical network interface

This is a physical interface to a connected network and has a (possibly unique) link-layer address. Multiple physical network interfaces on a single host may share the same link-layer address, but the address must be unique for different hosts on the same physical network.

IETF RFC 1122 (1989) entitled "Requirements for Internet Hosts --

Communication Layers", Section 1.3.3, at page 18. Examples of physical

networks include Ethernet and other IEEE 802 type networks. IETF RFC 1122,

Section 2.3.3 "Ethernet and IEEE 802 Encapsulation", at pages 24-25. RFC 1122

defines: "Physical network interface[:] This is a physical interface to a connected

network and has a (possibly unique) link-layer address." IETF RFC 1122, Section

1.3.3, at page 18. Also, "An IP address is a logical address, in contrast to the

hardware address of an Ethernet frame. While the Ethernet address is typically

"burned into" the Ethernet hardware (e.g., an Ethernet card in a PC), the IP address

is typically assigned through software." Also:

> In this frame, the destination and source addresses refer
> to the hardware addresses of the network interface cards
> of the two communicating endpoints on a network. If this
> frame were transmitted across the internetwork illustrated
> earlier, then the source address would be the hardware
> address of the Ethernet card in the client PC, and the
> destination address would be the hardware address of the
> first router (sometimes referred to as a "gateway"). That
> is, the Ethernet frame carries its data across a network,
> and the router marks the end of the first network of the
> figure. At this point, the router strips away (decapsulates)
> the Ethernet headers and examines the data field (i.e., the
> IP packet). For example, the IP destination address would
> be examined to determine what the next hop physical
> address should be. After interpreting the IP fields, the
> router re-encapsulates the packet in another frame
> appropriate to the outgoing network, such as Ethernet,
> Token Ring, or PPP. The source address of the new

> frame would be the router's (outgoing) port. The destination address would be the physical address that was determined from applying the routing table rules to the IP destination address.

Telcordia SR-2275, Issue 4, October 2000, Section 18.2.2.2.1 "Network Interface"

and Section 18.2.2.2, "Internet Protocol (IP)", at pages 18-14 to 18-16.

93.　A person of normal skill in the art, starting at least in the 1990's,

would have understood the physical and electrical IP network interface (e.g.,

Ethernet) is an Input / Output (I/O) port necessary for connecting a network device

to an IP network (including the Internet).

94.　RFC 791 depicts the IP packet format as follows:

```
                      3.   SPECIFICATION

       3.1.  Internet Header Format

        A summary of the contents of the internet header follows:


          0                   1                   2                   3
          0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         |Version|  IHL  |Type of Service|          Total Length         |
         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         |         Identification        |Flags|      Fragment Offset    |
         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         |  Time to Live |    Protocol   |         Header Checksum        |
         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         |                       Source Address                          |
         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         |                    Destination Address                        |
         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         |                    Options                    |    Padding    |
         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
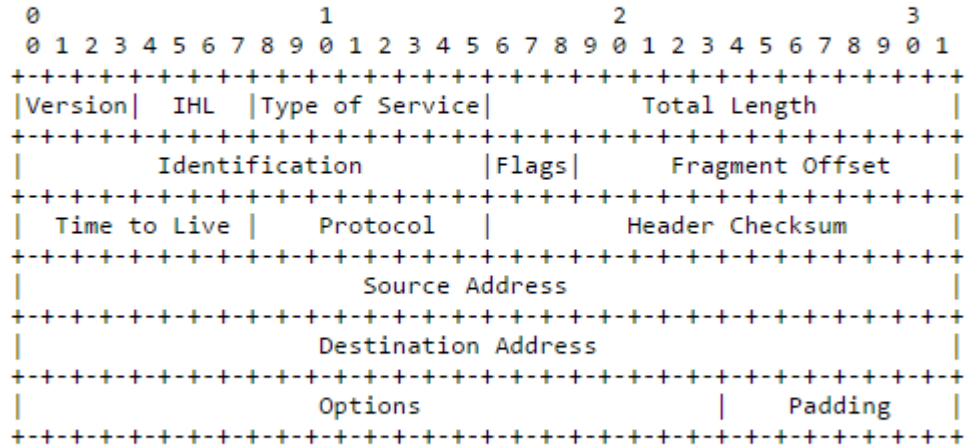
Example Internet Datagram Header

Figure 4.

Note that each tick mark represents one bit position.

IETF RFC 791 "Internet Protocol Darpa Internet Program Protocol Specification" (September 1981), Section 3.1, at page 11. The "internet module" (software) (i.e., the IP layer) that resides in every host associated with a local network interface will use the lower layer network interface to send the IP packet between network interfaces. The internet module will determine how to route the packet's next hop to the next local network interface based on the contents of the "Destination Address" IP field. IETF RFC 791, Section 1.4 "Operation", at pages 2-3, and Section 2.2 "Model of Operation", at pages 5-6.

95.   The Internet, or IP, layer of the IP protocol suite uses the capabilities

provided by the underlying network interface layer (e.g., physical and link layers)

to carry IP packets.   An IP layer packet is the unit of data that contains the IP

address which is used to route the packet through the interconnected IP networks.

All layers above the IP layer use the IP layer to transmit data from one endpoint's

(host computer, IP telephone, etc.) IP layer interface to another endpoint's IP layer

interface.   IETF RFC 791, Section 2.2 "Model of Operation", at pages 5-6.   A

person of normal skill in the art, starting at least in the 1990's, would have

understood that an IP address is the basis for routing all service, session, call, etc.

requests from one IP network endpoint to another IP network endpoint.

96.   The internet module of each local network interface which receives an

IP packet will continue routing the packet from one network interface to the next (a

"hop") until either 1) the packet is discarded because the packet has experienced

too many hops (as indicated by the "Time to Live" field being a value of zero); 2)

the packet is discarded due to a "Header Checksum" error indicating the data in the

header has been corrupted, or 3) the packet has reached the local network interface

which has been assigned the IP address present in the IP packet's "Destination

Address" field. IETF RFC 791, Section 3.1, "Internet Header Format", at page 14,

Section 1.4, "Operation", at page 3, and Section 2.2, "Model of Operation, at pages 5-6.

97.   The "Time to Live" field is normally set by the application initiating the IP packet transmission to control how long the IP packet may remain in the network before reaching its intended destination.   Although the IP protocol specifies this field to be in seconds of time, each network interface hop is required to decrement the Time to Live value by one so the Time to Live field is actually used to limit the number of hops a packet will be allowed to take. IETF RFC 791 Section 1.4 "Operation", at pages 2-3, and Section 3.1 "Internet Header Format", at page 14.

98.   RFC 791 is instructive regarding IP addressing:

```
Addressing

  A distinction is made between names, addresses, and routes [4].   A
  name indicates what we seek.  An address indicates where it is.  A
  route indicates how to get there.  The internet protocol deals
  primarily with addresses.  It is the task of higher level (i.e.,
  host-to-host or application) protocols to make the mapping from
  names to addresses.   The internet module maps internet addresses to
  local net addresses.  It is the task of lower level (i.e., local net
  or gateways) procedures to make the mapping from local net addresses
  to routes.
```

IETF RFC 791, Section 2.3 "Functional Description", at page 7. The reference to "[4]" is: "[4] Shoch, J., 'Inter-Network Naming, Addressing, and Routing,' COMPCON, IEEE Computer Society, Fall 1978." The IP layer uses IP addresses

65

and the underlying lower layers to route packets through an IP network. If a non-IP address identifier (e.g., a "name") is used at a higher layer protocol, then that name must be converted to an IP address to properly construct an IP layer packet. For example, "DNS, or Domain Naming Service, which associates a familiar user-friendly name with an IP address. DNS is used transparently to the end user to resolve host and domain names such as www.telcordia.com to an IP address with which a user layer application will complete an application layer connection." Telcordia SR-2275, Issue 4, October 2000, 18.2.2.2.4, "Applications", at pages 18-18.

99.   An IP address is coded to specify both a network and a host (e.g., computer, server) on that network. IETF RFC 791, Section 3.2, at page 24. The following figure from Telcordia SR-2275 depicts an example of a Class B IP address as /16 showing the part of the IP address which identifies a network as the first 16 bits of the IP address and the last 16 bits identifying a host (computer).
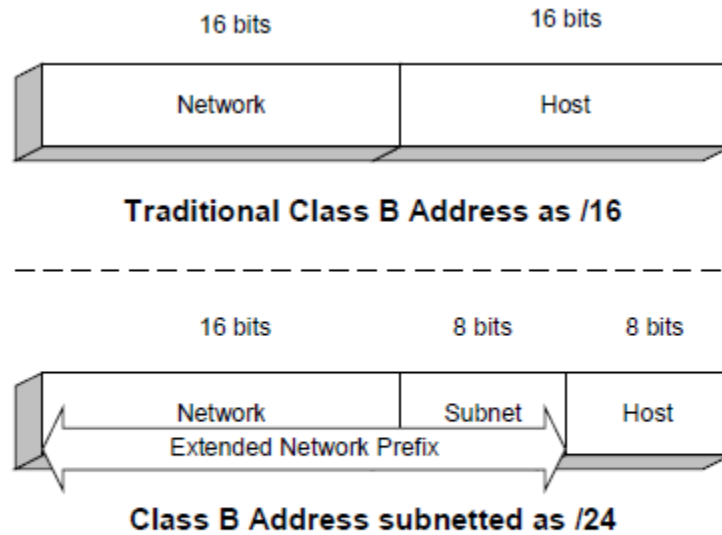
Figure 18-12. Class B Addresses

Telcordia SR-2275, Issue 4, October 2000, 18.2.2.2.4, "Applications", at pages 18-
18.

100.   Services that may be used by higher layer protocols have been
developed for translating "names", which human users may use as identifiers for
addressing a network endpoint, to an IP address usable by the IP network layer.
One example is the well-known Dynamic Name Service (DNS). For example, if a
user at an originating IP endpoint wanted to send a message to a terminating IP
endpoint, that user may provide a "Uniform Resource Identifier" (URI) (e.g.,
sip:jrbress@telecom-expert.com) to the higher layer application. If a URI type
address is used to facilitate the IP packet routing process, address translation would
be required using well-known services such as DNS. DNS provides a look-up of a

domain style name (such as a URI) and returns the IP address associated with the

URI provided in a look-up request. IETF standards RFC-1034 and RFC-1035,

published in November 1987, provide the details for the use of domain names in IP

networks. A person one of normal skill in the art, starting at least in the 1990's,

would have been familiar with the use of domain names and DNS services.

101. Another well-known method which is used to support translation of

telephone number style identifiers to IP addresses is presented in the IETF RFC

2916 standard entitled "E.164 number and DNS" published in September, 2000.

RFC 2916 was made obsolete by the publication of RFC 3761 entitled "The E.164

to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System

(DDDS) Application (ENUM)" published in April, 2004. RFC 2916 and RFC

3761 are generally known as the "ENUM" standard. IETF RFC 3761 (ENUM), at

page 1.

102. RFC 3761 (ENUM) describes the process used to convert an E.164

number into a format that can be used by an ENUM server as:

> 1. Remove all characters with the exception of the digits.
> For example, the First Well Known Rule produced the
> Key "+442079460148". This step would simply remove
> the leading "+", producing "442079460148".
>
> 2. Put dots (".") between each digit. Example:

4.4.2.0.7.9.4.6.0.1.4.8

3. Reverse the order of the digits. Example:

8.4.1.0.6.4.9.7.0.2.4.4

4. Append the string ".e164.arpa" to the end. Example:

8.4.1.0.6.4.9.7.0.2.4.4.e164.arpa

IETF RFC 3761 (ENUM), Section 2.4, at page 4.

103.   An example of an ENUM lookup is as follows:

4.1. Example

$ORIGIN 3.8.0.0.6.9.2.3.6.1.4.4.e164.arpa.

NAPTR   10   100   "u"   "E2U+sip"
"!^.*$!sip:info@example.com!"

NAPTR   10   101   "u"   "E2U+h323"
"!^.*$!h323:info@example.com!"

NAPTR   10   102   "u"   "E2U+msg"
"!^.*$!mailto:info@example.com!"

This   describes   that   the   domain
3.8.0.0.6.9.2.3.6.1.4.4.e164.arpa. is preferably contacted
by SIP, secondly via H.323 for voice, and thirdly by
SMTP for messaging. Note that the tokens "sip", "h323",
and "msg" are Types registered with IANA, and they
have no implicit connection with the protocols or URI
schemes with the same names.

In all cases, the next step in the resolution process is to
use the resolution mechanism for each of the protocols,
(specified by the URI schemes sip, h323 and mailto) to
know what node to contact for each.

RFC 3761 (ENUM), Section 4.1, at page 10. An ENUM server therefore provides

a means to convert a PSTN type E.164 telephone number to an address that may be

used for routing on the Internet. A person of normal skill in the art, starting at least

in the 1990's, would be familiar with the ENUM standard and the use of ENUM

servers to convert E.164 telephone numbers to IP network routable addresses.

104.   US patent 6,594,254 to Kelly discloses a process similar to the ENUM

standard:

> A method and apparatus for translating a domain name
> representing a telephone number into a network protocol
> address includes a domain name server architecture
> containing logic responsive to a telephone number
> domain name, the telephone number domain name
> representing the country code, area code, exchange, or
> subscriber number of a subscriber apparatus telephone
> number. The logic resolves the telephone number domain
> name into a network protocol address usable in
> ultimately initiating a communication with the subscriber
> apparatus on a circuit-switched network. In one
> embodiment, a hierarchical tree of domain names and
> subdomain names representing the country codes, area
> codes and exchange codes of telephone numbers is
> constructed to assist in the process of resolving domain
> names to network protocol addresses.

US Patent 6,594,254 to Kelly (published July 15, 2003, filed August 14, 1997, and

priority date August 16, 1996) entitled "Domain Name Server Architecture for

Translating Telephone Number Domain Names Into Network Protocol Addresses",

at Abstract.

105. Kelly discloses a capability similar to ENUM for address translation between PSTN addresses (telephone numbers) and IP routable addresses (IP addresses and domain names). In one embodiment disclosed by Kelly, the IP address returned by an address translation server is the IP address of a gateway providing access to the circuit-switched PSTN. The utility of the ENUM standard and the disclosures of Kelly would be well understood by one of normal skill in the art starting at least in the late 1990's. For example, when a need arises to connect a call request from an IP network endpoint (with its associated IP address) to a PSTN endpoint (with its associated E.164 telephone number) the system taught by Kelly and the methods provided in the ENUM standard would be an obvious solution.

106. In summary of the paragraphs supra regarding IP network address translations, IP protocol suite layers above the Internet (IP) layer may use names, URIs, telephone numbers, etc., to identify an intended destination endpoint. Higher layer protocols make use of the underlying IP layer for routing, by utilizing a service to translate name type addresses to an IP address which is provided to the IP layer. The IP layer uses the IP address in the Destination Address field of the IP packet to route the packet to the destination network interface assigned to that IP address. Telcordia SR-2275, Issue 4, October 2000, 18.2.2.2 "IP Protocol Suite",

at pages 18-13 to 18-20. A person of normal skill in the art, starting at least in the

1990's, would understand domain names, URIs, etc., and the services used to

translate these names to IP addresses for routing over the Internet.

107. The IP layer of the IP suite of protocols may be summarized in

general terms as being responsible for delivering a packet of data from a source

address associated with a physical network interface to a destination address

associated with a physical network interface. The IP layer does not provide flow

control, error detection, or retransmission. These features must be implemented in

the higher layers such as the TCP/transport layer or as part of an application layer

feature. The network interface physical I/O port (e.g., an Ethernet port) of an

endpoint which is the target destination of a packet is typically part of a computer

or some other device that will make use of the data encapsulated in the IP packet.

Telcordia SR-2275, Issue 4, October 2000, Section 18.2 "Survey of IP

Networking", at pages 18-8 to 18-20. See also IETF RFC 791.

108. The IP protocol suite layer above the IP layer is called the transport or

TCP layer. The TCP layer receives data from the application layer and

encapsulates the application data with a TCP layer header. The TCP layer is

generally responsible for delivering the application data (the "payload") to a

specific service or software program on the endpoint that will receive the IP layer

packets which are created to encapsulate the TCP layer data before being

transmitted to the network. The TCP layer may provide features for flow control,

error detection, and retransmission. In this way, the underlying IP network can be

used to carry packets for multiple services running at the same time on one

endpoint device. Some of the well-known and often used services (applications)

that make use of, and have their data carried using, IP protocols include File

Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Domain Name

System (DNS), Dynamic Host Configuration Protocol (DHCP), Hypertext Transfer

Protocol (HTTP), H.323, Session Initiation Protocol (SIP), Real Time Protocol

(RTP), and many others. Telcordia SR-2275, Issue 4, October 2000, Sections

18.2.2.2.3 Transport (TCP and UDP)" and 18.2.2.2.4 "Applications", at pages 18-

16 to 18-18.

109. The TCP layer uses "port numbers" associated with the source and

destination (input / output (I/O)) of applications which interface to the TCP layer.

> Once an IP datagram has arrived at its destination, the
> receiving host must decide what application is expected
> to deal with the incoming data. Consequently, the IP
> datagram is decapsulated so that transport layer
> information can be examined. In most cases, one of two
> transport layer protocols is used: the Transmission
> Control Protocol (TCP) or User Datagram Protocol
> (UDP). A common feature of both these protocols is that
> they use source and destination port numbers to control

the flow of information between sending and receiving applications within the end hosts.

TCP and UDP are designed for different types of applications. In particular, TCP is designed for guaranteeing (via acknowledgment numbers) the orderly (via sequence numbers) delivery of data. It essentially provides a virtual circuit for applications (e.g., file transfer) that require such services.

By comparing the TCP and UDP packet figures (Figures 18-10 and 18-11), it is obvious that TCP requires overhead for providing its services. In contrast, the UDP packet sacrifices these sequencing and delivery guarantees for faster service. If an application that uses UDP needs to be concerned with guaranteed delivery or sequencing, then the application itself is responsible for those services.

Bit Position

	Source Port	Destination Port
	Sequence Number	
	Acknowledgement Number	
Data Offset	Reserved	Code Bits	Window
	Checksum	Urgent Pointer
	Options	Padding
	Data	
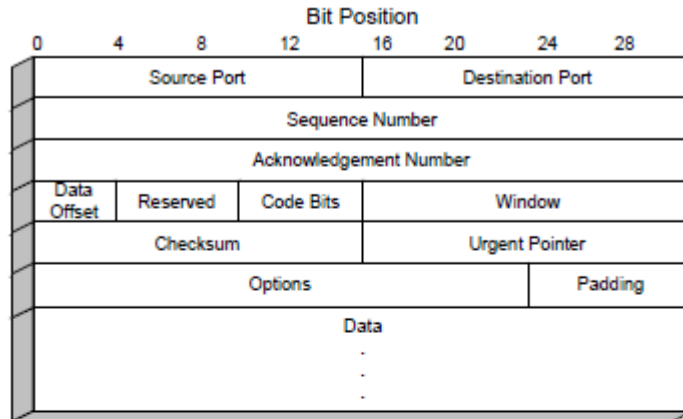
Figure 18-10. TCP Segment Format

Bit Position

Source Port	Destination Port
Message Length	Checksum
Data	
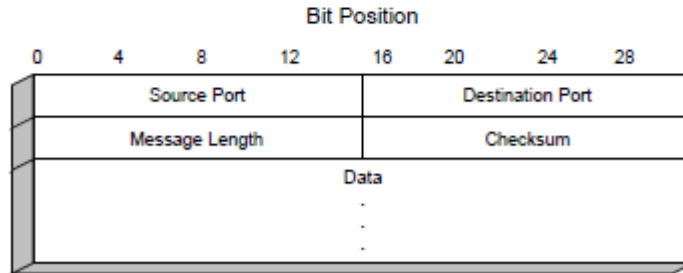
Figure 18-11. UDP Datagram Format

Telcordia SR-2275, Issue 4, October 2000, Section 18.2.2.2.3, at pages 18-15 to

18-16. A person of normal skill in the art, starting at least in the 1990's, would

have been understood the use of the IP protocol suite transport protocols TCP and

UDP and the use of source and destination ports (i.e., I/O ports) for handling data

between the transport layer and higher layer applications.

110. As described above, the RFC 791 defined Internet Protocol packet

header includes a data field called "Time to Live" (TTL). RFC 791 describes a

75

specific use for the TTL field which is to limit the number of hops (network

interfaces) that a packet may traverse before being discarded. Other IP protocol

suite layers and applications also include "Time to Live" fields with their own

specified use and operation that may not be related to the IP layer Time to Live

field. For example, the aforementioned DNS related IETF standards, RFC 1034

and RFC 1035, describe a different use and format for a header field also called

"Time To Live" (TTL).

> TTL a 32 bit unsigned integer that specifies the time
> interval (in seconds) that the resource record may be
> cached before it should be discarded. Zero values are
> interpreted to mean that the RR can only be used for the
> transaction in progress, and should not be cached.

IETF RFC 1035, Section 3.2.1, at page 11. In RFC 791 (Internet Protocol) the

TTL field is used to limit the time an IP layer packet may remain in the network by

limiting the number of hops an IP packet may take. In DNS Resource Record

(RR) queries or transactions, the Time to Live field is used to limit the time that a

resource record should be cached.

111.   The H.323 standard also describes use of a Time to Live field in the

messages used for terminals to register with an H.323 gatekeeper.

> An endpoint's registration with a Gatekeeper may have a
> finite life. An endpoint may request a **timeToLive** in the
> RRQ message to the Gatekeeper. The Gatekeeper may

> respond with an RCF containing the same **timeToLive**, a longer **timeToLive**, or a shorter **timeToLive**. If the endpoint cannot accommodate a larger **timeToLive** proposed by the Gatekeeper, the endpoint shall use the largest **timeToLive** value that it can support and that is less than the **timeToLive** proposed by the Gatekeeper. After this time, the registration shall be expired. The **timeToLive** is expressed in seconds.

H.323 standard (2003), Section 7.2.2.1, at page 55. A person of normal skill in the art, starting at least in the 1990's, would have been aware of the use of "Time to Live" (TTL) fields in a variety of communications protocols, messages, and databases with the specific use of a TTL field dependent upon the specific protocol or application in which the TTL field is included.

112. An IP network that is between two endpoints is usually depicted as a "cloud". The cloud represents network equipment which may include, inter alia, "routers", "soft-switches" (i.e., software based switches), "signaling gateways", "media gateways", "proxy servers", "registrar servers", "redirect servers" and in general, "application servers". The network components are designed to work together to route data packets from one endpoint to another using the destination IP address contained within each IP layer packet. Applications may provide information carried in layers above the IP layer which may be used to, inter alia, authenticate a user, negotiate capabilities, translate a name style address to an IP address, and route a call request. Once a session is established, packets may also

contain "media" which for VoIP would be digitized voice data. See Telcordia SR-2275, Issue 4, October 2000, Section 18.2 "Survey of IP Networking", at pages 18-8 to 18-20. Also see "Telecommunications Essentials", by Lillian Goleniewski, copyright 2002, Chapter 11, "Next-Generation Network Services", pages 329-368.

113. Two well-known protocols used "on top" (above) of the IP layer to provide transport are the "Transmission Control Protocol" (TCP) from which the well-known "TCP/IP" protocol is derived, and the "User Datagram Protocol" (UDP). Higher IP protocol suite application layer protocols such as "Real-Time Protocol" (RTP) are used for carrying voice data packets, normally using the UDP transport layer. "Session Initiation Protocol" (SIP) and ITU "H.323" are used, normally with TCP/IP or UDP, for carrying signaling related packets for session (call) establishment and control. See Telcordia SR-2275, Issue 4, October 2000, Section 18.2 "Survey of IP Networking", at pages 18-8 to 18-20. Also see "Telecommunications Essentials", by Lillian Goleniewski, copyright 2002, Chapter 11, "Next-Generation Network Services", pages 329-368.

114. In a typical end-to-end SIP VoIP scenario, the calling party telephone sends a SIP "INVITE" message to the called party telephone. This message is routed through the calling party's LAN, the Internet "cloud", to the called party's LAN, and is received by the called party's telephone. Several messages may be

transmitted between the calling and called party endpoints (and possibly other network elements used for authentication, address translation, capabilities negotiation, etc.) and eventually a bi-direction stream of voice data packets (e.g., RTP packets) will be transmitted to and from the calling and called party telephones and a voice conversation ensues. When one party ends the call, a SIP "Bye" message is sent in which case both endpoints stop sending voice data. Addressing for endpoints is either by a direct IP address or indirect addressing using, for example, a "Uniform Resource Identifier" (URI) (e.g., sip:jrbress@telecom-expert.com). If a URI type address is used, then as part of the call routing process, address translation will occur using well-known services such as the DNS or ENUM services described above. Softswitch Architecture for VoIP (Frankin D. Ohrtman, Jr., copyright 2003), Chapter 5 "SIP: Alternative Softswitch Architecture", at pages 87-112.

115. The connection of VoIP telephones over an all IP network (IP to IP) was enhanced through many standardized protocols and services including DNS and ENUM, described above. In the case of IP to IP connections, a gateway is generally not required. However, to enable IP to PSTN connections, a gateway is required to convert the incompatible call set-up and routing protocols (signaling) and the incompatible data (media) types. Softswitch Architecture for VoIP

(Frankin D. Ohrtman, Jr., copyright 2003), Chapter 4 "Voice over Internet Protocol", at pages 67-86.

116.   The general topic and related issues for VoIP connections LAN-to-LAN, LAN-to-Internet-to-LAN, LAN-to-PSTN, and LAN-to-Internet-to-PSTN is described as "network interconnection."   For IP-to-IP connections, the aforementioned DNS and ENUM services, inter alia, may be used to map domain style names and telephone numbers to IP addresses.   Additionally, Network Address Translation/Traversal (NAT) and other technologies are used for VoIP connections of endpoints connected to private or enterprise LANs to endpoints connected on remote private or enterprise LANs.   See IETF RFC-2663 "IP Network Address Translator (NAT) Terminology and Considerations" (published in August, 1999) and other associated IETF RFCs for more information regarding NAT.   In many cases, the Internet is used as a transport network for such IP-LAN to IP-LAN connections.   Whether or not the Internet is used for part of the transmission of VoIP call signaling and media data, end-to-end VoIP connections may be made from an endpoint connected to one private LAN to another endpoint connected to the same, or another, private LAN.   See Telcordia SR-2275, Issue 4, October 2000, Section 18.2 "Survey of IP Networking", at pages 18-8 to 18-20.

117. Because the PSTN is a mainstay of telecommunications for wireline and wireless communications for residential and business users, the need to provide interconnection of VoIP and PSTN endpoints and networks was well-known starting in the 1990's. The interconnection of IP-based (VoIP) and circuit-switched based (PSTN) telephones requires the use of gateways for both call routing and control signaling data, and for the voice media data. The interconnection of IP and PSTN networks for voice services is described in many published articles, books, standards, and requirements documents. For example, in Telcordia's SR-2275 the following figure is provided:
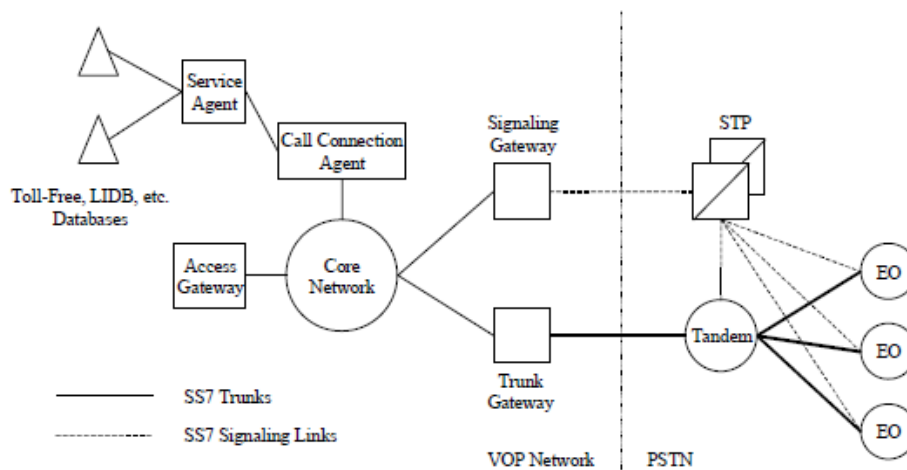
Figure 6-86. CCS Network to VOP Network Interconnection

On the left side of the figure is the VOP (Voice Over Packet) network (e.g., the Internet) and on the right side is the PSTN. Signaling gateways are used to bridge IP session establishment and control protocols (e.g., SIP) with PSTN call set-up

81

and control protocols (e.g., SS7). Trunking gateways are used to convert packet-based voice media (e.g., carried in RTP packets) to and from circuit-switched TDM (PSTN) based voice media. Telcordia SR-2275, Issue 4, October 2000, Section 6.26.3, at pages 6-306 to 6-309. A person of normal skill in the art, starting at least in the late 1990's, would have understood the network architectures, protocols, and standards used for IP to PSTN network interconnections for voice services.

118. Whether using the PSTN (e.g., using SS7), or VoIP (e.g., using SIP), the basic protocol for a call or session is the same: (1) a request to the network from the calling party to establish a connection with the called party; (2) call signaling routing and control; (3) an acknowledgement that the request was received and is being attempted; (4) an alerting signal provided to the called party; (5) a response from the called party accepting the call request; (6) bi-directional audio paths between the calling party and the called party such that a two-way voice conversation may ensue; and (7) a request to end the call when one party decides to end the session. Telcordia SR-2275, Issue 4, October 2000, Section 14.2.3 "CCS Call Setup", at pages 14-10 to 14-13 and Softswitch Architecture for VoIP (Frankin D. Ohrtman, Jr., copyright 2003), Chapter 5 "SIP: Alternative Softswitch Architecture", at pages 89-92.

119. The tasks related to interconnection include routing the signaling for call setup and routing the voice ("media") across the different network types. These tasks involve protocol conversions for call set-up, routing, control, and ending the call (e.g., using a signaling gateway). Transcoding or conversion of the voice media may also be required (e.g., using a media or trunking gateway). See Telcordia SR-2275, Issue 4, October 2000, Section 6.26.3, at pages 6-306 to 6-309. A person of normal skill in the art, starting at least in the late 1990's, would have understood the methods and systems for the tasks related to PSTN and VoIP interconnection.

120. The Internet Engineering Task Force (IETF) has established itself as one of the world's leading organizations for publishing standards documents "RFCs" (Request For Comment) for Internet communications. See IETF website at http://www.ietf.org/ (last visited May 4, 2017). The IETF published RFC 2543 ("SIP: Session Initiation Protocol") in March, 1999, and the IETF updated the SIP standard with the publication of RFC 3261 in June, 2002. SIP and other related IETF established protocols are used for routing, establishing, and controlling VoIP communications sessions over a packet network.

> SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP makes use of elements called proxy servers to help route requests to the user's

> current location, authenticate and authorize users for
> services, implement provider call-routing policies, and
> provide features to users. SIP also provides a registration
> function that allows users to upload their current
> locations for use by proxy servers.

IETF RFC 3261 (SIP), Abstract, at page 1. A person of normal skill in the art,
starting at least in the early 2000's, would have been familiar with RFC 3261 and
understood how SIP was used for VoIP and the general architecture of a SIP based
VoIP network, including SIP servers, used for call (session) control and routing
features as stated in RFC 3261.

121. A typical SIP VoIP network may include terminals or telephones,
Proxy Servers, Redirect Servers, Registrar Servers, and Gateways. The SIP
protocol is described as using "request" and "response" methods such that network
entities which produce request messages include a User Agent Client (UAC)
software component and network entities which receive requests and produce
response messages include a User Agent Server (UAS) software component. Thus,
some network entities (e.g., a SIP telephone) will include both a UAC and UAS
(denoted as "UAC/UAS") to manage producing request messages (UAC), and to
receive request messages and produce response messages (UAS). Refer to IETF
RFC 3261 Section 4 "Overview of Operation", at pages 10-18 and Section 8
"General User Agent Behavior", pages 34-53.

122. A SIP proxy server (sometimes referred to generically as a "SIP server") will receive session establishment requests, resolve address translations, and route the requests to the intended end user agent (UAS). A SIP redirect server performs a similar function as a SIP proxy server except the SIP redirect server receives session establishment requests and sends session routing information back to the calling party UA rather than forwarding the request to the called party. A SIP gateway is treated as any other endpoint (e.g., a terminal) as the SIP-PSTN gateway may be the determined destination of a session establishment request depending on the destination identity (e.g., called telephone number). Refer to IETF RFC 3261 Section 2, "Overview of SIP Functionality", at pages 9-10, Section 4 "Overview of Operation", at pages 10-18, Section 8 "General User Agent Behavior", at pages 34-53, and Section 19 "Common Message Components", at pages 147-159. An example use of a SIP-PSTN gateway was described above in the patent to Kelly and the IETF ENUM standard.

123. In a typical scenario, endpoints (e.g., SIP telephones and terminals) use a SIP REGISTER message, transmitted to a SIP registrar server, to register their IP addresses and any domain style names (e.g., sip:jrbress@telecom-expert.com) associated with the endpoint. The SIP registrar server may store the

endpoint / user information in a locations database. Refer to IETF RFC 3261 Section 10 "Registrations", at pages 56-66.

124. To initiate a call session, an endpoint may transmit a SIP INVITE message to a SIP proxy server. This INVITE message may include a called party identifier such as a domain style name (e.g., sip:jrbress@telecom-expert.com) or a telephone number type identifier (e.g., tel:+1-321-555-0123). If the SIP INVITE message includes an E.164 formatted number, and the SIP proxy server does not resolve the called party identifier to an IP addressable location, then the SIP proxy server may route the SIP INVITE message to a SIP-PSTN gateway for call completion through the PSTN. If the SIP INVITE message is routable over the IP network then the SIP proxy server may route the SIP INVITE message by transmitting it to the intended endpoint, or to another SIP proxy server. Therefore, SIP INVITE messages serve as routing request and call control messages in a VoIP network. An example of this scenario is presented in IETF RFC 3666, Section 2.1, at pages 7-14. A person of normal skill in the art in the early 2000's would have understood the SIP protocol, the components of a SIP-based VoIP network and their use in VoIP networking.

125. The concepts, protocols, and equipment to enable the connection of end-to-end calls or sessions can be viewed generally as tasks to control the call or

session connection (session set-up (establishment), session monitoring, and session

tear-down), and tasks for routing (e.g., determining network addresses) for the

intended connection. The processes to carry out the tasks for session control and

session routing may be implemented in the same physical device, or separate

devices. The concepts of call control and call routing are included in VoIP

networks (e.g., SIP and/or H.323 protocols) and PSTN (circuit-switched) networks.

The details for implementing these tasks is different for the different network

types. See "Telecommunications Essentials", by Lillian Goleniewski, copyright

2002, Chapter 5, "The PSTN" at pages 113-150 and Chapter 11, "Next-Generation

Network Services", at pages 329-368.

126. Consider a simple SIP VoIP network consisting of two endpoints

telephones (extension 101 and 102) and a SIP proxy server and registrar server.

Often the proxy server and registrar server will be implemented in the same

physical device, although they can also be implemented in physically separate

server devices. A SIP UA may use a variety of defined methods for discovering

the IP address of a SIP registrar and SIP proxy server, the details of which will not

be presented here. One simple method is for the IP addresses of the SIP proxy and

registrar servers to be manually configured (provisioned) into the settings of an

endpoint's UA. First, the SIP user agent (UA) software in each telephone will

register its extension number and its associated device's IP address with the
registrar server using a SIP REGISTER message. The registrar server will store
the telephone extension numbers and associated IP addresses in a location service
database. See IETF RFC 3261 Section 4 "Overview of Operation", at pages 10-18.

127. When a user at extension 101 initiates a call to extension 102,
extension 101's UA will determine the IP address of its SIP proxy server and
transmit a SIP INVITE message containing "102" (i.e., the telephone number for
extension 102) as the destination (called) party telephone number. The SIP proxy
server will locate the IP address associated with extension 102 in the registrar
server's locations database and reformat the SIP INVITE message to be
transmitted to extension 102 UA's IP address. The SIP proxy server may format
the new INVITE message to indicate that SIP response messages from extension
102's UA should be routed back through the SIP proxy server. Extension 102's
UA may then transmit a SIP "200 OK" message back to extension 101's UA (via
the SIP proxy server) to indicate acceptance of the session request. At this point
both endpoint 101 and 102 will begin to transmit voice media to each other using
IP addresses for media contained in the SIP INVITE and SIP 200 OK messages.
Voice media data is normally carried using RTP (Real-Time Protocol). This is a
simplified example, and in a real session establishment scenario, additional

signaling messages would be sent and received. See IETF RFC 3261 Section 4

"Overview of Operation", at pages 10-18 and IETF RFC 3665 (2003), Section 3.2,

"Session Establishment Through Two Proxies" at pages 15-25.

128. Extension 101's UA tasks of determining the IP address of the SIP

proxy server, the SIP proxy server accessing the locations database to find the IP

address of extension 102, the SIP proxy server forwarding a SIP INVITE or a SIP

200 OK to a SIP UA, and the SIP proxy server including routing information to

have the SIP proxy server included in the route of SIP messages between extension

101's UA and extension 102's UA, are examples of call or session routing tasks.

Likewise, extension 101's UA transmitting the INVITE message to extension

102's UA (via the SIP proxy server), extension 102's UA transmitting the 200 OK

message to extension 101's UA (via the SIP proxy server), are examples of call or

session control tasks. In general, tasks involving locating or translating network

addresses, and forwarding messages are session routing tasks. Tasks involving

transmission of messages to request session establishment, accept a session

establishment request, or any other tasks associated with controlling the session

(such as negotiating call parameters e.g., which voice codec to use for the call) are

call or session control tasks. Multiple network elements may implement call

routing and call control tasks including different protocol layers performing these

tasks within the same network element (see IP network layer description described

above). A person of normal skill in the art would understand that in the simple SIP

VoIP example provided here, the endpoint (telephone) UA's are primarily involved

with call/session control tasks and the SIP registrar and SIP proxy server are

responsible for call/session routing tasks. See IETF RFC 3261 Abstract, at page 1

and Section 4 "Overview of Operation", at pages 10-18.

129. SIP INVITE and SIP 200 OK response messages may include call

negotiation parameters (such as supported codecs and IP addresses and ports to be

used for call media) which are included in SDP (Session Description Protocol) data

that is embedded within the SIP INVITE and 200 OK messages. These parameters

control the routing of call media as well as the nature of the call media itself (e.g.,

which codec is used to encode the voice data). See IETF RFC 3261 Section 2

Overview of SIP Functionality at pages 9-10.

130. In a more realistic SIP VoIP network implementation there will be

many endpoints and many SIP registrars, SIP proxy servers, and possibly other

types of servers used for session routing and address translation (e.g., a DNS server

or an ENUM server described above). A session setup request message from an

endpoint UA may traverse several servers before reaching the UA of the

destination endpoint. The result is the same however as the endpoint UAs will

eventually receive the call control messages to set-up, control, and end the session

with the call signaling being routed as required through the necessary SIP server

and other entities. See IETF RFC 3261 Section 4 "Overview of Operation", at

pages 10-18.

131. The information in a SIP message is organized in fields divided into a

"message header" and a "message body". The information carried in the SIP

message provides for addressing such that messages will be able to reach their

intended destination (e.g., the called party), session related identifiers used to

control the flow of messages between the calling and called party and within the

network, information for security (e.g. encryption), and information related to

endpoint capabilities and attributes. See IETF RFC 3261 Section 4 "Overview of

Operation", at pages 10-18.

132. RFC 3665 was developed to be a companion document to the RFC

3261 (SIP) standard and describes the call flows presented in RFC 3665 as:

> The call flows shown in this document were developed in
> the design of a SIP IP communications network. They
> represent an example minimum set of functionality.
>
> It is the hope of the authors that this document will be
> useful for SIP implementers, designers, and protocol
> researchers alike and will help further the goal of a
> standard implementation of RFC 3261 [1]. These flows
> represent carefully checked and working group reviewed

> scenarios of the most basic examples as a companion to
> the specifications.
>
> These call flows are based on the current version 2.0 of
> SIP in RFC 3261 [1] with SDP usage described in RFC
> 3264 [2]. Other RFCs also comprise the SIP standard but
> are not used in this set of basic call flows.
>
> Call flow examples of SIP interworking with the PSTN
> through gateways are contained in a companion
> document, RFC 3666 [5].

IETF RFC 3665 (2003), Section 1 "Overview", at pages 2-3. IETF RFC 3665

provides sample call flows and details of the messages included in those call flows.

133. In a typical VoIP network, the User Agent (UA) for each telephone,

terminal, (endpoints in general), will register with a Registrar server which will

normally be interfaced to a SIP proxy server. The registration may include the

user's username and domain which will be used to create an association of the user

and domain names with the IP address (network address) of the endpoint. An

example registration message flow for a user "Bob" is provided in RFC 3665:

```
2.1.  Successful New Registration

   Bob                              SIP Server
    |                                   |
    |            REGISTER F1             |
    |---------------------------------->|
    |         401 Unauthorized F2        |
    |<----------------------------------|
    |            REGISTER F3             |
    |---------------------------------->|
    |             200 OK F4              |
    |<----------------------------------|
    |                                   |
```
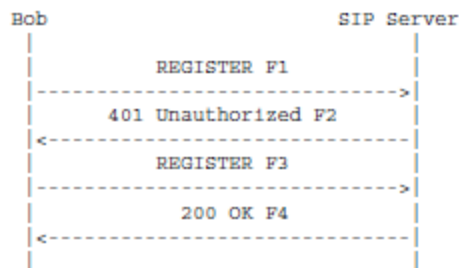
The "401 Unauthorized" F2 message and the subsequent "REGISTER" F3

message is described in RFC 3665 as being an authorization challenge from the

registrar server which requires the user, Bob, to enter a password. With the user

name and password, the SIP registrar server then performs authorization (separate

messaging not shown) with a SIP server, and when authorized, it stores Bob's

contact information in a database and sends the "200 OK" F4 message to Bob's

UA. IETF RFC 3665 (2003), Section 2.1 "Successful New Registration", at page

5.

134. The message details for message F3 (SIP REGISTER) and F4 (200

OK) are provided in RFC 3665 as follows:

```
F3 REGISTER Bob -> SIP Server

REGISTER sips:ss2.biloxi.example.com SIP/2.0
Via: SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashd92
Max-Forwards: 70
From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlflH
To: Bob <sips:bob@biloxi.example.com>
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 2 REGISTER
Contact: <sips:bob@client.biloxi.example.com>
Authorization: Digest username="bob", realm="atlanta.example.com"
 nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="",
 uri="sips:ss2.biloxi.example.com",
 response="dfe56131d1958046689d83306477ecc"
Content-Length: 0


F4 200 OK SIP Server -> Bob

SIP/2.0 200 OK
Via: SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashd92
 ;received=192.0.2.201
From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlflH
To: Bob <sips:bob@biloxi.example.com>;tag=37GkEhwl6
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 2 REGISTER
Contact: <sips:bob@client.biloxi.example.com>;expires=3600
Content-Length: 0
```

IETF RFC 3665 (2003), Section 2.1 "Successful New Registration", at pages 5-6.

135.   In the following call flow examples using Bob and Alice, it can be assumed that Alice's telephone UA would perform a similar SIP registration with the registrar server and SIP proxy server in the VoIP network serving Alice. In the F3 REGISTER message a username is included ("bob") which along with the password related fields, allows Bob's UA to be authorized by the SIP server which manages user accounts. The URI style addresses would normally be translated into IP addresses by DNS or ENUM lookup to be used by the IP layer for packet routing.

136.   In the F4 200 OK message in the registration example supra, the "expires=3600" parameter in the "Contact;" field is an indication to Bob's UA that the registration of the contact sips:bob@client.biloxi.example.com is only valid for 3600 seconds (1 hour). The "expire" feature is similar to the DNS feature which uses a "Time to Live" (TTL) field to convey how long a DNS record may be cached as described above. See IETF RFC 3261 Section 8.3 "Redirect Servers", at pages 51-53.

137.   An example call flow provided in RFC 3665 is as follows:

```
3.3.  Session with Multiple Proxy Authentication

    Alice          Proxy 1      Proxy 2          Bob
    |               |            |               |
    |  INVITE F1    |            |               |
    |-------------->|            |               |
    |  407 Proxy Authorization Required F2       |
    |<--------------|            |               |
    |  ACK F3       |            |               |
    |-------------->|            |               |
    |  INVITE F4    |            |               |
    |-------------->|            |               |
    |  100 F5       |            |               |
    |<--------------|  INVITE F6 |               |
    |               |----------->|               |
    |               |  407 Proxy Authorization Required F7
    |               |<-----------|               |
    |               |  ACK F8    |               |
    |               |----------->|               |
    |  407 Proxy Authorization Required F9        |
    |<--------------|            |               |
    |  ACK F10      |            |               |
    |-------------->|            |               |
    |  INVITE F11   |            |               |
    |-------------->|            |               |
    |  100 F12      |            |               |
    |<--------------|  INVITE F13|               |
    |               |----------->|               |
    |               |  100 F14   |               |
    |               |<-----------|  INVITE F15   |
    |               |            |-------------->|
    |               |            |  200 OK F16   |
    |               |  200 OK F17|<--------------|
    |  200 OK F18   |<-----------|               |
    |<--------------|            |               |
    |  ACK F19      |            |               |
    |-------------->|  ACK F20   |               |
    |               |----------->|  ACK F21      |
    |               |            |-------------->|
    |               RTP Media Path               |
    |<==========================================>|
```
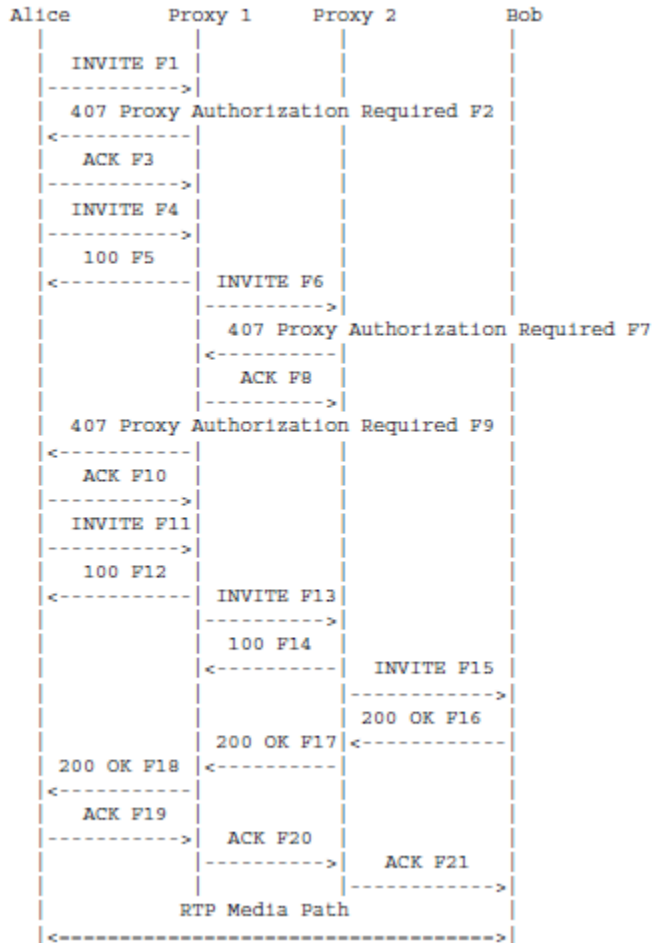
This call flow is described in RFC 3665 as:

> In this scenario, Alice completes a call to Bob using two proxies Proxy 1 and Proxy 2. Alice has valid credentials in both domains. Since the initial INVITE (F1) does not contain the Authorization credentials Proxy 1 requires, so a 407 Proxy Authorization response is sent containing the challenge information. A new INVITE (F4) is then sent containing the correct credentials and the call proceeds after Proxy 2 challenges and receives valid credentials. The call terminates when Bob disconnects by initiating a BYE message.

> Proxy 1 inserts a Record-Route header into the INVITE
> message to ensure that it is present in all subsequent
> message exchanges. Proxy 2 also inserts itself into the
> Record-Route header.

IETF RFC 3665 (2003), Section 3.3 "Session with Multiple Proxy Authentication",

at pages 26-36. Also included in RFC 3665 in section 3.3 are the details for each

of the SIP messages that are represented in the call flow diagram copied supra

(messages F1, F2, F3…F21). The following paragraphs include a copy of some of

the SIP messages in that call flow.

138. The initial SIP INVITE message (F1) to initiate the call is depicted as

follows.

```
F1 INVITE Alice -> Proxy 1

INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/UDP client.atlanta.example.com:5060;branch=z9hG4bK74b03
Max-Forwards: 70
Route: <sip:ss1.atlanta.example.com;lr>
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:alice@client.atlanta.example.com>
Content-Type: application/sdp
Content-Length: 151

v=0
o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

IETF RFC 3665 (2003), Section 3.3 "Session with Multiple Proxy Authentication",

at pages 12-13. SIP URIs are used for the called party (callee) identifier ("To: Bob

sip:bob@biloxi.example.com") and the calling party (caller) identifier ("From:

Alice <sip:alice@atlanta.example.com"). For IP layer routing, these domain style

URI identifiers will be translated to IP addresses as the message traverses from

Alice's UA to Bob's UA. The "From:" field is described as:

> 20.20 From
>
> The From header field indicates the initiator of the
> request. This may be different from the initiator of the
> dialog. Requests sent by the callee to the caller use the
> callee's address in the From header field.
>
> The optional "display-name" is meant to be rendered by a
> human user interface.

IETF RFC 3261 (SIP) (2002), Section 20.20, at page 172. The "To:" field is

described as:

> 20.39 To
>
> The To header field specifies the logical recipient of the
> request.
>
> The optional "display-name" is meant to be rendered by a
> human-user interface.

RFC 3261 (SIP) (2002), Section 20.39, at pages 178-179. In this example, the

From: and To: fields in the SIP INVITE message use SIP URI identifiers. SIP

URIs include a user name (e.g., "alice") and a host or domain name (e.g.,

"atlanta.example.com"). Thus the endpoint's UAs associated with "Alice" and

"Bob", and the SIP proxy servers, will produce network routing messages after the

call is initiated (i.e., the SIP INVITE message and ensuing call related messages)

using the underlying IP layer (IP addresses) as described above. Refer to IETF

RFC 3261 Section 4 "Overview of Operation", at pages 10-18.

139. Another field in the RFC 3665 example F1 INVITE message is the

"Via:" field. The F6 message that is sent from Proxy 1 (Alice's SIP proxy server)

to Proxy 2 (Bob's SIP proxy server) highlights the use of the Via: field:

```
F6 INVITE Proxy 1 -> Proxy 2

INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/UDP ss1.atlanta.example.com:5060;branch=z9hG4bK230f2.1
Via: SIP/2.0/UDP client.atlanta.example.com:5060;branch=z9hG4bK74b21
 ;received=192.0.2.101
Max-Forwards: 69
Record-Route: <sip:ss1.atlanta.example.com;lr>
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
CSeq: 2 INVITE
Contact: <sip:alice@client.atlanta.example.com>
Content-Type: application/sdp
Content-Length: 151

v=0
o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

IETF RFC 3665 (2003), Section 3.3 "Session with Multiple Proxy Authentication",

at page 29. In the F1 INVITE message for this call flow the Via: field contains an

address identifier associated with the UA of Alice's telephone

"client.atlanta.example.com". In the F6 INVITE message which is Alice's

INVITE message forwarded from Proxy 1 to Proxy 2 an additional Via: field was

added by Proxy 1 containing an address identifier associated with Proxy 1

"ss1.atlanta.example.com."   RFC 3261 (SIP) describes the use of the "Via:"

parameters for UACs (User Agent Client) as:

> 8.1.1.7 Via
>
> The Via header field indicates the transport used for the
> transaction and identifies the location where the response
> is to be sent. A Via header field value is added only after
> the transport that will be used to reach the next hop has
> been selected (which may involve the usage of the
> procedures in [4]). When the UAC creates a request, it
> MUST insert a Via into that request.
>
> …
>
> Via processing for proxies is described in Section 16.6
> Item 8 and Section 16.7 Item 3.

IETF RFC 3261 (SIP) (2002), section 8.1.1.7, pages 39-40. Proxy servers will add

a "Via:" field in a forwarded INVITE message so the SIP proxy server will be

included in the signaling path for session set-up response messages made to

Alice's SIP INVITE request message. SIP endpoints (e.g., telephones) and SIP

proxy servers perform functions for call routing and for call control.

140.   A person of ordinary skill in the art would understand that SDP is an

integral part of a SIP initiated session establishment which is made clear in RFC

3261 by:

> "The Session Description Protocol (SDP) (RFC 2327 [1])
> MUST be supported by all user agents as a means to
> describe sessions, and its usage for constructing offers

and answers MUST follow the procedures defined in
[13].”

IETF RFC 3261, Section 13.2.1 "Creating the Initial INVITE", at page 80.

Reference [13] in RFC 3261 is: "[13] Rosenberg, J. and H. Schulzrinne, "An

Offer/Answer Model with SDP", RFC 3264, June 2002." RFC 3261, at p. 261. A

person of normal skill in the art, starting at least in the 1990's, would understand

the use of the SDP offer/answer model used with SIP and VoIP to establish the

parameters of an end-to-end connection between endpoints.

141. The last part of the F1 INVITE message transmitted from Alice to

Proxy 1 is as follows:

```
v=0
o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

This is known as the SDP data "media line" or "media block" and is the data which

is carried in the F1 SIP INVITE message. The SDP data provides the offered

parameters for the call session requested by the SIP INVITE message. IETF RFC

3261 (SIP) (2002), Section 2 "Overview of SIP Functionality", at pages 9-10.

142. In the preceding SDP example, there are several fields with associated

parameter data. The fields most relevant to the present matter are the "o=" and

"c=" fields. RFC 2327 describes the "o=" field of the SDP protocol as "Origin"

with a format description in RFC 2327:

> Origin
>
> o=<username> <session id> <version> <network type>
> <address type> <address>
>
> The "o=" field gives the originator of the session (their
> username and the address of the user's host) plus a
> session id and session version number.
>
> <username> is the user's login on the originating host, or
> it is "-" if the originating host does not support the
> concept of user ids. <username> must not contain
> spaces. <session id> is a numeric string such that the
> tuple of <username>, <session id>, <network type>,
> <address type> and <address> form a globally unique
> identifier for the session.
>
> …

IETF RFC 2327, Section 6 "SDP Specification", at page 9. A person of normal

skill in the art would understand the use of usernames in SIP header fields, and

likewise the SDP data carried in the SIP message also using usernames to identify

the user associated with the session.

143. RFC 2327 describes the "c=" field of the SDP protocol as

"Connection Data" as follows:

> Connection Data
>
> c=<network type> <address type> <connection address>

The "c=" field contains connection data.

A session announcement must contain one "c=" field in each media description (see below) or a "c=" field at the session-level. It may contain a session-level "c=" field and one additional "c=" field per media description, in which case the per-media values override the session-level settings for the relevant media.

The first sub-field is the network type, which is a text string giving the type of network. Initially "IN" is defined to have the meaning "Internet".

The second sub-field is the address type. This allows SDP to be used for sessions that are not IP based. Currently only IP4 is defined.

The third sub-field is the connection address. Optional extra subfields may be added after the connection address depending on the value of the <address type> field.

For IP4 addresses, the connection address is defined as follows:

Typically the connection address will be a class-D IP multicast group address. If the session is not multicast, then the connection address contains the fully-qualified domain name or the unicast IP address of the expected data source or data relay or data sink as determined by additional attribute fields.

Conferences using an IP multicast connection address must also have a time to live (TTL) value present in addition to the multicast address. The TTL and the address together define the scope with which multicast packets sent in this conference will be sent. TTL values must be in the range 0-255.

The TTL for the session is appended to the address using a slash as a separator. An example is:

> c=IN IP4 224.2.1.1/127
>
> …

IETF RFC 2327, Section 6 "SDP Specification", at pages 12-13. Other fields in the SDP data are used to, inter alia, control the session parameters such as the codec used for voice. A person of normal skill in the art would understand that in SDP, the "connection-address" is the IP address for where media will be sent to or received from for the session and therefore SIP endpoint UAs, in addition to providing call control and call routing functions via the identifiers included in the SIP header, also provide call control and call routing functions via the information included in the SIP message's SDP data.

144.   As one of ordinary skill in the art, starting at least in the late 1990's, would understand that the messages transmitted to set-up the connection (commonly described as call set-up signaling) will generally follow a different network routing path than that used by the messages (or packets) used to convey the actual media (i.e., coded digital voice/audio) that will flow between the two endpoints of the call. Thus, SIP is used to (1) signal from a calling party endpoint, to a called party endpoint, a request to establish a voice session (call), (2) signal call progress and alerting, and (3) signal responses from the called party regarding the acceptance (or rejection) of the request to establish a session. A successful VoIP session establishment may be characterized by the bi-directional flow of

voice packets between the calling and called parties with the voice packets routed

through the network as required to connect from endpoint to endpoint. The voice

packets (media) for a session may be carried using the Real-Time Protocol (RTP).

RTP packets include the coded digital voice bits and also addressing information,

as well as other information used to control the flow of the RTP messages (media

packets). IETF RFC 3261 (SIP) (2002), Section 2 "Overview of SIP

Functionality", at pages 9-10, Section 4 "Overview of Operation" at pages 10-18,

Section 8 "General User Agent Behavior", at pages 34-53, and Section 13

"Initiating a Session", at pages 77-86.

145. RFC 3261 (SIP) includes information for the use of PSTN gateways

to allow IP endpoints to access and connect calls over the PSTN. For example:

> Gateway Control Protocol (MEGACO) (RFC 3015 [30])
> for controlling gateways to the Public Switched
> Telephone Network (PSTN), and the Session Description
> Protocol (SDP) (RFC 2327 [1]) for describing
> multimedia sessions.

IETF RFC 3261 (SIP) (2002), Section 2, at page 10. Additionally, regarding SIP

redirect servers:

> Note that a Contact header field value MAY also refer to
> a different resource than the one originally called. For
> example, a SIP call connected to PSTN gateway may
> need to deliver a special informational announcement
> such as "The number you have dialed has been changed."

IETF RFC 3261 (SIP) (2002), Section 8.3, at page 52. The SIP standard includes

information regarding addressing to identify PSTN gateways, for example:

> 19.1 SIP and SIPS Uniform Resource Indicators
>
> A SIP or SIPS URI identifies a communications resource. Like all URIs, SIP and SIPS URIs may be placed in web pages, email messages, or printed literature. They contain sufficient information to initiate and maintain a communication session with the resource. Examples of communications resources include the following:
> …
>   a PSTN number at a gateway service
> …

IETF RFC 3261 (SIP) (2002), Section 19.1, at page 148. The SIP standard also

includes examples of identifiers used to access a gateway including:

> 19.1.3   Example   SIP   and   SIPS   URIs
> …
>   sip:+1-212-555-1212:1234@gateway.com;user=phone
>   sips:1212@gateway.com
> …

IETF RFC 3261 (SIP) (2002), Section 19.1.3, at page 153.

146. RFC 3666 provides examples of VoIP and PSTN interworking:

> Abstract
>
> This document contains best current practice examples of Session Initiation Protocol (SIP) call flows showing interworking with the Public Switched Telephone Network (PSTN). Elements in these call flows include

> SIP User Agents, SIP Proxy Servers, and PSTN Gateways.

IETF RFC 3666 "Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows", Abstract, at page 1.

147. RFC 3666 introduces a SIP to PSTN scenario as:

> 2. SIP to PSTN Dialing
>
> In the following scenarios, Alice (sip:alice@a.example.com) is a SIP phone or other SIP-enabled device. Bob is reachable via the PSTN at global telephone number +19725552222. Alice places a call to Bob through a Proxy Server, Proxy 1, and a Network Gateway.
>
> …
>
> Alice uses his/her global telephone number +1-314-555-1111 in the From header in the INVITE messages. This then gives the Gateway the option of using this header to populate the calling party identification field in subsequent signaling.
>
> …
>
> In these scenarios, Alice is a SIP phone or other SIP-enabled device. Alice places a call to Bob in the PSTN…

IETF RFC 3666, Section 2 "SIP to PSTN Dialing", at page 6.

148. RFC 3666 provides a sample call flow for a SIP to PSTN call which uses a SIP-PSTN gateway (NGW1):

```
2.1.  Successful SIP to ISUP PSTN call

   Alice              Proxy 1            NGW 1             Switch B
     |                   |                 |                   |
     |   INVITE F1       |                 |                   |
     |----------------->|                 |                   |
     |   100  F2         |                 |                   |
     |<-----------------|    INVITE F3     |                   |
     |                   |---------------->|                   |
     |                   |    100  F4       |                   |
     |                   |<----------------|    IAM F5         |
     |                   |                 |----------------->|
     |                   |                 |    ACM F6         |
     |                   |    183 F7        |<-----------------|
     |   183 F8          |<----------------|                   |
     |<-----------------|                 |                   |
     |       Both Way RTP Media           |  One Way Voice    |
     |<=================================>|<===============|
     |                   |                 |    ANM F9         |
     |                   |    200 F10       |<-----------------|
     |   200 F11         |<----------------|                   |
     |<-----------------|                 |                   |
     |   ACK F12         |                 |                   |
     |----------------->|    ACK F13       |                   |
     |                   |---------------->|                   |
     |       Both Way RTP Media           |  Both Way Voice   |
     |<=================================>|<===============>|
     |   BYE F14         |                 |                   |
     |----------------->|    BYE F15       |                   |
     |                   |---------------->|                   |
     |                   |    200 F16       |                   |
     |   200 F17         |<----------------|    REL F18        |
     |<-----------------|                 |----------------->|
     |                   |                 |    RLC F19        |
     |                   |                 |<-----------------|
     |                   |                 |                   |
```
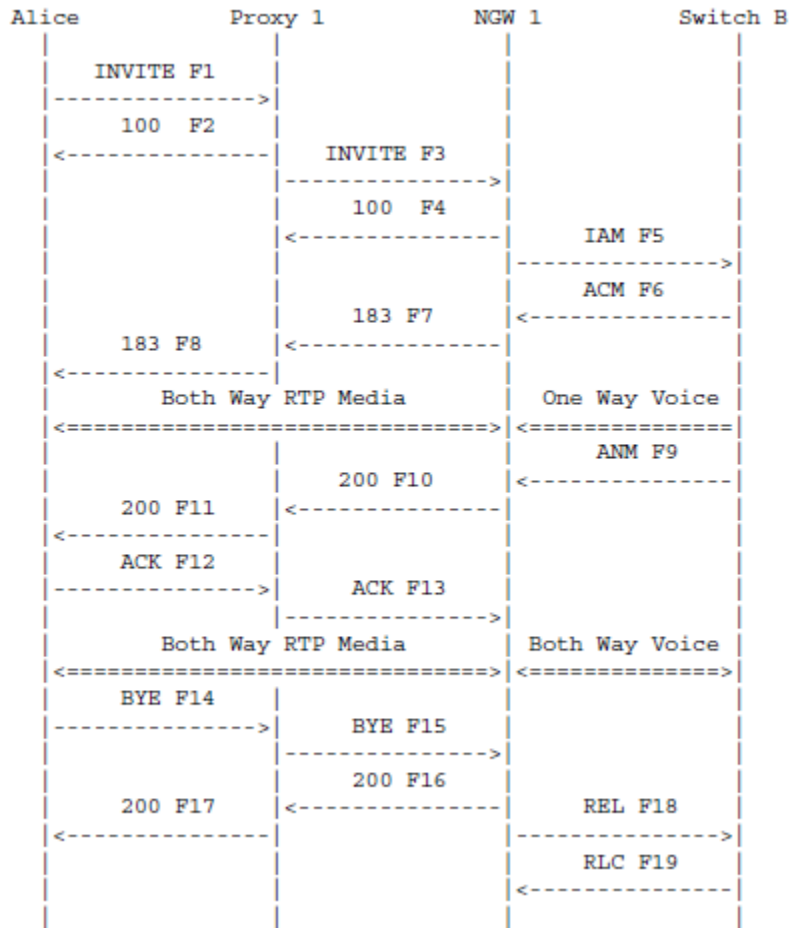
149. The call flow is described in RFC 3666 as:

Alice dials the globalized E.164 number +19725552222 to reach Bob. Note that A might have only dialed the last 7 digits, or some other dialing plan. It is assumed that the SIP User Agent Client converts the digits into a global number and puts them into a SIP URI. Note that tel URIs could be used instead of SIP URIs.

Alice could use either their SIP address (sip:alice@a.example.com) or SIP telephone number (sip:+13145551111@ss1.a.example.com;user=phone) in the From header. In this example, the telephone number is included, and it is shown as being passed as calling

107

party identification through the Network Gateway (NGW
1) to Bob (F5).

IETF RFC 3666, Section 2.1 "Successful SIP to ISUP PSTN call", at page 7.

150. The initial SIP INVITE message (F1) transmitted by Alice's UA to
initiate the call is presented in RFC 3666 as follows:

```
F1 INVITE Alice -> Proxy 1

INVITE sip:+19725552222@ss1.a.example.com;user=phone SIP/2.0
Via: SIP/2.0/TCP client.a.example.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:+13145551111@ss1.a.example.com;user=phone>
 ;tag=9fxced76sl
To: Bob <sip:+19725552222@ss1.a.example.com;user=phone>
Call-ID: 2xTb9vxSit55XU7p8@a.example.com
CSeq: 1 INVITE
Contact: <sip:alice@client.a.example.com;transport=tcp>
Proxy-Authorization: Digest username="alice", realm="a.example.com",
 nonce="dc3a5ab25302aa931904ba7d88falcf5", opaque="",
 uri="sip:+19725552222@ss1.a.example.com;user=phone",
 response="ccdca50cb091d587421457305d097458c"
Content-Type: application/sdp
Content-Length: 154

v=0
o=alice 2890844526 2890844526 IN IP4 client.a.example.com
s=-
c=IN IP4 client.a.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

IETF RFC 3666, Section 2.1 "Successful SIP to ISUP PSTN call", at page 8. This

SIP INVITE message is similar to the SIP INVITE message discussed supra for an

IP-to-IP call.

151. The forwarded SIP INVITE (F3) message transmitted from Alice's

SIP proxy server (Proxy 1) to the SIP-PSTN gateway (NGW 1) is presented in

RFC 3666 as follows:

```
F3 INVITE Proxy 1 -> NGW 1

INVITE sip:+19725552222@ngw1.a.example.com;user=phone SIP/2.0
Via: SIP/2.0/TCP ss1.a.example.com:5060;branch=z9hG4bK2d4790.1
Via: SIP/2.0/TCP client.a.example.com:5060;branch=z9hG4bK74bf9
 ;received=192.0.2.101
Max-Forwards: 69
Record-Route: <sip:ss1.a.example.com;lr>
From: Alice <sip:+13145551111@ss1.a.example.com;user=phone>
 ;tag=9fxced76sl
To: Bob <sip:+19725552222@ss1.a.example.com;user=phone>
Call-ID: 2xTb9vxSit55XU7p8@a.example.com
CSeq: 1 INVITE
Contact: <sip:alice@client.a.example.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 154

v=0
o=alice 2890844526 2890844526 IN IP4 client.a.example.com
s=-
c=IN IP4 client.a.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

IETF RFC 3666, Section 2.1 "Successful SIP to ISUP PSTN call", at page 9. Most

of the fields in the SIP INVITE message forwarded by the SIP proxy server to the

PSTN gateway are the same as the SIP INVITE message the SIP proxy server

received from Alice's UA, as expected.   However, the SIP proxy server has

performed call routing by determining that Alice's call request to Bob is required

to be routed to a PSTN gateway. This is made evident in the first line of the SIP

INVITE messages whereby the SIP proxy server changed the called party identifier

from   what   was   received   from   Alice's   UA,

"sip:+19725552222@ss1.a.example.com", to the address identifier associated with

the PSTN gateway, "sip:+19725552222@ngw1.a.example.com." A person of

normal skill in the art, starting at least in the late 1990's, would understand the

operation of a SIP proxy server to route session (call) establishment requests to

either an IP-based endpoint, or a SIP-PSTN gateway, based on the telephone

number provided in a SIP INVITE message.

152. The ITU is well-known to those skilled in the art of

telecommunications for the development and publication of standards which define

the protocols used for both the PSTN and VoIP networks. The H.323 standard was

first published by the ITU in 1996 originally to support video conferencing over a

Local Area Network (LAN). The H.323 standard has been revised and republished

several times since 1996 including the first revision in 1998 when the H.323 title

was changed to "Packet-based multimedia communications systems" to reflect the

more general nature of H.323 to support the communication of voice, video, and

other media types over packet-based networks. In addition to H.323, the ITU has

developed and published many other related standards that support the

interconnection and interoperability of multiple network components to enable

packet network based communications. The H.323 standard describes the details

for interworking between H.323 network entities and the PSTN in addition to

many other details for understanding how to implement the entities of an H.323

network. See ITU-T Recommendation H.323, "Summary", at page i and

"Foreword" at page ii.

153. The H.323 standard defines networked entities that create the basic

architecture of an H.323 network including "Terminals", "Gateways", and

"Gatekeepers." ITU H.323 (07/2003) Section 6 "System description", at page 14.

Following is the H.323 network reference architecture provided in the H.323

standard.
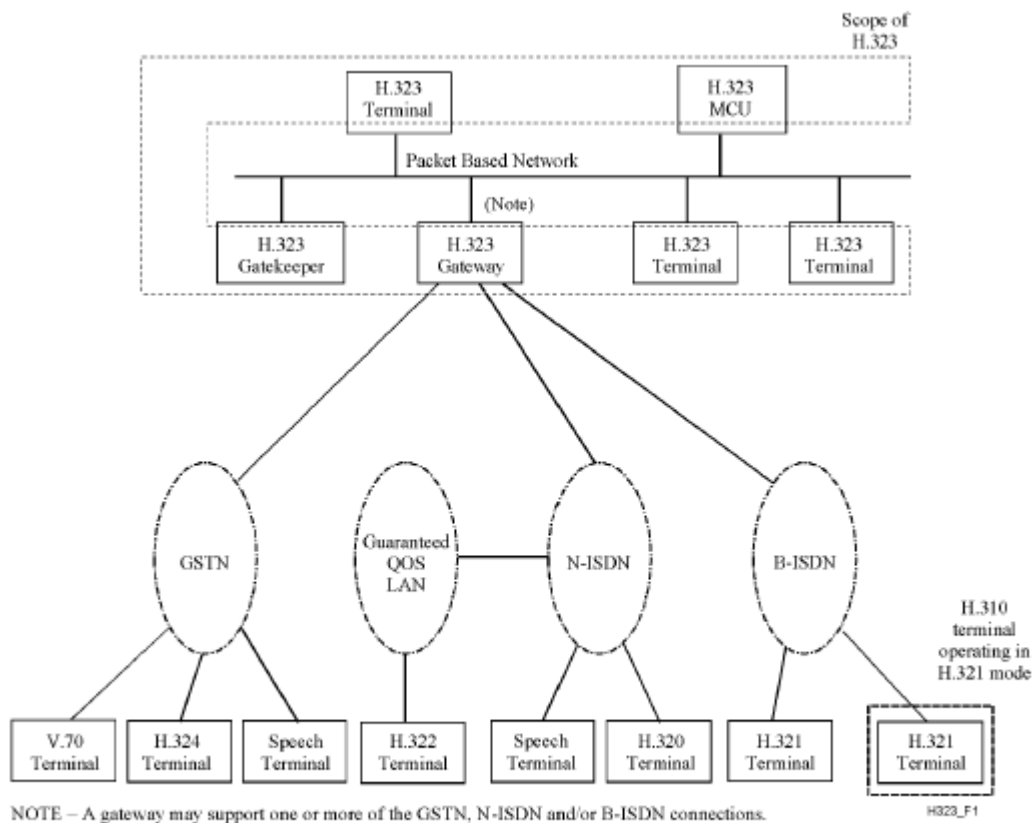
Figure 1/H.323 – Interoperability of H.323 terminals

ITU H.323, Section 1 "Scope", at page 2.

154.   The H.323 standard includes the following definitions:

> 3.18 gatekeeper: The Gatekeeper (GK) is an H.323 entity on the network that provides address translation and controls access to the network for H.323 terminals, Gateways and MCUs. The Gatekeeper may also provide other services to the terminals, Gateways and MCUs such as bandwidth management and locating Gateways.
>
> 3.19 gateway: An H.323 Gateway (GW) is an endpoint on the network which provides for real-time, two-way communications between H.323 Terminals on the packet based network and other ITU Terminals on a switched circuit network or to another H.323 Gateway. Other ITU Terminals include those complying with ITU-T Rec. H.310 (H.320 on B-ISDN), H.320 (ISDN), H.321
>
> 3.46 terminal: An H.323 Terminal is an endpoint on the network which provides for real-time, two-way communications with another H.323 terminal, Gateway, or Multipoint Control Unit. This communication consists of control, indications, audio, moving colour video pictures, and/or data between the two terminals. A terminal may provide speech only, speech and data, speech and video, or speech, data and video.
>
> 3.55 zone: A Zone (see Figure 3) is the collection of all terminals (Tx), Gateways (GW) and Multipoint Control Units (MCUs) managed by a single Gatekeeper (GK). A Zone has one and only one Gatekeeper. A Zone may be independent of network topology and may be comprised of multiple network segments which are connected using routers (R) or other devices.

ITU H.323, Section 3 "Definitions", at pages 6-10. More detailed information for

these network elements is provided in section 6 of the H.323 standard.

155. In a typical H.323 VoIP scenario the network is delineated by "zones" and only one Gatekeeper is allowed per zone. Thus, the Gatekeeper controls access to the H.323 network. ITU H.323, Section 3.55 "zone", at page 10 and Section 6.4 "Gatekeeper characteristics", at pages 43-44.

156. Following is a high-level summary of typical tasks to establish a call in an H.323 network. (1) terminals, a gatekeeper, and optionally, a PSTN gateway are connected to a LAN; (2) The terminals and the gateway use discovery protocols to find the gatekeeper; (3) The terminals and gateways register their IP address and any alias addresses (such as an email address type identifier) with the gatekeeper; (4) A calling party terminal transmits a call request, including a called party identifier and a calling party identifier, to the gatekeeper which may control the call routing, including any address translations required; (5) the call request is transmitted by the gatekeeper to the called party terminal; (6) Multiple call control messages will be transmitted between the calling party terminal, the gatekeeper, and the called party terminal; (7) A call is established between two terminals. Note, the called party terminal could instead be a PSTN gateway if the called party identifier was not resolved by the gatekeeper as an IP network accessible address. A person of normal skill in the art, at least by the late 1990's, would have

understood the H.323 protocol and its use in VoIP networking. ITU H.323,

Section 8 "Call signalling procedures", at pages 78-124.

157. H.323 depicts a sample flow of messages for a call set-up scenario

with two endpoints, each with their own separate gatekeeper:
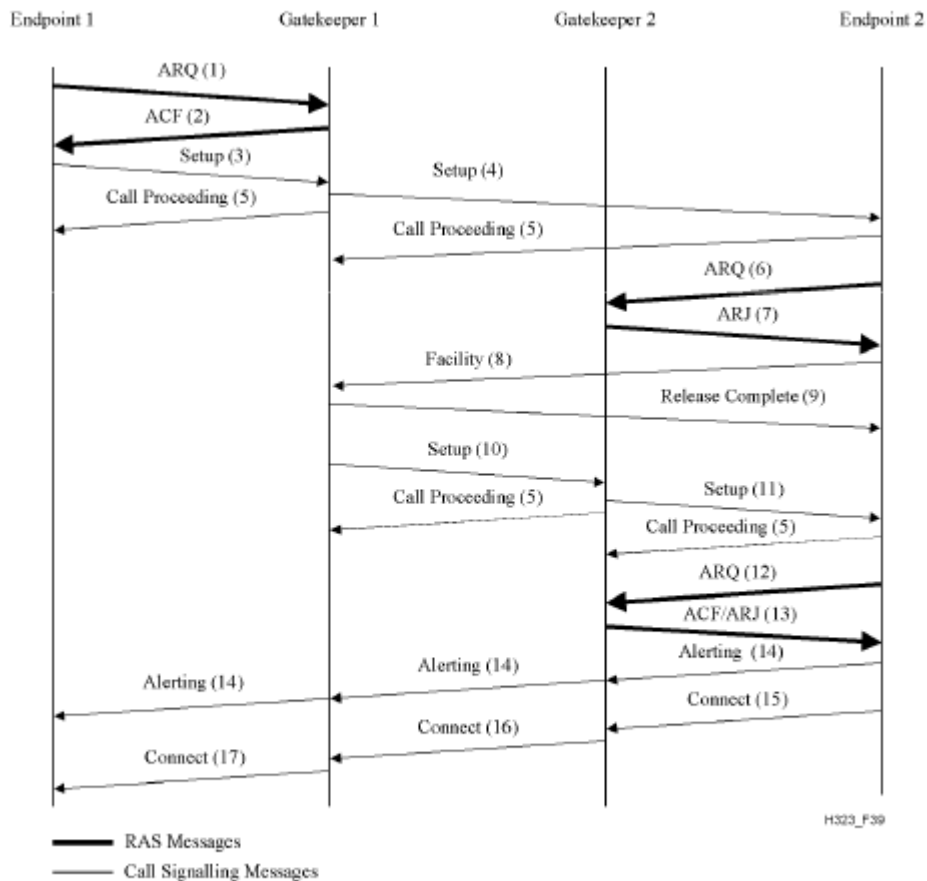
Figure 39/H.323 – Both endpoints registered – Both Gatekeepers routing call signalling

Assume there are two endpoint telephones, extension 101 and 102, and a separate

H.323 gatekeeper for each endpoint. In this example, the gatekeeper is configured

to route call control messages through the gatekeeper (the "gatekeeper-routed call

114

model") rather than routing call messages endpoint to endpoint (the "direct call model"). The telephones will each register with the gatekeeper creating an association of each telephone's extension number (101 or 102) with the IP address assigned to each telephone. These extension numbers (101 and 102) would be an "alias" in the H.323 parlance. When a user at extension 101 initiates a call to extension 102, extension 101 will determine the IP address of its gatekeeper and transmit an H.225 ARQ (Admission Request) message containing "102" (i.e., the telephone number for extension 102 as the destination (called) party address. As seen in H.323 Figure 39 (supra) standard H.323 signaling ensues between the endpoints and the gatekeepers. In the scenario depicted, the gatekeeper includes its own IP address as the address to send responses to in accordance with the aforementioned "gatekeeper-routed call model." When a person at endpoint 2 answers the call (e.g., picks up the handset), endpoint 2 will transmit a "Connect" message to its gatekeeper, which forwards the Connect message to endpoint 1's gatekeeper, which forwards the Connect message to endpoint 1, and the call set-up is completed. The Connect messages will include H.245 Control Channel Transport Address information to enable negotiation of call parameters. ITU H.323, Section 8.1.5 "Both endpoints registered to different gatekeepers", at pages 86-87.

158.   H.323 uses the call signaling formats specified in ITU H.225/0 which

specifies using the ITU Q.931 format:

> 7.3 Call signalling channel
>
> The Call Signalling Channel shall be used to carry
> H.225.0 call control messages.
>
> …
>
> ITU-T Rec. H.225.0 specifies the mandatory Q.931
> messages that are used for call signalling in this
> Recommendation. Clause 8 specifies the procedures for
> using them.

ITU H.323, Section 7.3 "Call signalling channel", at pages 63-64. The Q.931 call

setup message is as follows:

3.3.9 SETUP

This message is sent by the calling user to the network and by the network to the called user to initiate call establishment. See Table 3-43.

Table 3-43/Q.931 – SETUP message content

Message type: SETUP
Significance: Global
Direction: Both

Information element	Reference (subclause)	Direction	Type	Length
Protocol discriminator	4.2	Both	M	1
Call reference	4.3	Both	M	2-*
Message type	4.4	Both	M	1
Sending complete	4.5	Both	O (Note 1)	1
Bearer capability	4.5	Both	M (Note 2)	6-8
Channel identification	4.5	Both	M	3-*
Network-specific facility	4.5	Both	O (Note 3)	2-*
Display	4.5	n → u	O (Note 4)	(Note 5)
Keypad facility	4.5	u → n	O (Note 6)	2-34
Calling party number	4.5	Both	O (Note 7)	2-*
Calling party subaddress	4.5	Both	O (Note 8)	2-23
Called party number	4.5	Both	O (Note 9)	2-*
Called party subaddress	4.5	Both	O (Note 10)	2-23

Table 3-43/Q.931 – SETUP message content *(concluded)*

Message type: SETUP
Significance: Global
Direction: Both

Information element	Reference (subclause)	Direction	Type	Length
Transit network selection	4.5	u → n	O (Note 11)	2-*
Low layer compatibility	4.5	Both	O (Note 12)	2-18
High layer compatibility	4.5	Both	O (Note 13)	2-5

The notes associated with the Calling party and Called party fields are provided in

ITU Q.931 as follows:

NOTE 7 – May be included by the calling user or the network to identify the calling user.

NOTE 8 – Included in the user-to-network direction when the calling user wants to indicate the calling party subaddress. Included in the network-to-user direction if the calling user included a Calling party subaddress information element in the SETUP message.

NOTE 9 – Either the Called party number or the Keypad facility information element is included by the user to convey called party number information to the network during overlap sending. The Called party number information element is included by the network when called party number information is conveyed to the user.

NOTE 10 – Included in the user-to-network direction when the calling user wants to indicate the called party subaddress. Included in the network-to-user direction if the calling user included a Called party subaddress information element in the SETUP message.

ITU-T Q.931 (05/98) "ISDN user-network interface layer 3 specification for basic call control", at pages 41-42. The "Calling party number" and "Calling party number" fields in the Q.931 setup message identify the calling and called parties for the call. The endpoints and the gatekeepers will produce network routing messages after the call is initiated (i.e., the call setup message and ensuing call related messages) using the underlying IP layer (IP addresses) as described above.

159. After a Connect message is transmitted and received, generally the H.245 protocol is used between the endpoints (with messages routed via the gatekeeper) to negotiate parameters for the call (such as audio and/or video codecs). A number of different methods have been developed to enable call parameter negotiation with at least one of the goals being to minimize the delays between the call being answered (signaled from the called party extension with the "Connect" message) and when the actual voice media is transmitted between the endpoints. Endpoints exercise control of the call by negotiating the parameters and

the gatekeeper (and/or the endpoints) are responsible for routing the associated call

control signaling to the endpoints. Included in the negotiated call parameters is the

IP addresses and ports that the endpoints signal to the each other instructing the

other endpoint where it should send the call media (e.g., voice data) when the call

is established. In this manner, the endpoints are performing call signaling control

and call media routing tasks. ITU H.323, Section 8 "Call signalling procedures" at

pages 78-124.

160. The H.323 standard describes the use of gateways for completing calls

to the PSTN (SCN).

> 3.8 call: Point-to-point multimedia communication
> between two H.323 endpoints. The call begins with the
> call set-up procedure and ends with the call termination
> procedure. The call consists of the collection of reliable
> and unreliable channels between the endpoints. A call
> may be directly between two endpoints or may include
> other H.323 entities such as a Gatekeeper or MC. In case
> of interworking with some SCN endpoints via a
> Gateway, all the channels terminate at the Gateway
> where they are converted to the appropriate
> representation for the SCN end system.

ITU H.323 (2003), Section 3.8, at pages 5-6. Additionally, a gateway is defined in

H.323 as:

> 3.19 gateway: An H.323 Gateway (GW) is an endpoint
> on the network which provides for real-time, two-way
> communications between H.323 Terminals on the packet

> based network and other ITU Terminals on a switched circuit network or to another H.323 Gateway. Other ITU Terminals include those complying with ITU-T Rec. H.310 (H.320 on B-ISDN), H.320 (ISDN), H.321 (ATM), H.322 (GQOS-LAN), H.324 (GSTN), H.324M (Mobile), and V.70 (DSVD).

ITU H.323 (2003), Section 3.19 "gateway", at page 6. The H.323 standard

describes a gateway's characteristics as follows:

> 6.3   Gateway   characteristics
> The Gateway shall provide the appropriate translation between transmission formats (for example H.225.0 to/from H.221) and between communications procedures (for example H.245 to/from H.242). This translation is specified in ITU-T Rec. H.246. The Gateway shall also perform call setup and clearing on both the network side and the SCN side. Translation between video, audio, and data formats may also be performed in the Gateway. In general, the purpose of the Gateway (when not operating as an MCU) is to reflect the characteristics of a network endpoint to an SCN endpoint, and the reverse, in a transparent fashion.

ITU H.323 (2003), Section 6.3 "Gateway characteristics", at page 28. The H.323

standard therefore describes a use of an H.323 gateway is to provide access to the

PSTN (SCN). The H.323 standard may use the terms "GSTN" (General Switched

Telephone Network) and "SCN" (Switched-Circuit Network) when referencing the

PSTN.

161. In PSTN and VoIP networks, call controllers and routers (e.g., PSTN

SSPs, SCPs and gateways, SIP UAs, SIP proxies, and SIP-PSTN gateways, H.323

terminals, H.323 gatekeepers, and H.323 gateways) make use of timers and time-out values to control call flow and timing. In the descriptions of typical call flows for both SIP and H.323 VoIP protocols, the simplified examples mostly assume request messages were responded to in an amount of time that would not exceed any defined time-out periods. RFC 3261 (SIP) describes a time-out scenario after a UA transmits a SIP INVITE message as follows:

> The state machine for the INVITE client transaction is shown in Figure 5. The initial state, "calling", MUST be entered when the TU initiates a new client transaction with an INVITE request.
>
> …
>
> For any transport, the client transaction MUST start timer B with a value of 64*T1 seconds (Timer B controls transaction timeouts).
>
> …
>
> If the client transaction is still in the "Calling" state when timer B fires, the client transaction SHOULD inform the TU that a timeout has occurred. The client transaction MUST NOT generate an ACK.

IETF RFC 3261 (SIP) (2002), Sections 17.1.1 "INVITE Client Transaction" and 17.1.1.2 "Formal Description", at pages 125-126. Thus, when a call is initiated in SIP with an INVITE message, the UA controls the call by setting a timer and timing out if the expected response is not received within the set timer period (e.g., in SIP "timer B" for transaction timeouts). Table four on page 264 of RFC 3261

121

provides a list of various timers and time-out values to be used by SIP UAs to

control the behavior and timing of session establishment and other call control

requests. IETF RFC 3261 (SIP) (2002), "Table of Timer Values", at page 264.

162. The AIN provides similar capabilities using timeouts to control call

processing One example of such a timeout control is:

> 14.7.5.2 Event Detection Points (EDPs)
>
> Events are detected as a result of processing a call. AIN enables an SCP to send a list of subsequent events that may occur during a call handled by an AIN SSP such that when one of the events on the list occurs, the SSP may be required to suspend call processing and launch a query to the SCP.
>
> …
>
> The SCP activates EDPs (during an already open transaction) by sending the SSP a NEL. The SSP detects the need for additional AIN control when an event included in the NEL is encountered at an EDP.
>
> …
>
> When the SSP recognizes an event as an EDP-Request, the SSP stops call processing, sends an EDP-Request message to the SCP, and awaits instruction from the SCP for further call processing.
>
> …
>
> Some EDPs supported by AIN include the following:
>
> …

> • O_No_Answer − tells the calling party's service that the called party has not answered the call before a timer expired.

Telcordia SR-2275, Issue 4, October 2000, Section 14.7.5.2 "Event Detection

Points (EDPs)", at pages 14-76 to 14-77. Another example of the use of time outs

in the PSTN is related to network congestion:

> Switching delays cause timeout conditions during call setup and occur when switching systems become severely overloaded. Timeouts are designed into switching systems to release common-control components after excessively long delay periods and provide the customer with a signal indicating call attempt failure. Switching-congestion timeouts with short holding-time attempts on circuit groups replace normal holding-time calls. Switching delays spread quickly throughout the network.

Telcordia SR-2275, Issue 4, October 2000, Section 10.1.2 "Network Traffic

Management Functions", at page 10-7. A person of normal skill in the art, starting

at least in the 1990's, would understand the use of timers and timeouts for call

processing in both the PSTN and VoIP, including call setup timeouts which may

lead to attempting another call route.

163. Usernames are used in both the SIP and H.323 standards as identifiers

of an account and associated information. H.323 describes the use of "alias"

names:

> 7.1.3 Alias address
> An endpoint may also have one or more alias addresses
> associated with it. An alias address may represent the
> endpoint or it may represent conferences that the
> endpoint is hosting. The alias addresses provide an
> alternate method of addressing the endpoint. These
> address include dialledDigits or partyNumber addresses
> (including private telephone numbers and public E.164
> numbers), H.323 IDs (alphanumeric strings representing
> names, e-mail like addresses, etc.), and any others
> defined in ITU-T Rec. H.225.0. Alias addresses shall be
> unique within a Zone. Gatekeepers, MCs, and MPs shall
> not have alias addresses.

Therefore, the H.323 standard allows alias names which may be a telephone

number or an alphanumeric "H.323 ID". The H.323 standard further describes an

H.323 ID as:

> "The H.323 ID consists of a string of ISO/IEC 10646-1
> characters as defined in ITU-T Rec. H.225.0. It may be a
> user name, conference name, e-mail name, or other
> identifier."

ITU H.323 (2003), Section 7.1.3 "Alias address", at page 51.

164. The SIP standard uses URI (Uniform Resource Identifier) type

identifiers which are well-known formats for network addresses. For example,

> 19.1 SIP and SIPS Uniform Resource Indicators
>
> A SIP or SIPS URI identifies a communications resource.
> Like all URIs, SIP and SIPS URIs may be placed in web
> pages, email messages, or printed literature. They contain
> sufficient information to initiate and maintain a

communication session with the resource. Examples of communications resources include the following:

- a user of an online service

IETF RFC 3261 (SIP) (2002), Section 19.1, at page 148. RFC 3261 specifies the

format of the URI:

> 19.1.1 SIP and SIPS URI Components
> The "sip:" and "sips:" schemes follow the guidelines in RFC 2396 [5]. They use a form similar to the mailto URL, allowing the specification of SIP request-header fields and the SIP message-body. This makes it possible to specify the subject, media type, or urgency of sessions initiated by using a URI on a web page or in an email message. The formal syntax for a SIP or SIPS URI is presented in Section 25. Its general form, in the case of a SIP URI, is:
>
> sip:user:password@host:port;uri-parameters?headers
>
> …
>
> user: The identifier of a particular resource at the host being addressed. The term "host" in this context frequently refers to a domain. The "userinfo" of a URI consists of this user field, the password field, and the @ sign following them. The userinfo part of a URI is optional and MAY be absent when the destination host does not have a notion of users or when the host itself is the resource being identified. If the @ sign is present in a SIP or SIPS URI, the user field MUST NOT be empty.
>
> If the host being addressed can process telephone numbers, for instance, an Internet telephony gateway, a telephone subscriber field defined in RFC 2806 [9] MAY be used to populate the user field. There are special escaping rules for encoding telephone-subscriber fields in SIP and SIPS URIs described in Section 19.1.2.

Declaration of James Bress in Support of Petition for *Inter Partes* Review
of U.S. Patent No. 8,542,815

IETF RFC 3261 (SIP) (2002), Section 19.1.1, pages 148-149. RFC 3261 explains

the use of usernames for authorization, for example when a call is attempted and

the request is sent to a SIP proxy server:

> 20.28 Proxy-Authorization
> The Proxy-Authorization header field allows the client to identify itself (or its user) to a proxy that requires authentication. A Proxy-Authorization field value consists of credentials containing the authentication information of the user agent for the proxy and/or realm of the resource being requested. See Section 22.3 for a definition of the usage of this header field.
>
> …
>
> Example:
> Proxy-Authorization: Digest username="Alice",
> realm="atlanta.com",
> nonce="c60f3082ee1212b402a21831ae",
> response="245f23415f11432b3434341c022"

IETF RFC 3261 (SIP) (2002), Section 20.28, at page 175. Also:

> 26.3.2 Security Solutions
> The operation of these security mechanisms in concert can follow the existing web and email security models to some degree. At a high level, UAs authenticate themselves to servers (proxy servers, redirect servers, and registrars) with a Digest username and password;

IETF RFC 3261 (SIP) (2002), Section 26.3.2, at page 242. Usernames are also

included in a User Agent registration. See IETF RFC 3261 (SIP) (2002) Section

26.3.2.1 "Registration", at pages 242-243. A person of normal skill in the art,

starting at least in the 1990's, would understand the use of usernames for identifying and controlling user accounts, profiles, registrations, etc.

165. Calling party and called party identifiers are the required information used for routing call and session establishment requests. For example, it was explained how in the PSTN an SCP may provide routing instructions for a call request. The calling party number and the called party number would be included in the SS7 routing request messages transmitted from the SSP (PSTN switch serving the calling party) to the SCP. Likewise, SIP and H.323 call set-up messages include calling party and called party identifiers as described above. A person of normal skill in the art would have known, at least by the 1990's, of the use of calling party and called party identifiers used for call routing in the PSTN, and VoIP H.323 and SIP based networks.

IX. CLAIM CONSTRUCTION

A. "receiving means for receiving a caller identifier and a callee identifier, in response to initiation of a call by a calling subscriber"

166. This term appears in Claim 28. I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my opinion for this term using the structure "an I/O port." I have not formed an

opinion as to whether this structure is corresponding structure or whether the

specification discloses corresponding structure for this term.

> **B.** **"means for locating a caller dialing profile comprising a username associated with the caller and a plurality of calling attributes associated with the caller" and "means for accessing a database of caller dialing profiles wherein each dialing profile associates a plurality of calling attributes with a respective subscriber, to locate a dialing profile associated with the caller, in response to initiation of a call by a calling subscriber"**

167. These terms appear in Claim 28 and 93, respectively. I have been

informed that these terms are governed by 35 U.S.C. § 112, Paragraph 6. I have

been instructed to provide my opinion for these terms using the structure "a

processor programmed to implement the algorithm illustrated in block 254 of

Figure 8A." I have not formed an opinion as to whether this structure is

corresponding structure or whether the specification discloses corresponding

structure for these terms.

> **C.** **"means for determining a match when at least one of said calling attributes matches at least a portion of said callee identifier"**

168. This term appears in Claim 28. I have been informed that this term is

governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my

opinion for this term using the structure "a processor programmed to implement

one or more of the algorithms illustrated in blocks 257, 380, 382, 390, and 396 of

Figure 8B." I have not formed an opinion as to whether this structure is

corresponding structure or whether the specification discloses corresponding structure for this term.

D.   "means for classifying the call as a public network call when said match meets public network classification criteria"

169.   This term appears in Claim 28. I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my opinion for this term using two alternative structures "a processor programmed to implement one or more branches of the algorithm illustrated in Figure 8B that leads to the end of block 408" and "a processor programmed to implement one or more branches of the algorithm illustrated in Figure 8B that leads to the end of block 410." I have not formed an opinion as to whether any of these structures are corresponding structure or whether the specification discloses corresponding structure for this term.

E.   "means for classifying the call as a private network call when said match meets private network classification criteria"

170.   This term appears in Claim 28. I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my opinion for this term using the structure "a processor programmed to implement one or more branches of the algorithm illustrated in Figure 8B that leads to the end of block 406 or block 279." I have not formed an opinion as to whether this

structure is corresponding structure or whether the specification discloses corresponding structure for this term.

F. **"means for producing a private network routing message for receipt by a call controller, when the call is classified as a private network call, said private network routing message identifying an address, on the private network, associated with the callee"**

171. This term appears in Claim 28. I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my opinion for this term using two alternative structures "a processor programmed to (i) produce a routing message identifying an address on the private network with which the callee identified by the contents of the callee ID buffer is associated OR (ii) implement the algorithm illustrated in block 644 of Figure 8C" and "a processor programmed to implement cell 350 of Figure 8A or cell 644 of Figure 8C." I have not formed an opinion as to whether any of these structures are corresponding structure or whether the specification discloses corresponding structure for this term.

G. **"means for producing a public network routing message for receipt by a call controller, when the call is classified as a public network call, said public network routing message identifying a gateway to the public network"**

172. This term appears in Claim 28. I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my

opinion for this term using two alternative structures "a processor programmed to implement the algorithm in block 563 of Figure 8D" and "a processor programmed to implement the algorithm illustrated in Figure 8D." I have not formed an opinion as to whether any of these structures are corresponding structure or whether the specification discloses corresponding structure for this term.

H. "formatting means for formatting said callee identifier into a pre-defined digit format to produce a re-formatted callee identifier"

173. This term appears in Claim 34. I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my opinion for this term using the structure "a processor programmed to implement the algorithm illustrated in block 261, block 388, block 394, or block 400 of Figure 8B." I have not formed an opinion as to whether this structure is corresponding structure or whether the specification discloses corresponding structure for this term.

I. "means for producing a private network routing message for receipt by a call controller, said private network routing message identifying an address, on a private network, through which the call is to be routed, when at least one of said calling attributes and at least a portion of a callee identifier associated with the callee match and when the match meets a private network classification criterion, the address being associated with the callee"

174. This term appears in Claim 93. I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my

opinion for this term using two alternative structures "a processor programmed to

(i) implement one or more branches of the algorithm illustrated in Figure 8B that

leads to the end of block 406 or block 279 and (ii) produce a routing message

identifying an address on the private network with which the callee identified by

the contents of the callee ID buffer is associated OR implement the algorithm

illustrated in block 644 of Figure 8C" and "a processor programmed to (i)

implement one or more branches of the algorithm illustrated in Figure 8B that

leads to the end of block 406 or block 279 and (ii) implement cell 350 of Figure 8A

or cell 644 of Figure 8C." I have not formed an opinion as to whether any of these

structures is corresponding structure or whether the specification discloses

corresponding structure for this term.

> **J.** **"means for producing a public network routing message for receipt by a call controller, said public network routing message identifying a gateway to a public network when at least one of said calling attributes and said at least said portion of said callee identifier associated with the callee match and when the match meets a public network classification criterion"**

175. This term appears in Claim 93. I have been informed that this term is

governed by 35 U.S.C. § 112, Paragraph 6 because it recites a "means for." I have

been instructed to provide my opinion for this term using two alternative structures

"a processor programmed to (i) implement one or more branches of the algorithm

illustrated in Figure 8B that leads to the end of block 408 and (ii) implement the

algorithm in block 563 of Figure 8D" and "a processor programmed to (i)

implement one or more branches of the algorithm illustrated in Figure 8B that

leads to the end of block 410 and (ii) implement the algorithm illustrated in Figure

8D." I have not formed an opinion as to whether any of these structures is

corresponding structure or whether the specification discloses corresponding

structure for this term.

> **K.** **"means for causing the private network routing message or the
> public network routing message to be communicated to a call
> controller to effect routing of the call"**

176. This term appears in Claim 111. I have been informed that this term

is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my

opinion for this term using the structure "a processor programmed to implement

the algorithm illustrated in block 381 of Figure 8A, block 646 of Figure 8C, and

block 568 of Figure 8D." I have not formed an opinion as to whether this structure

is corresponding structure or whether the specification discloses corresponding

structure for this term.

X. ANALYSIS OF THE PRIOR ART

177. In my opinion, all of the Challenged Claims are unpatentable as

obvious over a number of combinations of prior art references. An overview of the

prior art references I rely on in this Declaration is provided below, followed by a summary of the particular grounds that I believe render these claims obvious.

178.   As I discussed above, it is my understanding that for the purposes of this proceeding, the *earliest possible* priority date that the '815 Patent can claim is November 2, 2006. Even if one considers this priority date, I understand that each of the references described below qualify as prior art to the '815 Patent. Like the '815 Patent, each of the asserted prior art references relate at least to VoIP and call routing and address challenges presented by VoIP routing.

A.   Nadeau

179. U.S. Patent No. 6,240,449, entitled "Method and Apparatus for Automatic Call Setup in Different Network Domains," was filed on November 2, 1998 and issued on May 29, 2001. (EX1005.) Generally, *Nadeau* discloses a system that can be configured by a subscriber such that in response to a subscriber initiated communication request on a packet network the ensuing disposition of the routing of the communication request is controlled by the user's configuration. It would be understood by a person of ordinary skill in the art that a "communication request", "call request", "call initiation", "session set-up request", etc. are all referring to the same thing, which is the subscriber attempting to originate a call as the calling (caller) party to a called (callee) party.

180. Specifically, *Nadeau* teaches a service logic controller ("SLC"), shown below, that routes calls in response to "events occurring in a telecommunications network (PSTN or Mobile network) or a data communications network (such as the Internet)." (*Id*. at 1:45–52.)
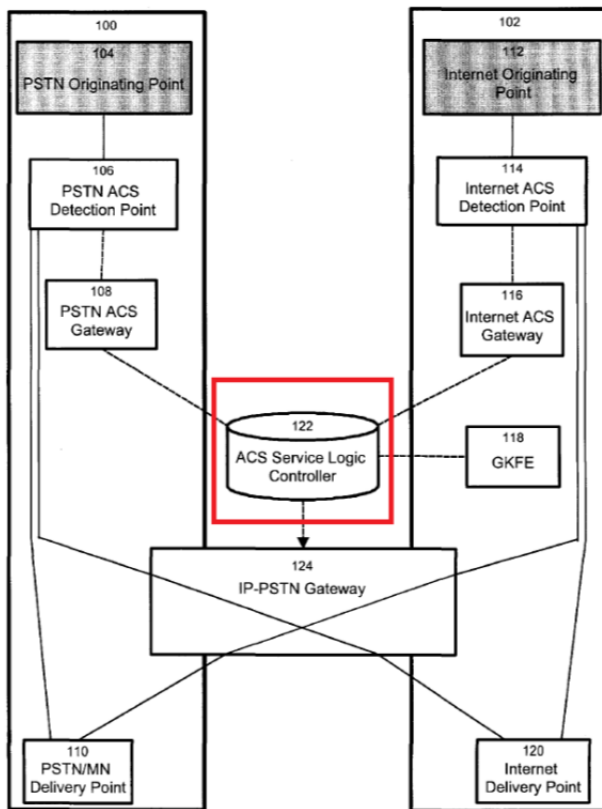
Figure 1
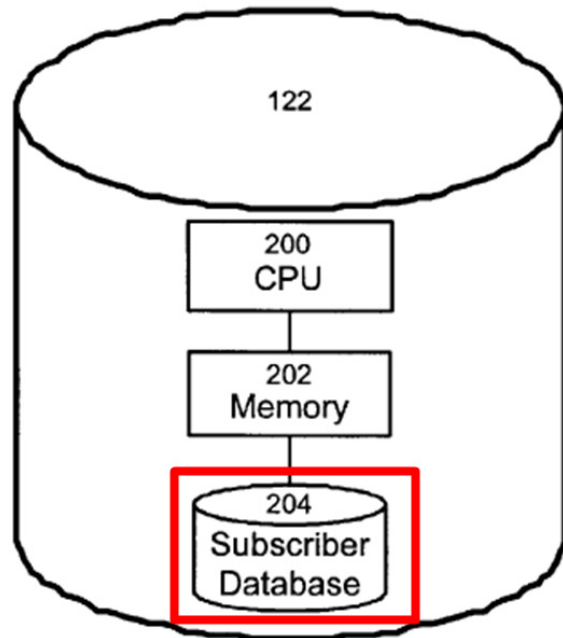
Figure 2

181. The SLC includes a "mass storage unit" that stores a database, shown above, of subscriber or user profiles. (*Id*. at 3:54–65.) Each profile is built by a subscriber. (*Id*. at 9:18–23.) A subscriber's profile includes subscriber identifiers, such as a subscriber ID and a home phone number, that associate the profile to the subscriber. (*Id*. at 9:55–64.) For example, a subscriber's home phone number may

135

be used to "automatically associate calls made to the service from the subscriber's

main directory number." (*Id*. at 9:62–64.)

182. Each subscriber profile also includes entries for individual called

parties. (*Id*. at 9:18–23, 9:55–10:20.) When a subscriber builds his profile, the

subscriber includes entries in the profile for individuals that he "wishes to be able

to reach." (*Id*. at 9:18–20.) An entry for an individual includes identifiers for that

individual, such as a name, directory number, IP address, or pseudo-address (e.g.,

an email address). (*Id*. at 9:20–23, 10:1–5.)

183. The entry also includes routing information that indicates whether a

call to the individual should be routed over an IP network or the PSTN. (*Id*. at

3:65–4:6, 10:1–20.) For example, the routing information may include rules based

on time of day or day of week, least cost routing, network priority, or quality of

service. (*Id*. at 10:8–20.) For example, the routing information may indicate that

calls to an individual between 8:00AM and 6:00PM should be routed over an IP

network. (*Id*. at 11:61–64, 12:49–52.) As another example, the routing

information may indicate that calls to an individual should be routed over the

PSTN if it is the routing option with the least cost. (*Id*. at 10:11–16.)

184. *Nadeau* provides an example profile, shown below. (*Id*. at 9:55–

10:20.) The identification information for the subscriber is shown in black. The

identification information for the called party is shown in green. The routing

information for the called party is shown in red.

PROFILE

subscriber ID;

the home phone directory number (if different from the subscriber ID) to automatically associate calls made to the service from the subscriber's main directory number;

the number of entries allowed in the subscriber's directory;

the directory itself which contains multiple entries, each entry including:

name of the person, e.g. John Smith;

directory number;

IP address or pseudo-address, where a sample pseudoaddress would be an e-mail address such as johns@xxx.xx;

server for address translation;

preferred IP carrier;

routing information;

time of day routing;

day of week routing;

least cost routing, such as:

complete to VoIP if IP address available;

137

complete to called party directory number using IP
through a terminating VOIP gateway;

complete to called party directory number using PSTN;

priority list (e.g. IP first, PSTN otherwise if calling from IP);

Quality of Service (QoS) bypass flag (e.g. force ACS to use IP in spite of low quality of service).

185.   When a caller initiates a VoIP call, the call is forwarded to the SLC for routing determination. (*Id*. at 7:1–5, 12:43–47.) The SLC retrieves the profile for the caller from the database and locates the entry for the callee in the profile. (*Id*. at 7:22–27, 12:48–52.) Based on the routing information in the entry for the callee, the SLC determines, for example, whether the call should be routed over an IP network or the PSTN. (*Id*. at 10:8–20, 11:27–31.) The SLC then generates and sends routing instructions to an ACS Gateway and a detection point (also referred to as a DPFE and an SSP (*id.* at 6:66–7:9, 11:43–46)) to route the call over the IP network or to an IP-PSTN Gateway for routing over the PSTN (*id*. at 7:5–9, 7:22–23, 11:27–31, 12:59–61). *Nadeau* describes the processes of the DPFE and the SLC as a service provided to subscribers for providing routing instructions for the subscriber's originating (outgoing) call requests from an Originating Point Functional Element (OPFE) (e.g., a telephone). *Nadeau* describes the DPFE associated process from the perspective of the DPFE receiving an ***incoming***

request for service from a subscriber which is actually the subscribers originating

(***outgoing***) call request that is received by the DPFE for which the DPFE consults

the SLC to provide routing instructions.

> Each domain comprises several different Functional Elements (FEs). **An ACS subscriber will originate a call through the ACS service by using an Originating Point Functional Element (OPFE)**. There are OPFEs in all three network domains, namely the PSTN or Mobile network OPFE **104,** for example a phone in the PSTN network or a handset in the Mobile network. A Detection Point Functional Element (DPFE) implements the network functionality which is responsible for **identifying call requests that require ACS treatment. For such calls, the DPFE will suspend call processing and originate a request for instructions to the Service Logic Controller (SLC)** via a Gateway Functional Element (GWFE). Upon reception of routing instructions from the SLC through the GWFE, **the DPFE will resume call processing according to the received instructions and route the incoming call directly to a Delivery Point FE or to the IP/PSTN GWFE 124 if needed**.

(*Id*. at 6:58–7:9 (emphasis added.)

186. *Nadeau*'s disclosure of the call routing capabilities provided by the

SLC and the user's directory entries teach that the user is able to configure the

system to include network classification criterion on a per called party basis. For

example, a person of ordinary skill in the art would understand from *Nadeau*'s

teaching that the call disposition information for a called party directory entry may

include routing the call to an IP address accessible on a local network (LAN) or an

IP address accessible on the Internet. More specifically, because *Nadeau* discloses

the ACS as being deployed in an H.323 VoIP network, the user's directory entry

could classify the call as "local" by providing an IP address for the called party that

is configured in the same H.323 zone as the calling party (the user). Alternatively,

the user's directory entry could classify the call as "external" by providing an IP

address for the called party that is configured on the Internet.

187. A person of ordinary skill in the art would know that in an H.323

network, endpoints (and gateways) register with an H.323 gatekeeper and that

there may only be one H.323 gatekeeper providing registration and call control

services per zone. *Nadeau* provides insight into how the ACS and SLC of *Nadeau*

interwork with the H.323 network by disclosing some of the basic premises of

H.323 gatekeeper functionality: "Specifically, in H.323 compliant networks, the

GKFE functionality is implemented on a gatekeeper which is responsible for

managing all IP telephony related activities in a particular zone, performing call

control, managing bandwidth and performing address translation. There are as

many gatekeepers as there are zones." (*Id*. at 4:13–19.) Therefore, a person of

ordinary skill in the art would know, and *Nadeau* explicitly discloses that, an

H.323 zone is controlled by the H.323 gatekeeper entity.

188.   In addition to the example provided above where a called party call
routing disposition may be classified as "local" when routed to an IP address in the
same H. 323 zone as the calling party or "external" when routed to an Internet IP
address, there may be numerous other examples of how the user in *Nadeau*'s
system may configure his or her user profile's called party directory to provide
network classification criterion.   For example, time of day routing could be
configured to classify the network to use as the local IP network or (private
classification) H.323 zone to contact a user's co-worker during the daytime and
weekdays and to classify the network to use as the PSTN through an IP/PSTN
Gateway (public classification).

189.   Another example of the use of network classification criterion in a
user profile's directory would be to configure for one called party's call disposition
to be routed to an IP carrier (such as an Internet Telephony Service Provider
(ITSP) or an Internet Service Provider (ISP)) and for another called party's call
disposition to be routed to the PSTN through an IP/PSTN Gateway.   When a call is
routed to an ITSP or ISP, the part of the Internet network the call is routed to is
controlled by the ISP by virtue of the fact that the ISP would own the IP addresses
used to connect to it through the Internet.   *Nadeau* discloses such a case for a
called party connected to the Internet through an ISP.   "The IP address associated

141

with that type of connection is valid only for the duration of a call. The IP address

is picked from **a pool of addresses owned by the ISP**.” (*Id*. at 10:35–38

(emphasis added).) Thus, in the case of routing a call to an ISP, the call is routed

to a part of the packet network (Internet) that is controlled by the ISP. In the case

of the network classification being to route the call over the PSTN, the call is first

routed to a IP/PSTN gateway which would be controlled or owned by any one of

the different VoIP PSTN gateway service providers (such as a carrier) and likewise

the Internet IP addresses it uses to connect to the Internet would be owned or

controlled by that VoIP Gateway service provider. (*Id*. at 7:5–9, 7:22–23, 11:27–

31, 12:59–61.) Thus, a call connected using the network classification of Internet

Service Provider (ISP) would route the call to a first part of the packet network

controlled by an entity (the ISP) and a call connected using the network

classification of PSTN would route the call to different (second) part of the packet

network not controlled by the ISP.

B.   Kelly

190. U.S. Patent No. 6,594,254, entitled “Domain Name Server

Architecture for Translating Telephone Number Domain Names into Network

Protocol Addresses,” was filed on August 14, 1997 and issued on July 15, 2003.

(EX1006.)

191. *Kelly* teaches a WebPhone client that determines whether a call should be routed over the PSTN or the Internet. (*Id*. at 11:16–40, 12:55–57, 13:21–57.) The WebPhone client performs a digit analysis algorithm, shown below, that allows it to select a carrier and gateway to route the call. (*Id*. at 11:66–12:14, 12:32–57, 13:58–59.)
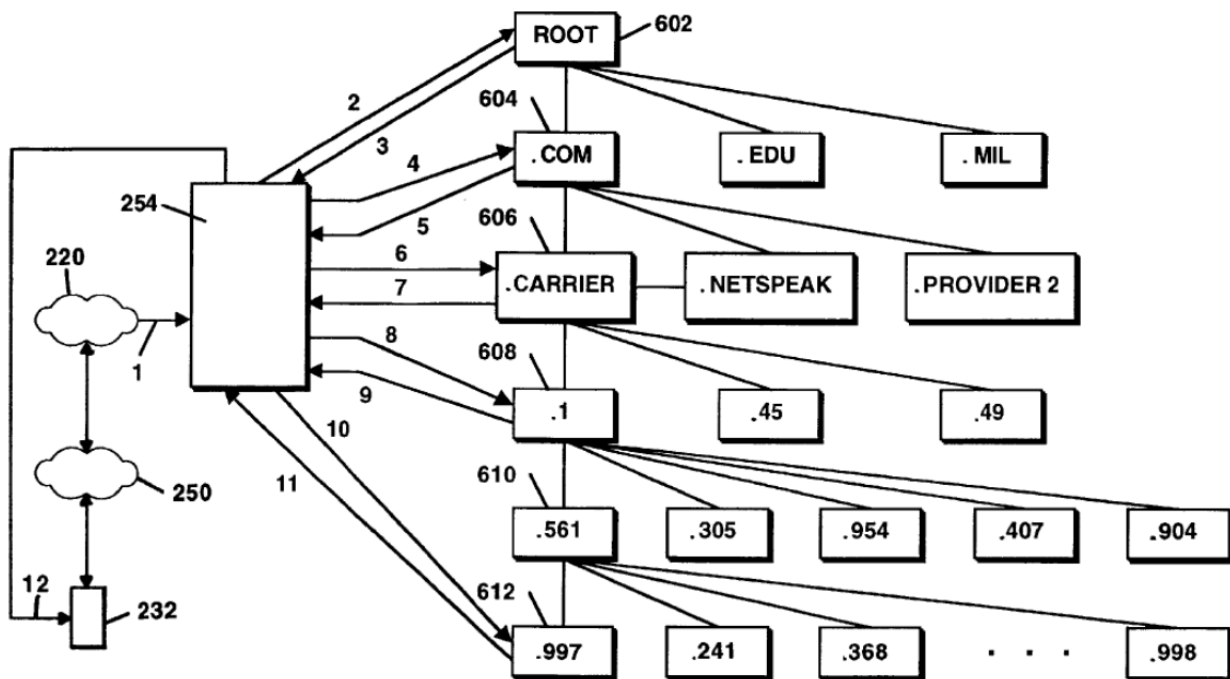
Figure 6

192. The WebPhone client receives a dialed telephone number from a caller. (*Id*. at 11:54–59.) The WebPhone client determines a carrier for the call and generates a hybrid telephone number domain using the carrier name and the dialed telephone number. (*Id*. at 12:3–15.) The WebPhone client then uses

successive portions of the hybrid telephone number domain to retrieve successive references to different name servers. (*Id*. at 12:32–54.) The last returned reference contains the IP address of the appropriate carrier gateway. (*Id*. at 12:55–57.) The WebPhone client then initiates the call by sending the hybrid telephone number domain to the IP address of the appropriate carrier gateway. (*Id*. at 13:22–26.)

C. Vaziri

193. U.S. Patent No. 7,715,413 ("*Vaziri*"), entitled "Multi-Network Exchange System for Telephony Applications," filed on October 25, 2004 and published on April 28, 2005. (EX1007.)

194. *Vaziri* teaches MNES servers and MNES bridges, shown below, that determine whether calls should be routed over the Internet or the PSTN. (*Id*. at 12:59–64.)

Figure 2

Figure 20

195. The MNES bridge performs the algorithm shown below to remove international dialing digits and national dialing digits from a dialed telephone number if they match the caller's international and/or national dialing digits. (*Id*. at 29:25–36.) The MNES bridge and server then determine whether the formatted telephone number should be routed over the Internet or the PSTN. (*Id*. at 30:57–67.)

Figure 12

XI. SUMMARY OF THE GROUNDS FOR UNPATENTABILITY OF THE CHALLENGED CLAIMS

196. Based on my review of the prosecution history of the '815 Patent, I understand that *Nadeau*, *Kelly*, and *Vaziri* were not cited as considered by the United States Patent and Trademark Office during the original prosecution of the '815 Patent.

146

197. Below is a table summarizing the grounds for unpatentability of all
claims of the '815 Patent that I address in this Declaration.

Ground	'815 Patent Claims	Obvious under 35 U.S.C. § 103
1	1, 7, 27, 54, 72–74, and 92	*Nadeau* in view of *Kelly*
2	28, 34, 93, and 111	*Nadeau* in view of *Kelly* and *Vaziri*

198. A detailed explanation of why the various combinations above render
the Challenged Claims obvious is provided below.

XII. *NADEAU-KELLY* RENDERS OBVIOUS CLAIMS 1, 7, 27, 54, 72–74, AND 92

A. It was obvious to modify the service logic controller ("SLC") of *Nadeau* to perform the gateway selection process taught in *Kelly*

199. One of ordinary skill in the art would have considered *Kelly* when
implementing or improving *Nadeau*. *Nadeau* and *Kelly* are from the same
technical field—telecommunications systems, such as telephony systems (wired
telephony, wireless telephony, IP telephony, etc.). Specifically, *Nadeau* relates to
a call setup service that routes PSTN, VoIP, or wireless/mobile calls over one of
the PSTN, an IP network, or a wireless/mobile network. (EX1005 at 1:5–11, 2:38–
48, 3:33–4:6, Figure 1.) *Kelly* relates to a call setup service that routes calls over
either the PSTN or an IP network. (EX1006 at 1:59–64, 2:42–51, Figure 2.) Both
Nadeau and *Kelly* are concerned with reducing the cost associated with making
VoIP calls. (EX1005 at 2:3–6, 6:30, 10:11–16; EX1006 at 13:46–57.)

147

200. *Nadeau* teaches that the call setup service includes a service logic
controller ("SLC") that determines call routing. (EX1005 at 2:38–43, 3:56–4:6,
7:20–27.) The SLC may determine to route a VoIP call over the PSTN or an IP
network based on least cost routing. (*Id.* at 10:11–16.) The system in *Nadeau*,
however, includes only one gateway called the IP-PSTN Gateway or Gateway
Functional Element (GWFE), to route the VoIP call to the PSTN. (*Id.* at Figure 1.)
As a result, one of ordinary skill would understand that the cost for such a routing
is dictated by that one gateway.

201. *Kelly* recognizes that costs may be further reduced by selecting a
gateway that provides lower cost routing compared to other gateways (e.g., by
selecting a gateway of a carrier that charges less to route calls to a particular callee
compared to other carriers). (EX1006 at 13:39–57.) *Kelly* teaches a gateway
selection process that involves three steps: (1) transform a dialed telephone
number (e.g., 1-561-997-4001) into a hybrid telephone number domain name (e.g.,
4001-997561-1.carrier.com) (*id.* at 11:54–12:11); (2) use successive portions of the
hybrid telephone number domain name to retrieve references to name servers that
contain an IP address of a carrier gateway (*id.* at 12:32–57); and (3) produce a call
packet containing the hybrid telephone number domain name and the IP address of
the carrier gateway to effect the call (*id.* at 13:21–26). By performing this

process, the system in *Kelly* is able to select a carrier gateway that "minimize[s]

toll charges." (*Id*. at 13:46–49.)

202.   One of ordinary skill would have been motivated to modify the SLC

of *Nadeau* to perform the gateway selection process taught in *Kelly* to further

reduce the cost of routing VoIP calls over the PSTN as recognized by *Kelly*.

Nadeau explains that it would be desirable to find a least cost routing path for a

VoIP call to avoid "paying unnecessary toll charges." (EX1005 at 2:3–6; *see also*

id. at 6:30, 10:11–16.) *Kelly* teaches a gateway selection process that improves the

cost savings desired by *Nadeau*. According to *Kelly*, the gateway selection process

allows selection of a gateway that "minimize[s] the toll charges." (EX1006 at

13:46–57.) In other words, *Kelly* explains that performing the gateway selection

process allows selection of a gateway that minimizes toll charges (EX1006 at

13:46–49), which is the same result desired by *Nadeau* (EX1005 at 2:3–6; *see also*

id. at 6:30, 10:11–16).

203.   Additionally, one of ordinary skill in the art could have easily made

this modification because it is merely a combination of prior art elements (the SLC

of *Nadeau* and the gateway selection process of *Kelly*) according to known

methods (the modification would require nothing more than programming the SLC

to perform the gateway selection process taught in *Kelly*) to yield predictable

results (*Kelly* teaches the result: allows selection of a gateway). Furthermore, this modification involves the application of a known technique (the gateway selection process of *Kelly*) to a known device (the SLC of *Nadeau*) ready for improvement (the modification would merely require programming the SLC) to yield predictable results (*Kelly* teaches the result: allows selection of a gateway). This modification could be made with a reasonable expectation of success without undue experimentation because it would merely require programming of the SLC to perform a known process with the known result of selection of a gateway. Additionally, this modification is the use of a known technique (the gateway selection process of *Kelly*) to improve similar devices (*Nadeau* and *Kelly* both disclose call routing systems) in the same way (the gateway selection process improves both systems of *Nadeau* and *Kelly* by allowing them to select a gateway).

204. Therefore, it would have been obvious to modify the SLC of *Nadeau* to perform the gateway selection process, as taught in *Kelly*.

B. Claim 1

    1. **Preamble: "A process for operating a call routing controller to facilitate communication between callers and callees in a system comprising a plurality of nodes with which callers and callees are associated"**

205. To the extent this preamble is limiting, *Nadeau-Kelly* teaches this preamble.

206. *Nadeau-Kelly* teaches an automatic call service ("ACS") that facilitates communication between callers and callees by establishing calls (both PSTN and VoIP) between callers and callees. "[T]he ACS service **allows the establishment of a connection from a caller (subscriber) to a called party, transparently using whichever network (PSTN/Mobile, IP) is best**, based on conditions specified by the service subscriber and external conditions." (EX1005 at 6:15–23 (emphasis added).) One of ordinary skill in the art would understand that calls over a PSTN network are traditional, PSTN telephone calls and that calls over an IP network are VoIP calls.

207. The ACS includes a Service Logic Controller ("SLC") that performs call routing. (*Id.* at Figures 1–4; 2:49–52; 11:33–12:65.) "As embodied and broadly described herein, the invention provides a **service logic controller for the management of communication sessions**." (*Id.* at 2:49–51 (emphasis added).) ""The primary goal of the SLC 122 is to provide the DPFEs with **call processing instructions**." (*Id.* at 7:22–23 (emphasis added).) The ACS and SLC are shown below using Figures 1 and 2 of *Nadeau*.
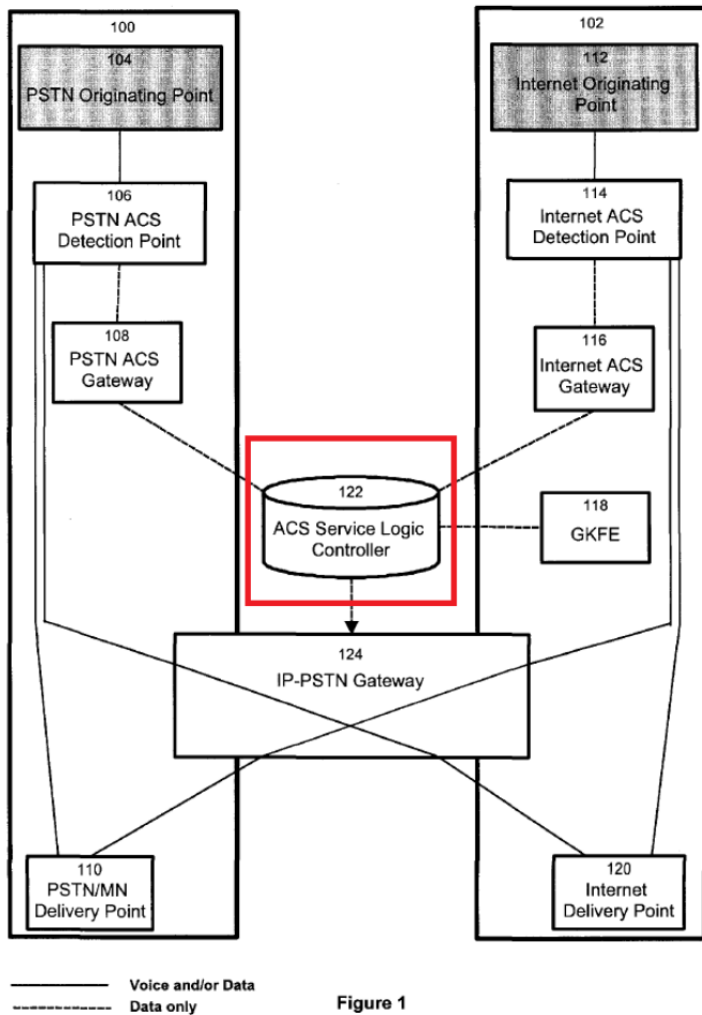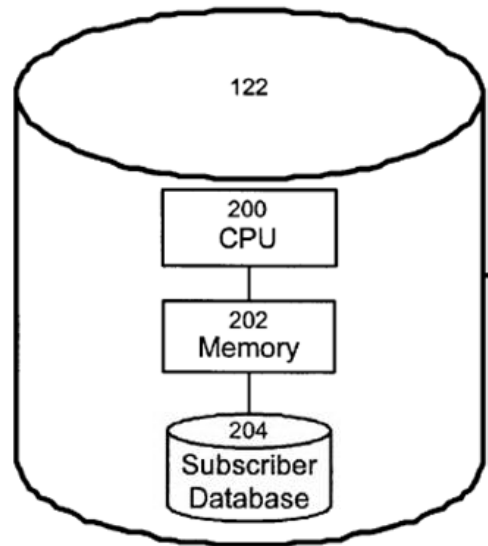
Figure 1

Figure 2

208. In the ACS, callers and callees use telephones, PCs, a DPFE, and a gateway in the system to communicate with each other. (*Id*. at Figures 1, 3, and 4; 6:58–8:6; 8:45–9:7.) "An ACS subscriber will originate a call through the ACS service by using...**a phone in the PSTN network** or...a **multimedia PC**." (*Id*. at 6:59–65 (emphasis added).) "Finally, examples of an Internet Delivery Point FE 120 include**: a multimedia PC with: a Voice-over-IP (VoIP) client**." (*Id*. at 9:1–

4 (emphasis added); s*ee also*, *id*. at 7:41–44 (referencing "**many different nodes in the IP telephony network**") (emphasis added), 8:42–50.).)

209. Thus, *Nadeau-Kelly* teaches a process for operating a call routing controller, such as using the SLC, to facilitate communication between callers and callees, such as by establishing calls between callers and callees, in a system, such as the ACS, comprising a plurality of nodes with which callers and callees are associated, such as telephones, PCs, a DPFE, and a gateway. One of ordinary skill in the art would understand the Service Logic **Controller** to be a controller. Additionally, *Nadeau-Kelly* explains that the primary goal of the SLC is to provide routing instructions to route a call. (EX1005 at 7:20–27.) Thus, one of ordinary skill in the art would understand that the SLC is a call routing controller.

> **2. Limitation 1a: "in response to initiation of a call by a calling subscriber, receiving a caller identifier and a callee identifier"**

210. *Nadeau-Kelly* teaches Limitation 1a.

211. *Nadeau-Kelly* teaches a caller initiating a call using a PC. (EX1005 at 6:58–65.) "[T]he ACS service **allows the establishment of a connection from a caller (subscriber) to a called party,** transparently using whichever network (PSTN/Mobile, IP) is best, based on conditions specified by the service subscriber and external conditions." (*Id*. at 6:19–23 (emphasis added).) "An ACS **subscriber**

will originate a call through the ACS service by using...**a phone in the PSTN network** or...a **multimedia PC**." (*Id*. at 6:59–65 (emphasis added).) "1. The **user** connects to the Internet and **starts a VOIP client** modified to support this service. The **user** either **enters the name of the person to call, uses a Speed Dial entry, or speaks the name of the person to call** if the client is voice-enabled." (*Id*. at 12:34–38 (emphasis added).) This caller is also referred to as a subscriber and a user. (*Id*. at 6:19–23, 6:59–65, 12:34–38.)

212. The SLC will receive a message indicating the caller's home telephone number and the callee's name. The caller enters "the name of the person to call" into a VoIP client. (*Id*. at 12:34–38.) The client then sends the SLC the caller's "home phone number" and "the name of the person to reach." (*Id*. at 12:42–47.)

> 1. The **user** connects to the Internet and **starts a VOIP client** modified to support this service. The **user** either **enters the name of the person to call, uses a Speed Dial entry, or speaks the name of the person to call** if the client is voice-enabled.
>
> 2. The VOIP client (Internet ACS DPFE 114) detects that the data entered in the called party field is not an address and suspends call processing.
>
> 3. The VOIP client sends a message to a node in the Internet domain that acts as the Internet ACS GWFE 116. The message contains the subscriber ID **(e.g. his home phone number) and the name of the person to reach**.

> 4. The ACS IP GWFE 116 reformats and **sends the query to the SLC 122**."

(*Id*. at 12:34–47 (emphasis added).) An overall diagram of this call process is shown in Figure 4 of the '815 Patent, reproduced below.

Figure 4
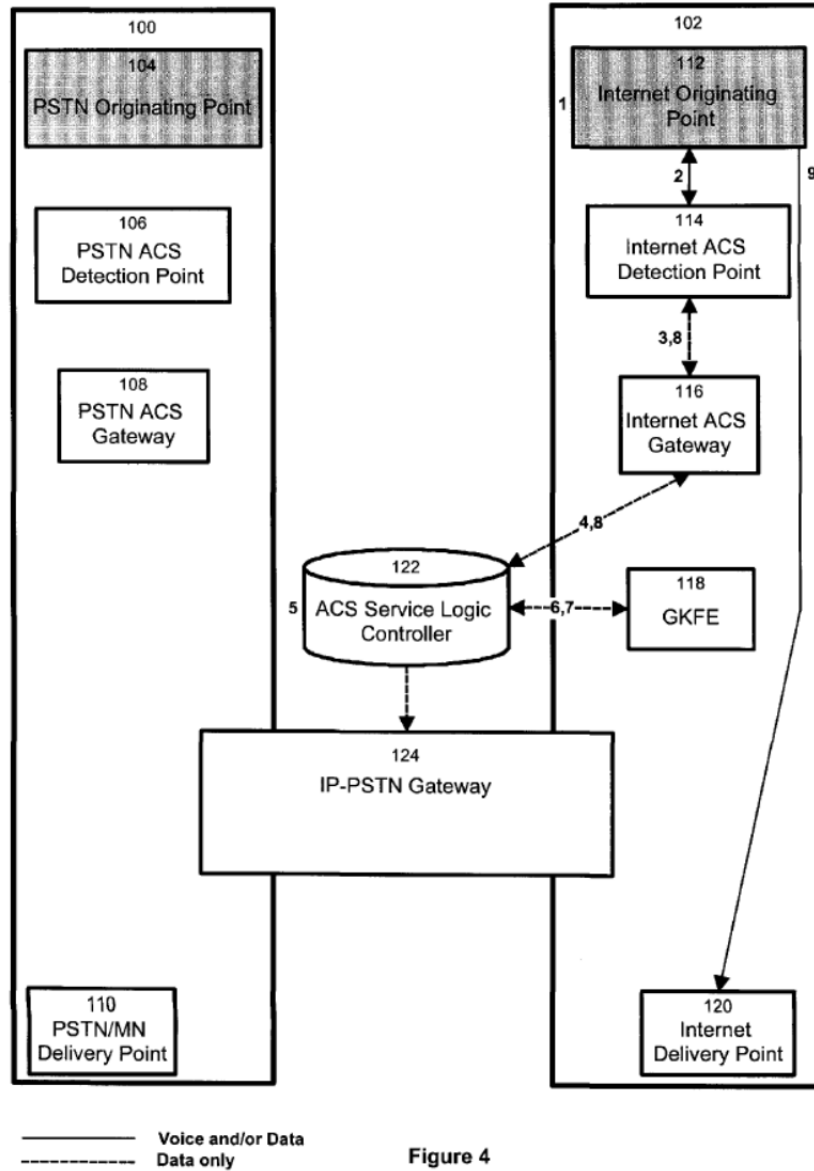
213.   Thus, *Nadeau-Kelly* teaches the SLC receiving a caller identifier, such as the caller's home telephone number, and a callee identifier, such as the name of the callee, in response to initiation of a call by a calling subscriber, such as the caller.

> **3.   Limitation 1b: "locating a caller dialing profile comprising a username associated with the caller and a plurality of calling attributes associated with the caller"**

214.   *Nadeau-Kelly* teaches Limitation 1b.

215.   The SLC locates a caller's profile in a database because the SLC "consults [the] particular caller's service profile" in a "Subscriber Database" to process the call.   (EX1005 at 3:56–65, 7:24–27, 7:34–40, 9:62–64, 9:55–64 (locating profile using "home phone directory number").)   "[T]he SLC 122 will **consult a particular caller's service profile**, consisting in service logic as well as a list of conditions and events to be used to process the caller's incoming calls." (*Id*. at 7:24–27.)   "The ACS system **uses the routing information associated to a particular name in the subscriber's database** to decide how to handle an outgoing call." (*Id*. at 11:13–15 (emphasis added).)

216.   The profile includes a "subscriber ID." (*Id*. at 9:55–10:20.)

> The Subscriber Database 204 as shown in FIG. 2 contains a **record for each such subscriber**, where this

> record includes an information element formed of
> multiple fields, each containing specific information,
> such as:
>
> > **a subscriber ID**;
> >
> > **the home phone directory number** (if different from
> > the subscriber ID) **to automatically associate calls
> > made to the service from the subscriber's main
> > directory number**.

(*Id*. at 9:55–64 (emphasis added).)

217.   The profile also includes an entry for each person that the caller wants

to call. (*Id*. at 9:18–23, 9:66–67.) Each entry includes calling attributes specified

by the caller like identifiers for the called party, such as a name or telephone

number, and routing information that indicates how calls to that party should be

routed. (*Id*. at 9:18–23, 9:66–10:20; *see also* 4:2–6 (example entry for "John

Smith"), 12:48–52 (example entry for time of day routing).) "In terms of the ACS

service itself, an **ACS subscriber first builds a directory of the individuals**

he/she wishes to be able to reach, prior to using the ACS system. The directory

must include some **routing information for each entry, such as the individual's**

directory number (DN) for the PSTN and an IP address or pseudo-address for

the Internet." (*Id*. at 9:18–23 (emphasis added).) "In a very specific example, an

illustrative script can be: "**Between 8 and 6 on working days, route calls made to**

John Smith to his office unless his cellular phone is activated, in which case

calls should be routed to the cellular phone." (*Id.* at 3:56–4:6 (emphasis

added).)

> The Subscriber Database 204 as shown in FIG. 2 contains a **record for each such subscriber**, where this record includes an information element formed of multiple fields, each containing specific information, such as:
>
> ...
>
> the directory itself which contains multiple entries, each entry including:
>
> > **name of the person, e.g. John Smith**;
> >
> > **directory number**;
> >
> > IP address or pseudo-address, where a sample pseudoaddress would be an e-mail address such as johns@xxx.xx;
> >
> > server for address translation;
> >
> > preferred IP carrier;
> >
> > routing information;
> >
> > > **time of day routing**;
> > >
> > > day of week routing;
> > >
> > > least cost routing, such as:
> > >
> > > > **complete to VoIP if IP address available**;
> > > >
> > > > complete to called party directory number using IP through a terminating VOIP gateway;
> > > >
> > > > **complete to called party directory number using PSTN**;

158

> **priority list (e.g. IP first, PSTN otherwise if
> calling from IP)**."

(*Id*. at 9:55–10:20 (emphasis added).)

218.   Thus, *Nadeau-Kelly* teaches locating a caller dialing profile, such as
the caller's profile in the database, comprising a username associated with the
caller, such as a subscriber ID, and a plurality of calling attributes associated with
the caller, such as callee entries that include identifiers for the callee and routing
information for the callee.

**4.   Limitation 1c: "determining a match when at least one of
said calling attributes matches at least a portion of said
callee identifier"**

219.   *Nadeau-Kelly* teaches Limitation 1c.

220.   The SLC matches a callee's name provided by a caller with the callee
names indicated in the profile to determine the appropriate routing information to
use.   The SLC uses a callee's name (callee identifier) to locate an entry for the
callee in the caller profile. (EX1005 at 4:3–6, 10:1–2, 11:13–15, 12:42–52.) "The
ACS system uses the routing information associated to a **particular name** in the
subscriber's database to decide how to handle an outgoing call." (*Id*. at 11:13–15
(emphasis added).)

> 3. The VOIP client sends a message...the Internet ACS
> GWFE 116. The message contains the subscriber ID (e.g.

159

> his home phone number) and the **name of the person to reach**.
>
> 4. The ACS IP GWFE 116 reformats and sends the query to the SLC 122.
>
> 5. **The SLC 122 uses the received information to access the subscriber's database.** This record indicates that **the call to this person** should be completed using the Internet between 08:00 and 18:00 if the person is connected to the Internet.

(*Id*. at 12:34–52 (emphasis added).)

221. When the callee's name (e.g., John Smith) matches the name indicated in an entry (at least one of said calling attributes), the SLC knows it has located the entry for the callee. (*Id*. at 4:2–6, 10:1, 11:13–15.) The callee could also be identified and matched with calling attributes using other information, such as a directory number, IP address, or pseudo-address such as an e-mail address. (*Id*. at 10:2–5, 11:13–15.)

> the directory itself which contains multiple entries, each entry including:
>
> name of the person, e.g. **John Smith**;
>
> **directory number**;
>
> **IP address** or **pseudo-address**, where a sample pseudoaddress would be an email address such as johns@xxx.xx;"

(*Id*. at 9:66–10:5 (emphasis added).) "In a very specific example, an illustrative script can be: 'Between 8 and 6 on working days, **route calls made to John Smith** to his office unless his cellular phone is activated, in which case calls should be routed to the cellular phone.'" (*Id*. at 4:3–6 (emphasis added).)

222.   Thus, *Nadeau-Kelly* teaches determining a match when at least one of said calling attributes, such as the callee's name, directory number, IP address, or email address in the directory entry in the caller profile, matches at least a portion of said callee identifier, such as the name, directory number, IP address, or email address provided by the caller.

5.   Limitation 1d: "classifying the call as a public network call when said match meets public network classification criteria and classifying the call as a private network call when said match meets private network classification criteria"

223.   *Nadeau-Kelly* teaches Limitation 1d.

224.   The SLC uses the routing information in the directory entry to determine whether the VoIP call should be routed over an IP network or the PSTN. The routing information in a callee's entry specifies conditions under which a call is routed either over the PSTN or an IP network. (EX1005 at 10:8–20, 11:27–30.)

routing information;

time of day routing;

> day of week routing;
>
> **least cost routing, such as:**
>
>> **complete to VoIP if IP address available;**
>>
>> complete to called party directory number using IP through a terminating VOIP gateway;
>>
>> **complete to called party directory number using PSTN;**
>
> **priority list (e.g. IP first, PSTN otherwise if calling from IP);**
>
> **Quality of Service (QoS) bypass flag (e.g. force ACS to use IP in spite of low quality of service).**

(*Id*. at 9:55–10:20 (emphasis added).) The SLC can determine that a call should be routed over the IP network when an IP address for the callee is available (i*d*. at 10:12) or when a Quality of Service bypass flag is set (*id*. at 10:19–20).

225. *Nadeau-Kelly* provides examples of routing information and routes. "This record indicates that **the call to this person** should be completed using the Internet between 08:00 and 18:00 if the person is connected to the Internet." (*Id*. at 12:34–52 (emphasis added).) "This communication session disposition program determines how a communication session to a particular called party is to be managed in dependence upon various factors, such as the time of day, type of communication, etc. In a very specific example, an illustrative script can be: 'Between 8 and 6 on working days, **route calls made to John Smith** to his office

162

unless his cellular phone is activated, in which case calls should be routed to the cellular phone.'" (*Id*. at 3:65–4:6 (emphasis added).)

226.   Based on the routing information, the SLC determines where to route a call. (*Id*. at 7:24–27.) "[T]he SLC 122 will **consult a particular caller's service profile**, consisting in service logic as well as a list of conditions and events to be used to process the caller's incoming calls." (*Id*. at 7:24–27.) "The ACS system uses the **routing information** associated to a particular name in the subscriber's database to **decide how to handle an outgoing call**." (*Id.* at 11:13–15 (emphasis added); *see also id*. at 11:27–31 (showing "PSTN" and "IP network" as routing choices).)

227.   *Nadeau* discloses that a call can be routed over the PSTN or an "IP network." (EX1005 at 3:44–55, 11:27–31, 9:55–10:20.) *Nadeau* however does not explicitly state that the IP network is a "private network." As I discussed above in the State of the Art, one of ordinary skill in the art would know that an IP network, such as the Internet includes private networks like intranets and local area networks ("LAN" or "LANs"). *See* ¶¶ 87, 116 above. These private networks differ from public networks in that the public generally cannot access or purchase access to a private network like a LAN. The public generally can access or purchase access to public networks like the PSTN and the Internet backbone.

Therefore, when Nadeau discloses that a call can be routed over an IP network, one

of ordinary skill in the art would understand that Nadeau is teaching that the call

can be routed over private networks like intranets and LANs.

228. Additionally, *Kelly* teaches that an IP network includes private

networks like intranets and LANs. "A popular network protocol, the Transmission

Control Protocol/Internet Protocol (TCP/IP) is utilized by the Internet and

lntranets>lntranets are private networks such as Local Area Networks

(LANs) and Wide Area Networks (WAN)." (EX1006 at 2:26–35 (emphasis

added).) It would have been obvious for one of ordinary skill to modify the IP

network of *Nadeau* to include intranets and LANs as taught by *Kelly*. This

modification is simply a combination of known elements (an IP network in *Nadeau*

and intranets and LANs in *Kelly*) according to known methods (adding an intranet

or LAN would require nothing more than adding a common router that has long

existed in homes and businesses) to yield predictable results (allows an intranet or

LAN to be implemented). Furthermore, this modification involves application of a

known technique (implementing an intranet or LAN) to improve a known device

(the IP network of *Nadeau*) ready for improvement (the modification would merely

require adding a common network router to the IP network) to yield predictable

results (allows an intranet or LAN to be implemented). Additionally, this

modification is the use of a known technique (adding an intranet or LAN to an IP

network) to improve similar devices (*Nadeau* and *Kelly* both disclose IP networks)

in the same way (allows an intranet or LAN to be implemented). Moreover, this

modification is the simple substitution of one known element (the IP network of

Nadeau) for another (the LAN of *Kelly*) to obtain predictable results (the results of

Nadeau would not change based on this modification because a LAN is still an IP

network and routing a call over a LAN instead of a general IP network would be

substantially similar operations).

229. The SLC can also determine that a call should be routed over the

PSTN based on a least cost routing rule (*id*. at 10:11, 10:15–16) or a priority list

(*id*. at 10:17–18).

230. Thus *Nadeau-Kelly* teaches classifying the call as a public network

call, such as by determining that the call should be routed over the PSTN, when

said match meets public network classification criteria, such as when the routing

information in the matching directory entry indicates that the call should be routed

over the PSTN, and classifying the call as a private network call, such as by

determining that the call should be routed over an IP network, when said match

meets private network classification criteria, such as when the routing information

in the matching directory entry indicates that the call should be routed over an IP

network.

> **6.   Limitation 1e: "when the call is classified as a private
> network call, producing a private network routing message
> for receipt by a call controller, said private network routing
> message identifying an address, on the private network,
> associated with the callee"**

231.   *Nadeau-Kelly* teaches Limitation 1e.

232.   When the VoIP call should be routed over an IP network, the SLC

produces routing instructions and sends those instructions to a DPFE and ACS

Gateway.   The routing instructions instruct the DPFE to route the call to an IP

address of the callee.   The SLC generates and sends "routing instructions" to a

detection point ("DPFE") or Internet ACS Gateway.   (EX1005 at 7:22–23, 12:55–

61.)   "The primary goal of the SLC 122 is to provide the **DPFEs** with **call**

processing instructions." (*Id*. at 7:22–23 (emphasis added).)   "**Upon reception of**

routing instructions from the SLC through the GWFE, **the DPFE will resume**

call processing according to the received instructions and route the incoming

call **directly to a Delivery Point FE** or to the IP/PSTN GWFE 124 if needed."

(*Id*. at 7:5–9; *see also*, *id*. at 11:27–28 (showing "IP network" as routing option).)

233. For an IP call, when the SLC determines that the call should be routed over the IP network, the routing instructions instruct the DPFE to route the call to an IP address of the callee.

> 7. The IP GKFE 118 returns to the SLC 122 **the IP address** corresponding to this pseudo-address indicating that **this person is currently connected to the Internet and ready to receive VoIP calls**.
>
> 8. The SLC 122 returns to the Internet **ACS GWFE 116** a **message** indicating to **route the call to the IP address** retrieved from the Internet domain.

(*Id*. at 12:55–61 (emphasis added).)

234. Although *Nadeau* does not explicitly call the DPFE and ACS Gateway a "call controller," they are nevertheless a call controller as described in the '815 Patent. The specification of the '815 Patent explains that a call controller receives a routing message from a routing controller and then completes a call according to the routing message. (EX1001 at 14:10–23.)

235. The DPFE and ACS Gateway form a "call controller" as contemplated by the '815 Patent because the DPFE and ACS Gateway receive "routing instructions" from the SLC and then complete a call according to those "routing instructions." (EX1005 at 7:5–9, 7:20–23, 12:59–65.) Thus, the DPFE and ACS Gateway are a call controller.

236. Although *Nadeau* does not disclose that the routing instructions explicitly identify the IP address of the callee, this feature would have been obvious.

237. The routing instructions must include an identifier for the destination of the call in order for the DPFE to know where to route the call (e.g., to a callee IP address or an IP-PSTN Gateway). The purpose of the routing instructions is to instruct the DPFE and ACS Gateway where to route a call. (EX1005 at 7:1–9, 7:20–27, 12:59–61.) If the routing instructions did not include an identifier for the destination, then the DPFE and ACS Gateway would not know where to route the call based on the routing instructions, thus defeating the purpose of the routing instructions. Therefore, the routing instructions must include an identifier of the destination. If the destination is a callee IP address (*id*. at 7:5–9, 11:27–31, 12:59–61), then it would be obvious that the routing instructions include that IP address.

238. Therefore, one of ordinary skill in the art would know that the routing instructions produced by the SLC must include the callee's IP address, in view of the teaching that the network is an IP network (*id*. at 11:27) and that the SLC returns "a message indicating to route the call **to the IP address** retrieved from the Internet domain" (*Id*., 12:55–61 (emphasis added)), which is the IP address of the callee.

239. Additionally, *Kelly* teaches routing instructions that include an IP address of the callee to "initiate[] a direct point-to-point communication link with the callee." (EX1006 at 7:56–8:1.) "The connection/information server then transmits to the calling party an **information packet containing the IP address of the callee party**. Upon receipt of the located IP address from the connection server, the calling party's WebPhone **initiates a direct point-to-point communication link with the callee party by sending a call packet directly to the IP address of the callee party**." (*Id*. (emphasis added).) It would have been obvious to one of ordinary skill in the art to modify the SLC of *Nadeau* to include the callee IP address in the routing instructions as taught by *Kelly*.

240. One of ordinary skill in the art would be motivated to make this modification to route calls to the callee IP address. *Kelly* explains that including a callee's IP address in a routing message allows a call to be routed to the callee's IP address (EX1006 at 7:59–67), which is the same result desired by *Nadeau* (EX1005 at 12:59–61).

241. Furthermore, this modification is merely a combination of prior art elements (routing instructions of *Nadeau* and the callee IP address in *Kelly*) according to known methods (this modification merely requires programming the SLC to include the callee IP address (information that it already has (EX1005 at

169

10:3, 12:55–58) in the routing instructions) to yield predictable results (routing

instructions that include the callee IP address). Moreover, this modification is

merely the application of a known technique (including a callee IP address in a

routing message as taught by *Kelly*) to a known device (the SLC of *Nadeau*) ready

for improvement (this modification merely requires programming of the SLC) to

yield predictable results (the SLC will produce routing instructions that include the

callee IP address as taught by *Kelly*). Additionally, this modification is the use of a

known technique (including a callee IP address in a routing message as taught by

Kelly) to improve similar devices (*Nadeau* and *Kelly* both disclose call routing

systems) in the same way (allows routing to a callee IP address).

242. Additionally, it would have been obvious to try including the callee's

IP address in the routing instructions, as taught by *Kelly*, with a reasonable

expectation of success. *Nadeau* recognizes that routing instructions can be used to

route a call to a callee's IP address. (EX1005 at 7:5–9, 7:22–23, 11:27–28, 12:55–

61.) *Kelly* teaches that one way to achieve such routing is by including the callee's

IP address in the routing message. (EX1006 at 7:64–67.) One of ordinary skill in

the art could have pursued the teaching in *Kelly* with a reasonable expectation of

success (the result is a routing message that includes a callee IP address as taught

by *Kelly*) and without undue experimentation (this modification would merely require programming of the SLC).

243. Thus, *Nadeau-Kelly* teaches the SLC producing a private network routing message, such as routing instructions indicating that a call should be routed over an IP network, for receipt by a call controller, such as the DPFE and ACS Gateway, when the call is classified as a private network call, such as when the directory entry indicates that the call should be routed over an IP network. The routing instructions identify an address, on the private network, associated with the callee, such as the callee IP address.

7. Limitation 1f: "when the call is classified as a public network call, producing a public network routing message for receipt by the call controller, said public network routing message identifying a gateway to the public network"

244. *Nadeau-Kelly* teaches Limitation 1f.

245. When the VoIP call should be routed over the PSTN, the SLC produces routing instructions and sends those instructions to a DPFE and ACS Gateway. The routing instructions instruct the DPFE to route the call to an IP-PSTN Gateway.

246. The SLC generates and sends "routing instructions" to a DPFE or
Internet ACS. (EX1005 at 7:5–9, 7:22–23.) "The primary goal of the SLC 122 is
to provide the **DPFEs** with **call processing instructions**." (*Id*. at 7:22–23
(emphasis added).)

247. For an IP call, when the SLC determines that the call should be routed
over the PSTN, the routing instructions instruct the DPFE and Internet ACS
Gateway to route the call to an IP-PSTN Gateway, also referred to as a Gateway
Functional Element (GWFE). (*Id*. at 7:5–9, 8:39–42, 11:29–33.) "**Upon
reception of routing instructions** from the SLC through the GWFE, **the DPFE
will resume call processing according to the received instructions** and route the
incoming call directly to a Delivery Point FE or **to the IP/PSTN GWFE 124** if
needed." (*Id*. at 7:5–9 (emphasis added).) "[W]hen a call originating from one
network has to terminate on the other, the ACS system forwards the call **to a
PSTN/IP gateway for proper bridging**." (*Id*. at 11:27–33 (emphasis added); *see
also*, *id*. at 8:39–42 (the IP/PSTN gateway routes calls between network domains).)

248. As discussed in Limitation 1e, the DPFE and ACS Gateway form a
call controller.

249. Furthermore, although not explicitly stated in *Nadeau-Kelly*, the
PSTN is a public network because the general public can access or purchase access

to the PSTN, as discussed in the State of the Art. Therefore, the IP-PSTN Gateway

is a gateway to the public network because it is a gateway to the PSTN.

250. Although *Nadeau* does not explicitly state that the routing instructions

identify the IP-PSTN Gateway to which the call is routed, one of ordinary skill in

the art would know that the routing instructions must include such an identification

to complete the call.

251. The routing instructions must include an identifier for the destination

of the call in order for the DPFE to know where to route the call (e.g., to a callee IP

address or an IP-PSTN Gateway). The purpose of the routing instructions is to

instruct the DPFE and ACS Gateway where to route a call. (*Id*. at 7:1–9, 7:20–27,

12:59–61.) If the routing instructions did not include an identifier for the

destination, then the DPFE and ACS Gateway would not know where to route the

call based on the routing instructions, thus defeating the purpose of the routing

instructions. Therefore, the routing instructions must include an identifier of the

destination.

252. Because the destination is the IP-PSTN Gateway (*id*. at 7:5–9, 11:27–

31), some identifier for the IP-PSTN Gateway must be included in the routing

instructions. Because *Nadeau* discloses that routing is occurring in an IP network,

one of ordinary skill in the art would know that, an IP address is used to identify

the IP-PSTN Gateway.

253. Moreover, *Kelly* teaches a gateway selection process that includes the

IP address of the gateway in the routing instructions to "initiate a call session to

the IP address of the gateway." (EX1006 at 12:32–35, 12:55–57, 13:22–26.)

"**This last reference contains the IP address of the desired gateway** which is

then forwarded via Internet 220 and ISP 250 to WebPhone client 232 by name

server 254 in step 12." (*Id*. at 12:55–57; *see also*, 12:32–35 (gateway selection

process resolves the appropriate "IP address of a gateway").) "After step 12 of

FIG. 6, the **call packet** containing the entire telephone number domain name entry

'4001.997.561.1.carrier.com' is then sent to initiate a call session to the **IP address**

of the gateway, for example, gateway 218C, and the call is offered." (*Id*. at

13:22–26.) As discussed in Section XII.A, it would have been obvious to modify

the SLC of *Nadeau* to perform the gateway selection process taught in *Kelly*.

254. Therefore, the SLC of *Nadeau* as modified by *Kelly* produces a public

network routing message, such as routing instructions indicating that a call should

be routed to the IP-PSTN Gateway, for receipt by the call controller, such as the

DPFE and ACS Gateway, when the call is classified as a public network call, such

as when the directory entry in the caller profile indicates that the call should be

routed over the PSTN. The routing instructions identify a gateway to the public

network, such as by including the IP address of the IP-PSTN Gateway.

C. Claim 7: "The process of claim 1 further comprising formatting said callee identifier into a pre-defined digit format to produce a re-formatted callee identifier"

255. *Nadeau-Kelly* teaches Claim 7.

256. A caller can send a call request that includes the telephone number of

the callee. The SLC receives the dialed number. (EX1005 at 9:32–38.) "[T]he

user must...inform the system of the particular individual, listed in his/her

subscriber directory, to be reached, either by speaking a name (Voice-Activated

Dialling or VAD) or by **entering the DN or any other code uniquely identifying

the party to be called**." (*Id*. at 9:32–38 (emphasis added).)

257. *Nadeau* does not explicitly disclose formatting the dialed number into

a pre-defined digit format, but *Kelly* teaches a gateway selection process that

involves formatting a dialed number by "revers[ing] the number and append[ing]

[a] carrier's domain name" to produce a "hybrid telephone/domain name."

(EX1006 at 11:50–12:14.) "Upon receiving the desired telephone number the

WebPhone client **reverses the number and appends the carrier's domain name**

resulting in a **hybrid telephone/domain name** having the form '4001-997-561-

1.carrier.com'." (*Id*. at 11:50–12:14 (emphasis added); *see also*, *id*. at 12:15–13:60.)

258. As discussed in Section XII.A, it would have been obvious to modify the SLC of *Nadeau* to perform the gateway selection process taught in *Kelly*. Thus, the SLC of *Nadeau* as modified by *Kelly* formats a callee identifier, such as a dialed number, into a pre-defined digit format, such as by reversing the number and appending a carrier domain, to produce a re-formatted callee identifier, such as a hybrid telephone/domain name.

D.   Claim 27

259. Claim 27 recites a non-transitory computer readable medium storing codes for directing a processor to perform a method identical to the method recited in Claim 1. *Nadeau-Kelly* teaches that the SLC includes a non-transitory computer readable medium, such as a memory, storing codes, such as program elements, for directing a processor, such as a CPU, to perform the functions of the SLC. (EX1005 at 3:56–62, Figure 2.)
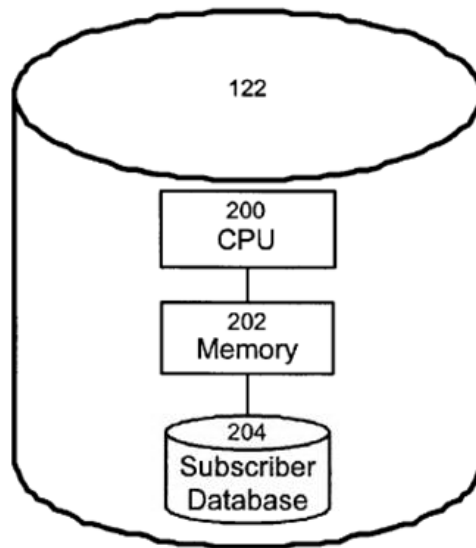
Figure 2

260. As discussed above for Claim 1, *Nadeau-Kelly* teaches that the SLC performs all the steps of the method recited in Claim 1. Thus, the analysis for the limitations of Claim 1 is cross-applicable to the limitations of Claim 27 and *Nadeau-Kelly* teaches this claim. *See* Limitations 1a–1f.

E.   Claim 54

261. Claim 54 is substantially similar to Claim 1. Limitations that appear separately in Claim 1 are combined in Claim 54. Thus, the analysis for Claim 1 is cross-applicable to Claim 54.

1. Preamble: "A process for operating a call routing controller to establish a call between a caller and a callee in a communication system"

262.   This preamble is substantially similar to the preamble of Claim 1. The only difference is that Claim 1 recites operating a call routing controller "to facilitate communication between callers and callees in a system" while this preamble recites operating a call routing controller "to establish a call between a caller and a callee in a communication system."

263.   To the extent this preamble is limiting, the disclosure in *Nadeau-Kelly* that teaches operating a call routing controller to facilitate communication between callers and callees in a system also teaches operating a call routing controller to establish a call between a caller and a callee in a communication system. *See* Claim 1 Preamble. One of ordinary skill in the art would understand the Service Logic **Controller** to be a controller. Additionally, *Nadeau-Kelly* explains that the primary goal of the SLC is to provide routing instructions to route a call. (EX1005 at 7:20–27.) Thus, one of ordinary skill in the art would understand that the SLC is a call routing controller. Thus, *Nadeau-Kelly* teaches this preamble.

2. Limitation 54a: "in response to initiation of a call by a calling subscriber, locating a caller dialing profile comprising a plurality of calling attributes associated with the caller"

264.   *Nadeau-Kelly* teaches Limitation 54a

265.   Limitations 1b and 54a both recite "locating a caller dialing profile comprising a plurality of calling attributes associated with the caller." Thus, *Nadeau-Kelly* teaches this portion of Limitation 54a as discussed for Limitation 1b.

266.   Additionally, the SLC locates a caller profile in response to the caller initiating a call.

> "1. The user connects to the Internet and **starts a VOIP client** modified to support this service. The user either **enters the name of the person to call, uses a Speed Dial entry, or speaks the name of the person to call** if the client is voice-enabled...
>
> 4. The ACS IP GWFE 116 reformats and **sends the query to the SLC 122**."

(EX1005 at 12:34–47 (emphasis added), 7:24–27, 9:55–64 (locating caller profile using caller's telephone number).)   "[T]he SLC 122 will **consult a particular caller's service profile**, consisting in service logic as well as a list of conditions and events to be used to process the caller's incoming calls." (*Id*. at 7:24–27.)

179

3. **Limitation 54b: "when at least one of said calling attributes and at least a portion of a callee identifier associated with the callee match and when the match meets a private network classification criterion, producing a private network routing message for receipt by a call controller, said private network routing message identifying an address, on a private network, the address being associated with the callee"**

267. Limitation 1c recites elements substantially similar to "when at least one of said calling attributes and at least a portion of a callee identifier associated with the callee match," as recited in Limitation 54b.

268. Limitations 1d recites elements substantially similar to "when the match meets a private network classification criterion," as recited in Limitation 54b.

269. Limitation 1e recites elements substantially similar to "producing a private network routing message for receipt by a call controller, said private network routing message identifying an address, on a private network, the address being associated with the callee," as recited in Limitation 54b.

270. Thus, the analysis for Limitations 1c, 1d, and 1e is cross-applicable to Limitation 54b and *Nadeau-Kelly* teaches Limitation 54b.

4. **Limitations 54c: "when at least one of said calling attributes and said at least said portion of said callee identifier associated with the callee match and when the match meets**

180

> **a public network classification criterion, producing a public
> network routing message for receipt by a call controller,
> said public network routing message identifying a gateway
> to a public network"**

271. Limitation 1c recites elements substantially similar to "when at least

one of said calling attributes and at least a portion of a callee identifier associated

with the callee match," as recited in Limitation 54c. Limitations 1d recites

elements substantially similar to "when the match meets a public network

classification criterion," as recited in Limitation 54c. Limitation 1f recites

elements substantially similar "producing a public network routing message for

receipt by a call controller, said public network routing message identifying a

gateway to a public network," as recited in Limitation 54c. Thus, the analysis for

Limitations 1c, 1d, and 1f is cross-applicable to Limitation 54c and *Nadeau-Kelly*

teaches Limitation 54c.

**F.   Claim 72: "The process of claim 54 further comprising causing
the private network routing message or the public network
routing message to be communicated to a call controller to effect
routing of the call"**

272. Claim 72 requires "causing the private network routing message or the

public network routing message to be communicated to a call controller to effect

routing of the call." As discussed for Limitations 1e and 1f, the SLC of *Nadeau* as

modified by *Kelly* sends routing instructions (private/public network routing

message) to a DPFE and ACS Gateway (collectively a call controller) to effect

routing of the call, whether the call is to be routed over an IP network or the PSTN.

Therefore, *Nadeau-Kelly* teaches this claim.

G.   Claim 73: "A non-transitory computer readable medium encoded with codes for directing a processor to execute the method of claim 54"

273.   *Nadeau-Kelly* teaches the SLC performing Claim 54. *See* Claim 54.

Furthermore, as explained for Claim 27, *Nadeau-Kelly* teaches the SLC including a

non-transitory computer readable medium encoded with codes for directing a

processor to perform the functions of the SLC. *See* Claim 27 Preamble. Thus,

Nadeau-Kelly teaches this claim.

H.   Claim 74

274.   Claim 74 recites an apparatus that performs substantially similar steps

to the steps recited in Claim 1. Thus, the analysis of Claim 1 is cross-applicable to

Claim 74.

1.   Preamble: "A call routing controller apparatus for establishing a call between a caller and a callee in a communication system"

275.   This preamble is substantially similar to the preamble of Claim 54.

Instead of reciting a process for operating a call routing controller like the

preamble of Claim 54, this preamble recites "a call routing controller apparatus."

To the extent this preamble is limiting, *Nadeau-Kelly* teaches this preamble

because it teaches a call routing controller apparatus, such as the SLC. *See* Claim

1 Preamble. One of ordinary skill in the art would understand the Service Logic

Controller to be a controller apparatus. Additionally, *Nadeau-Kelly* explains that

the primary goal of the SLC is to provide routing instructions to route a call.

(EX1005 at 7:20–27.) Thus, one of ordinary skill in the art would understand that

the SLC is a call routing controller apparatus.

2. Limitation 74a: "a processor operably configured to"

276. *Nadeau-Kelly* teaches Limitation 74a because it teaches that the SLC

includes a processor, such as a CPU. (EX1005 at 3:56–62 (disclosing CPU of

SLC).)
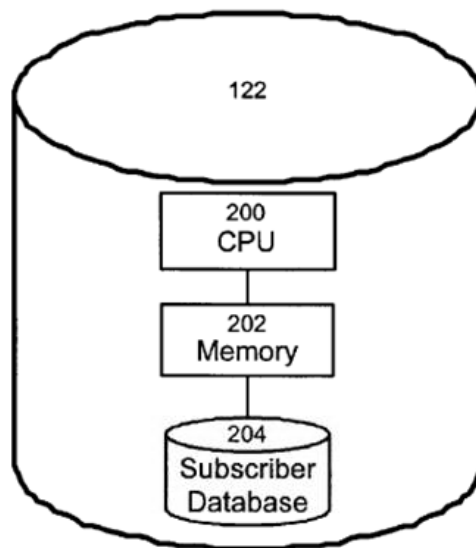
Figure 2

     3.   **Limitation 74b: "access a database of caller dialing profiles
wherein each dialing profile associates a plurality of calling
attributes with a respective subscriber, to locate a dialing
profile associated with the caller, in response to initiation of
a call by a calling subscriber"**

277.   *Nadeau-Kelly* teaches Limitation 74b.

278.   The caller profiles are stored in a "Subscriber Database." (EX1005 at
3:60–64.) "The SLC server further includes...a **database, referred to as the
Subscriber Database**, including a plurality of records, each record being a
subscriber or **user profile**." (*Id*. at 3:60–64 (emphasis added).)

279.   The SLC "access[es] the subscriber's database" to locate a profile for
a caller in response to a phone call being made. (*Id*. at 7:24–27, 9:55–64, 12:34–
49.) "[T]he SLC 122 will **consult a particular caller's service profile**, consisting
in service logic as well as a list of conditions and events to be used to process the
caller's incoming calls." (*Id*. at 7:24–27.) "The ACS system **uses the routing
information associated to a particular name in the subscriber's database** to
decide how to handle an outgoing call." (*Id*. at 11:13–15 (emphasis added).)

> 1. The user connects to the Internet and **starts a VOIP
> client** modified to support this service. The user either
> **enters the name of the person to call, uses a Speed
> Dial entry, or speaks the name of the person to call** if
> the client is voice-enabled.
>
> ...

> 4. The ACS IP GWFE 116 reformats and **sends the query to the SLC 122**.

> 5. The SLC 122 uses the received information to **access the subscriber's database**."

(*Id*. at 12:34–49 (emphasis added); *see also*, *id*. at 9:55–10:20 (showing example profile with calling attributes), 12:42–52 (disclosing example entry).) Thus, *Nadeau-Kelly* teaches that the SLC accesses a database, such as the Subscriber Database, of caller dialing profiles, such as the caller's service profile.

280. Limitation 1b recites elements substantially similar to "wherein each dialing profile associates a plurality of calling attributes with a respective subscriber," as recited in Limitation 74b. Thus, *Nadeau-Kelly* teaches this portion of Limitation 74b as discussed for Limitation 1b.

4. **Limitation 74c: "produce a private network routing message for receipt by a call controller, said private network routing message identifying an address, on a private network, through which the call is to be routed, when at least one of said calling attributes and at least a portion of a callee identifier associated with the callee match and when the match meets a private network classification criterion, the address being associated with the callee"**

281. Limitations 1e recites elements substantially similar to "produce a private network routing message for receipt by a call controller, said private network routing message identifying an address, on a private network,...the address being associated with the callee," as recited in Limitation 74c.

282. Limitation 1c recites elements substantially similar to "when at least one of said calling attributes and at least a portion of a callee identifier associated with the callee match," as recited in Limitation 74c.

283. Limitation 1d recites elements substantially similar to "when the match meets a private network classification criterion," as recited in Limitation 74c.

284. Thus, *Nadeau-Kelly* teaches these portions of Limitation 74c as discussed for Limitations 1c. 1d, and 1e.

285. Moreover, as discussed for Limitation 1e, one of ordinary skill in the art would know that the routing instructions produced by the SLC must include the callee IP address. Furthermore, as discussed for Limitation 1e, the SLC of *Nadeau* as modified by *Kelly* produces routing instructions that include the callee IP address. (EX1006 at 7:56–8:1.)

286. Furthermore, as I discussed in the State of the Art, one of ordinary skill in the art would know that an IP address generally includes two parts: (1) a first part that identifies a network and (2) a second part that identifies a node, host, or device. *See* ¶ 99 above. Generally, the first part identifies a network to which the node, host, or device identified by the second part is connected. One of

ordinary skill in the art would know that a message routed to the device would be

routed through the network to which the device is connected. Thus, because the

routing instructions include an IP address of the callee, the routing instructions

include an address, on the private network, through which the call is to be routed,

such as the part of the callee IP address that identifies the network to which the

callee's device, such as the callee's multimedia PC, is connected.

5.   Limitation 74d: "produce a public network routing message for receipt by a call controller, said public network routing message identifying a gateway to a public network, when at least one of said calling attributes and said at least said portion of said callee identifier associated with the callee match and when the match meets a public network classification criterion"

287.   Limitation 1f recites elements substantially similar to "produce a

public network routing message for receipt by a call controller, said public network

routing message identifying a gateway to a public network," from Limitation 74d.

288.   Limitation 1c recites elements substantially similar to "when at least

one of said calling attributes and said at least said portion of said callee identifier

associated with the callee match," from Limitation 74d.

289.   Limitation 1d recites elements substantially similar to "when the

match meets a public network classification criterion," from Limitation 74d.

290. Thus, *Nadeau-Kelly* teaches these portions of Limitation 74d as discussed for Limitations 1c, 1d, and 1f.

I. **Claim 92: "The apparatus of claim 74 wherein said processor is further operably configured to cause the private network routing message or the public network routing message to be communicated to a call controller to effect routing of the call"**

291. This claim recites a processor configured to perform the recited step in Claim 72. *Nadeau-Kelly* teaches a processor configured to perform the functions of the SLC. See Limitation 74a. *Nadeau-Kelly* also teaches the SLC performing the recited step in Claim 72. See Claim 72; see also Limitations 1e and 1f.

XIII. *NADEAU-KELLY-VAZIRI* RENDERS OBVIOUS CLAIMS 28, 34, 93, AND 111

A. **It was obvious to modify the service logic controller ("SLC") of *Nadeau-Kelly* to perform the prefix translation process taught by *Vaziri***

292. As discussed in Section XII.A and Limitations 1d, 1e, and 1f, it would have been obvious to modify the SLC of *Nadeau* with the teachings of *Kelly*. It would have been obvious to further modify the SLC of *Nadeau-Kelly* to perform the telephone number reformatting process taught by *Vaziri*.

293. *Vaziri* is from the same field of endeavor as *Nadeau* and *Kelly*. *Vaziri* is from the same technical field as *Nadeau and* Kelly—telecommunications systems, such as telephony systems (wired telephony, wireless telephony, IP

telephony, etc.). Like *Nadeau* and *Kelly*, *Vaziri* also addresses challenges arising from making VoIP calls. (EX1007 at 1:40–64.) Furthermore, *Vaziri* is also concerned with routing calls over an IP network or the PSTN, like *Nadeau* and *Kelly*. (*Id*. at 1:27–30, 1:35–39, 2:59–67, 3:7–10; EX1005 at 6:15–23; EX1006 at 2:42–51.) Therefore, one of ordinary skill in the art would have considered the teachings of *Vaziri* when implementing or improving *Nadeau-Kelly*.

294. As discussed in Section XII.A, *Nadeau-Kelly* teaches a SLC that routes VoIP calls based on entries in a caller profile. An entry for a callee may be located based on a telephone number dialed or provided by the caller. (EX1005 at 9:34–38, 9:66–10:2.) *Nadeau-Kelly* recognizes a desire for the SLC to handle calls over any number of disparate networks, such as the PSTN, mobile network, and Internet (*id*. at 3:44–55) from callers in different countries on different continents, such as Germany and the United States (EX1006 at 13:46–57).

295. Telephone numbers in different networks may have different addressing schemes. For example, there are networks that can process a local call even if the national or international dialing digits are included in the dialed number. On the other hand, some networks may not be able to process a local call if the caller includes a national dialing digit or international dialing digit in the dialed number. *See* ¶ 78 above. These different addressing schemes may affect

189

how a user dials a telephone number or builds his directory in the caller profile of

Nadeau-Kelly.

296. The SLC of *Nadeau-Kelly* does not reconcile different PSTN
addressing schemes. As a result, if the dialed telephone number for a callee
included digits such as international dialing digits (IDD) and national dialing digits
(NDD) but the telephone number in the callee's entry did not include an IDD or
NDD, then the callee's entry may not be located and the call may be improperly
routed. For example, if a caller called the number 1-234-567-8910 but entry for
the desired callee in the caller profile lists the telephone number for the callee as
234-567-8910 or 567-8910, then the SLC would not locate the callee's entry.
Thus, improper routing of the call may occur, thereby increasing costs.

297. One of ordinary skill in the art would be motivated to improve the
SLC of *Nadeau-Kelly* by modifying it to perform the telephone number
reformatting process taught in Figure 12 of *Vaziri*. The reformatting process
involves two steps: (1) determining that a dialed telephone number includes
international dialing digits (IDD) and national dialing digits (NDD) that match an
IDD and NDD in a caller profile and (2) removing the matching IDD and NDD
from the dialed number to conform the number to a predefined format (e.g.,
Country Code+City Code+Number). (EX1007 at 29:25–36, Figure 12.) *Vaziri*

teaches that performing this reformatting process "allows all units to access other units...regardless of that network's underlying PSTN addressing format." (*Id*. at 29:33–36.) The SLC can then use the formatted telephone number to locate the callee entry regardless of the PSTN addressing scheme of the caller. Using the previous example, the reformatting process could strip out the '1' from 1-234-567-8910 to produce 234-567-8910, which could match an entry in *Nadeau*'s subscriber database with the telephone number 234-567-8910.
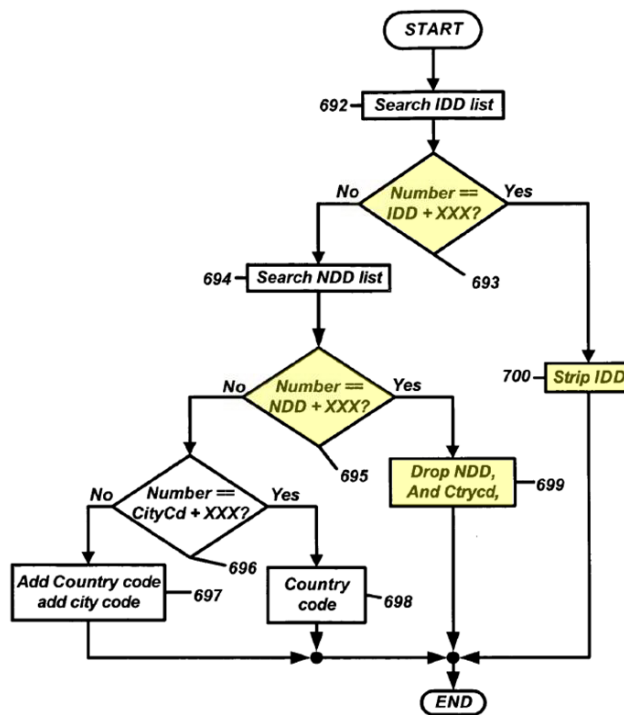
Figure 12

298. Additionally, one of ordinary skill in the art could easily modify the SLC of *Nadeau-Kelly* to perform the reformatting process taught by *Vaziri*. This

modification is merely a combination of prior art elements (SLC of *Nadeau-Kelly* and the reformatting process of *Vaziri*) according to known methods (this modification would require nothing beyond programming the SLC to perform basic computer operations such as (1) comparing dialed IDDs and NDDs with IDDs and NDDs in a subscriber's service profile and (2) removing IDDs and NDDs from dialed numbers) to yield predictable results (*Vaziri* teaches the result: a number with IDD or NDD stripped out that can reconcile different PSTN addressing schemes (EX1007 at 29:33–36)). Furthermore, this modification involves the application of a known technique (reformatting process of *Vaziri*) to a known device (the SLC of *Nadeau-Kelly*) ready for improvement (this modification would require nothing beyond programming the SLC to perform basic computer operations such as (1) including the IDD and the NDD in a subscriber's service profile; (2) comparing dialed IDDs and NDDs with IDDs and NDDs in the subscriber's service profile; and (3) removing IDDs and NDDs from dialed numbers to yield predictable results (*Vaziri* teaches the result: a number with IDD or NDD stripped out that can reconcile different PSTN addressing schemes (EX1007 at 29:33–36)). Additionally, this modification is the use of a known technique (reformatting process of *Vaziri*) to improve similar devices (*Nadeau* and *Kelly* both disclose call routing systems) in the same way (a number with IDD or NDD stripped out that can reconcile different PSTN addressing

192

schemes). Moreover, it was obvious to modify the caller profile in *Nadeau-Kelly*

to include a caller's IDD and NDD as taught by *Vaziri*. Both *Nadeau-Kelly* and

Vaziri teach the use of profiles for storing caller information such as a caller's

home telephone number and a caller's IDD and NDD. (EX1005 at 3:56–4:6, 9:55–

65 (caller's "home telephone number"); EX1007 at 29:25–36, Figure 12 blocks

692 and 694 (the caller's "IDD list" and "NDD list").) Both *Nadeau-Kelly* and

Vaziri use their profiles to process calls. (EX1005 at 7:20–40; EX1007 at 30:57–

67.) *Nadeau-Kelly* recognizes that its description of a profile is "non-exhaustive

and could contain other elements." (EX1005 at 10:21–22.) *Vaziri* teaches that

including the caller's IDD and NDD in the profile allows for the prefix translation

process to be performed, which allows the system to reconcile different PSTN

addressing schemes. (EX1007 at 29:25–36.) Additionally, this modification

would require nothing beyond adding the caller's IDD and NDD to the caller's

profile as taught by *Vaziri*. Thus, one of ordinary skill in the art was motivated to

make this modification, which is merely a combination of prior art elements (the

caller's home telephone number provided in *Nadeau-Kelly* and the IDD and NDD

in *Vaziri*) according to known methods (this modification would require nothing

beyond the simple task of adding the IDD and NDD to the caller's profile) to yield

predictable results (*Vaziri* teaches the result: a profile with an IDD and NDD).

299. Therefore, it would have been obvious to modify the SLC of *Nadeau-Kelly* to perform the reformatting process taught in *Vaziri*.

B.   Claim 28

300. The elements of Claim 28 are substantially similar to the elements of Claim 1 even though Claim 28 is a means-plus-function claim. Thus, Claim 1 is cross-applicable to Claim 28 including the motivations to combine *Nadeau* and *Kelly* discussed in Section XII.A and in Limitations 1d, 1e, and 1f.

1.   Preamble: "A call routing apparatus for facilitating communications between callers and callees in a system comprising a plurality of nodes with which callers and callees are associated"

301. This preamble is substantially similar to the preamble of Claim 1. Instead of reciting a process for operating a call routing controller like Claim 1, this claim recites a call routing apparatus that performs the process of Claim 1. As explained above for Claim 1, the SLC of *Nadeau* as modified by *Kelly* performs every step of Claim 1. Further modifying the SLC of *Nadeau* to perform the prefix translation algorithm taught in *Vaziri* does not change that fact. Therefore, to the extent this preamble is limiting, *Nadeau-Kelly-Vaziri* teaches a call routing apparatus, such as the SLC, which facilitates communications between callers and callees. *See* Claim 1 Preamble. Thus, *Nadeau-Kelly-Vaziri* teaches this preamble for substantially the same reasons discussed in Claim 1 Preamble. One of ordinary

skill in the art would understand the Service Logic **Controller** to be an apparatus.

Additionally, *Nadeau-Kelly* explains that the primary goal of the SLC is to provide

routing instructions to route a call. (EX1005 at 7:20–27.) Thus, one of ordinary

skill in the art would understand that the SLC is a call routing apparatus.

>   **2.   Limitation 28a: "receiving means for receiving a caller
>   identifier and a callee identifier, in response to initiation of
>   a call by a calling subscriber"**

302. I have been informed that this term is governed by 35 U.S.C. § 112,

Paragraph 6. I have been instructed to provide my opinion for this term using the

structure "an I/O port" (an input/output port). I have not formed an opinion as to

whether this structure is corresponding structure or whether the specification

discloses corresponding structure for this term.

303. *Nadeau-Kelly-Vaziri* teaches Limitation 28a.

304. The SLC is a server that connects with a PSTN network and IP

network through connection points. (EX1005 at 2:49–3:28, 7:30–31,8:7–38,

11:38–12:18, 12:32–66.) "The SLC 122 is the system component which is actually

responsive to the events occurring within the different networks, and can be

implemented on any suitable **server that connects to the different domain**

gateways 108 and 116." (*Id*. at 7:27–31 (emphasis added).) "In a specific

embodiment of this invention, **the SLC connects with three independent**

network domains, namely the **PSTN, a mobile telephone network and the**

Internet.” (*Id*. at 3:44–46 (emphasis added).)

> [T]he invention provides a **service logic controller** for the management of communication sessions originating in either one of a telecommunications network and the Internet, said service logic controller including:
>
> ...
>
> **a first connection point** permitting to exchange data between said service logic controller and the telecommunications network;
>
> **a second connection point** permitting to exchange data with the Internet.”

(*Id*. at 2:49–3:28 (emphasis added).)

305.   Furthermore, the SLC performs call routing based on whether or not

“all local ports” are in use. (*Id.* at 6:19–26; *see also*, *id*. at 8:7–38, 11:38–12:18,

12:32–66 (disclosing the SLC sending and receiving messages).)

306.   *Nadeau-Kelly-Vaziri* does not explicitly state that the “connection

points” or I/O ports, but it is apparent that they are. As discussed in the State of

the Art, every network device that supports the TCP/IP protocol suite must have a

physical network interface (i.e., an Input/Output port) for transmitting and

receiving IP data. *See* ¶¶ 92–93, 107 above. An example Input/Output port is an

Ethernet physical interface. Thus, because *Nadeau* discloses that the SLC is a

"server" that "connects" to different gateways through "connection point[s]," one
of ordinary skill in the art would understand that these "connection point[s]" are or
include Input/Output ports.   (EX1005 at 2:49–3:28, 7:30–31, 8:7–38, 11:38–
12:18,12:32–66.)
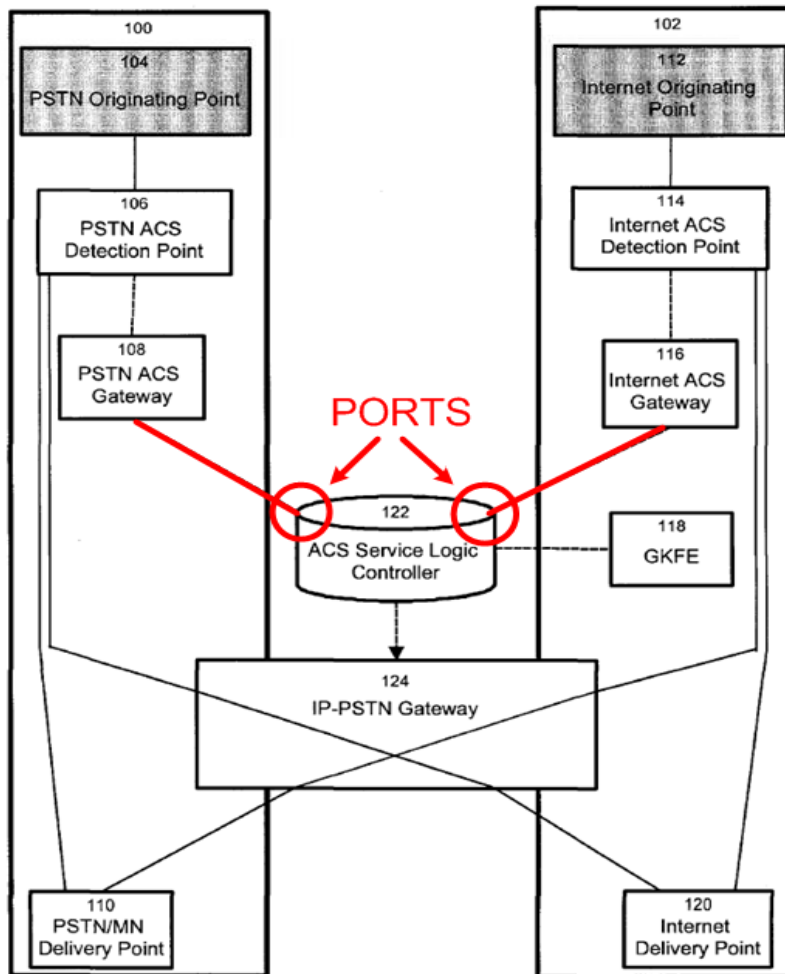
307.   Therefore, *Nadeau-Kelly-Vaziri* teaches that the SLC includes an I/O
port.

> **3. Limitation 28b: "means for locating a caller dialing profile comprising a username associated with the caller and a plurality of calling attributes associated with the caller"**

308. I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my opinion for this term using the structure "a processor programmed to implement the algorithm illustrated in block 254 of Figure 8A." I have not formed an opinion as to whether this structure is corresponding structure or whether the specification discloses corresponding structure for this term.

309. Block 254 recites "Use caller field to get dialing profile for caller from database." (EX1001 at Figure 8A.)

310. *Nadeau-Kelly-Vaziri* teaches Limitation 28b.

311. The SLC includes a memory and CPU programmed to perform the functions of the SLC. (*See id*. at 3:56–61 (disclosing the SLC including a memory and CPU).) Therefore, the SLC includes a processor circuit, such as a CPU and memory.
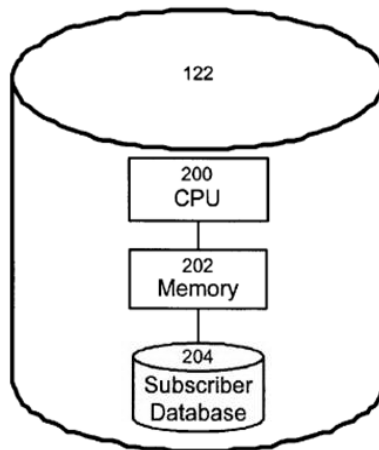
Figure 2

312.   The SLC also includes a "Subscriber Database" of subscriber profiles.
(*Id*. at 3:61–65.) When a call is made, the SLC gets the caller's subscriber profile
to process the call. (*Id*. at 7:24–27, 11:13–15.) To locate the profile, the SLC uses
caller identification information, such as "the home phone directory number...to
automatically associate calls made to the service from the subscriber's main
directory number." (*Id*. at 9:61–64.) "[T]he SLC 122 will **consult a particular
caller's service profile**, consisting in service logic as well as a list of conditions
and events to be used to process the caller's incoming calls." (*Id*. at 7:24–27.)
"The ACS system **uses the routing information associated to a particular name
in the subscriber's database** to decide how to handle an outgoing call." (*Id*. at
11:13–15 (emphasis added).)

> The Subscriber Database 204 as shown in FIG. 2
> contains a **record for each such subscriber**, where this

199

> record includes an information element formed of
> multiple fields, each containing specific information,
> such as:
>
> ...
>
> the **home phone directory number** (if different from the
> subscriber ID) **to automatically associate calls made to
> the service from the subscriber's main directory
> number**."

(*Id*. at 9:55–64 (emphasis added).) Thus, the SLC uses a caller field, such as a

subscriber phone number, to get a dialing profile for a caller from a database

(**block 254**).

313. Therefore, *Nadeau-Kelly-Vaziri* teaches this limitation.

**4.   Limitation 28c: "means for determining a match when at
least one of said calling attributes matches at least a portion
of said callee identifier"**

314. I have been informed that this term is governed by 35 U.S.C. § 112,

Paragraph 6. I have been instructed to provide my opinion for this term using the

structure "a processor programmed to implement one or more of the algorithms

illustrated in blocks 257, 380, 382, 390, and 396 of Figure 8B." I have not formed

an opinion as to whether this structure is corresponding structure or whether the

specification discloses corresponding structure for this term. These steps are

shown below. (EX1001 at Figure 8B.)

FIG. 8B

315. *Nadeau-Kelly-Vaziri* discloses Limitation 28c at least because it teaches a processor programmed to implement blocks 257 and 380. Block 257 recites "Callee identifier begins with caller IDD?" (*Id.*) Block 380 recites "Callee identifier begins with caller NDD?" (*Id.*)

316. As discussed for Limitation 28b, the SLC includes a processor, such as a CPU, programmed to perform the functions of the SLC.

317. The SLC of *Nadeau* as modified by *Kelly* and *Vaziri* performs a telephone number reformatting process in which the SLC compares a dialed number with the caller's IDD (international dialing digits) or NDD (national

dialing digits). (EX1007 at 29:29–36, Figure 12 blocks 693 and 695.) "The

scheme is as follows Country Code+City Code+User Telephone Number. The

MNES Bridge will have this information plus the **users IDD and NDD and will**

process all attempted VoIP calls to format 692 . . . 700 the dialed number into

Country Code+City Code+Number." (EX1007 at 29:25–36 (emphasis added).)

If the caller's IDD or NDD matches the callee's IDD or NDD, then the callee's

IDD or NDD is removed. (*Id*. at Figure 12 blocks 699 and 700.)
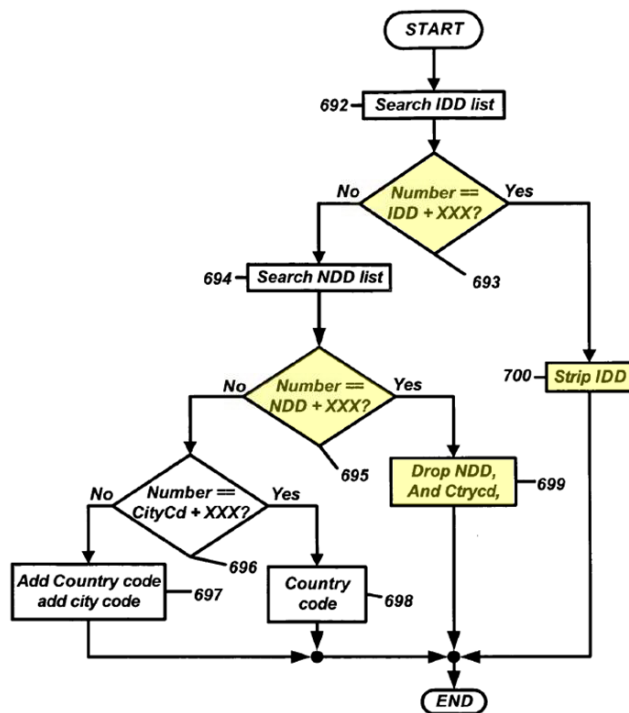
Figure 12

318. As discussed in Section XIII.A, it would have been obvious to modify the SLC of *Nadeau-Kelly* to perform the telephone number reformatting process taught by *Vaziri*.

319. Thus, the modified SLC compares a callee's telephone number provided in a subscriber's originating call request with the IDD and NDD in a caller's profile (**blocks 257 and 380**).

320. Therefore, *Nadeau-Kelly-Vaziri* teaches this limitation.

5. Limitation 28d: "means for classifying the call as a public network call when said match meets public network classification criteria"

321. I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my opinion for this term using two alternative structures "a processor programmed to implement one or more branches of the algorithm illustrated in Figure 8B that leads to the end of block 408" and "a processor programmed to implement one or more branches of the algorithm illustrated in Figure 8B that leads to the end of block 410." I have not formed an opinion as to whether any of these structures is corresponding structure or whether the specification discloses corresponding structure for this term. These steps are shown below. (EX1001 at Figure 8B.)
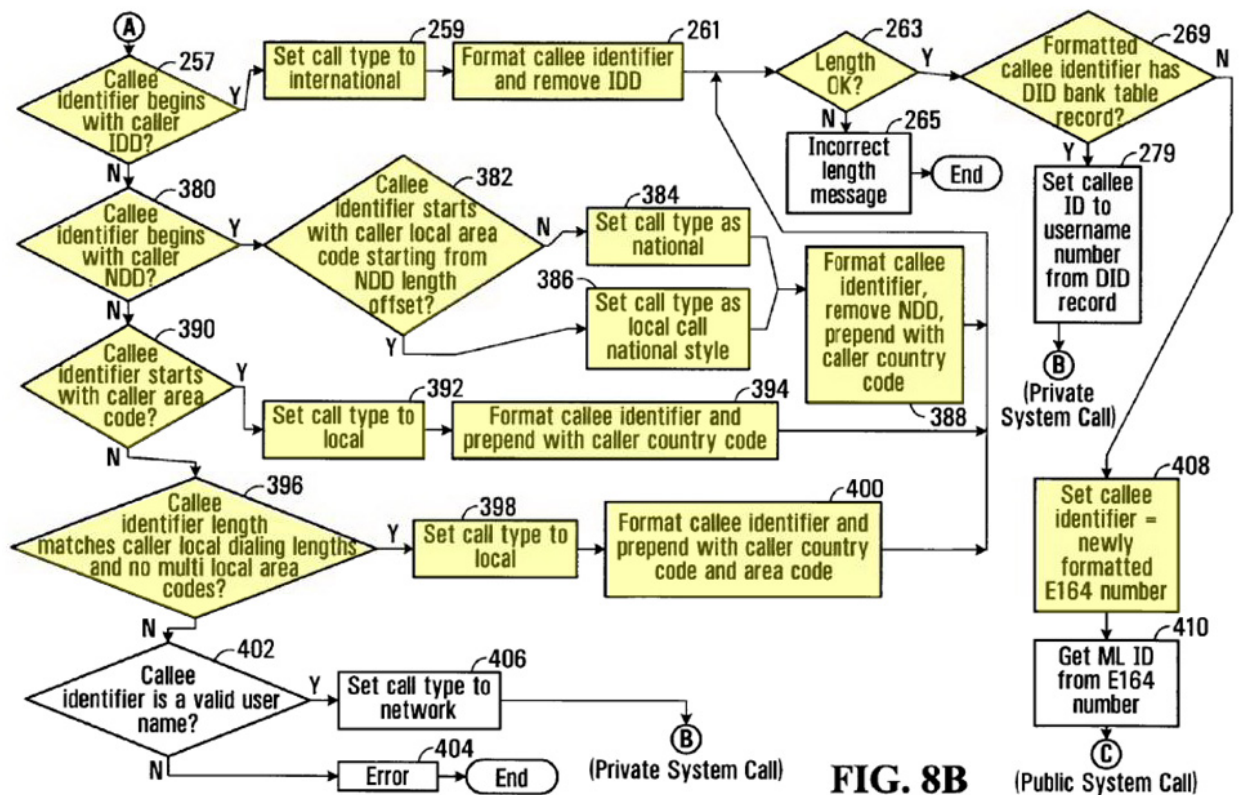
FIG. 8B

322. *Nadeau-Kelly-Vaziri* teaches Limitation 28d under either of these structures because it teaches a processor programmed to implement at least blocks 257, 259, 261, 263, 269, 408, and 410.

323. As discussed for Limitation 28b, the SLC includes a processor, such as a CPU, that performs the functions of the SLC.

324. Also, as discussed for Limitation 28c, the SLC as modified by *Kelly* and *Vaziri* performs a telephone number reformatting process in which the SLC compares a dialed telephone number with an IDD in a caller profile (**block 257**).

325. The IDD is a prefix identifying an international call. (EX1007 at 28:60–29:24.) "The **IDD prefix** is the **international prefix** needed to dial a call FROM the country listed TO another country." (*Id*. at 28:66–67 (emphasis added).) Thus, the modified SLC sets a call type to international (**block 259**).

326. As part of the reformatting process, the modified SLC strips the IDD from the dialed telephone number if it matches the caller's IDD in the caller's profile. (*Id*. at 29:28–36, Figure 12 block 700.) "The scheme is as follows **Country Code+City Code+User Telephone Number**. The MNES Bridge will have this information plus the **users IDD and NDD and will process all attempted VoIP calls to format 692 . . . 700 the dialed number into Country Code+City Code+Number**." (*Id*. at 29:25–36 (emphasis added).)

START

692 — Search IDD list

No — Number ==
IDD + XXX? — Yes

693

694 — Search NDD list

700 — Strip IDD

No — Number ==
NDD + XXX? — Yes

695

Drop NDD,
And Ctrycd, — 699

No — Number ==
CityCd + XXX? — Yes

696

Add Country code
add city code — 697

Country
code — 698

END
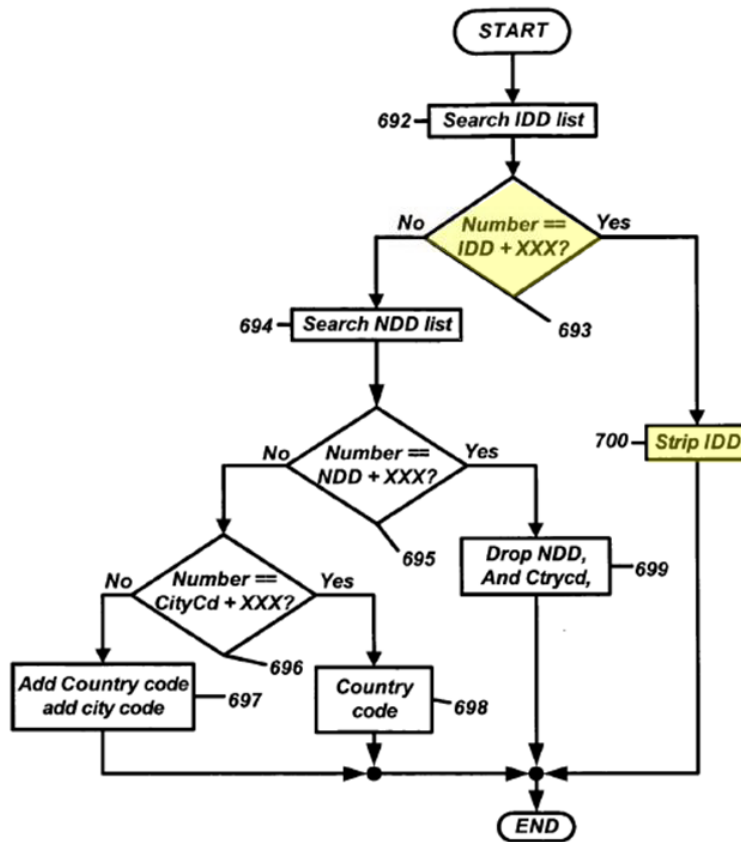
Figure 12

(*Id*. at Figure 12.) Block 261 in Figure 8B of the '815 Patent states, "Format callee

identifier and remove IDD." (EX1001 at Figure 8B.) However, the specification

of the '815 Patent explains that block 261 is met simply when the IDD is removed.

"[B]lock 261 directs the processor to produce a reformatted callee identifier by

reformatting the callee identifier into a predefined digit format. In this

embodiment, this is done by removing the pattern of digits matching the IDD field

contents 264 of the caller dialing profile to effectively shorten the callee

identifier." (EX1001 at 19:28–63.) In other words, no additional formatting of the

206

dialed number is necessary to perform block 261. Thus, the modified SLC

performs **block 261** when it removes an IDD from the dialed number if the

removed IDD matches the caller's IDD. (EX1007 at Figure 12, block 700.)

327. As part of the telephone number reformatting process, the dialed

number is formatted to conform to a predefined format of a certain length (e.g.,

country code + city code + telephone number). (*Id*. at 29:25–32.) Thus, the

modified SLC validates the length of a formatted number (**block 263**).

328. The SLC can determine that a callee does not have an entry in the

caller profile. (EX1005 at 11:13–20.) For a PSTN call, if the callee does not have

an entry in the caller's subscriber profile, the SLC completes the call over the

PSTN. (*Id*. at 11:17.) For an IP call, if there is no entry for the callee in the

caller's subscriber profile, the SLC completes the call over the PSTN if an IP

address of the callee is not available. (*Id*. at 11:18–20.)

> **If no routing information is available**, the system uses
> a default routing algorithm:
>
> For PSTN-originated calls: complete the call on the
> PSTN.
>
> For IP-originated calls:
>
> complete the call on IP if an address is available;
>
> **complete the call on the PSTN** through a gateway.

(*Id*. at 11:15–20 (emphasis added).) Thus, the SLC determines that a callee identifier, such as a dialed telephone number, does not have a DID bank table record, such as an entry in the caller's subscriber profile (**block 269**).

329. As part of the telephone number reformatting process, the modified SLC formats the dialed number to be E.164 compatible (e.g., country code + city code + telephone number). (EX1007 at 29:25–32.) Thus, the modified SLC sets a callee identifier, such as a dialed telephone number, to be compatible with the E.164 standard (**block 408**).

330. Therefore, *Nadeau-Kelly-Vaziri* teaches this limitation under the first structure because it teaches a processor programmed to implement blocks 257, 259, 261, 263, 269, and 408.

331. *Kelly* teaches a gateway selection process that generates a hybrid telephone/domain name from an E.164 number and then resolves an IP address of a carrier gateway. (EX1006 at 11:54–59, 12:7–11, 12:32–35.) The process involves using successive portions of the hybrid (e.g., 4001.997.561.1.carrier.com) to retrieve successive references to different name servers. (*Id*. at 12:35–54.) The successive portions can be ".com," "carrier.com," and so on. *Id*. The last reference returned "contains the IP address of the desired gateway which is then forwarded via the Internet and ISP." (*Id*. at 12:55–57.)

> A user enters a **destination telephone number** consisting of **country code, area code, exchange and subscriber number** segment or data, for example **'1-561-997-4001'**, into the WebPhone client utilizing either the WebPhone virtual keypad or computer keyboard.

(*Id*. at 11:54–59 (emphasis added).)

> Upon receiving the desired telephone number the WebPhone client reverses the number and appends the carrier's domain name resulting in a **hybrid telephone/domain name** having the form **'4001-997-561-1.carrier.com'**.

(*Id*. at 12:7–11 (emphasis added).)

> Referring to FIG. 6, a **recursive process of resolving** the telephone number domain name previously entered into the WebPhone client to **the appropriate IP address of a gateway on a PSTN** is illustrated conceptually: In step 1, the WebPhone client 232 forwards the telephone number domain name to primary name server 254 in packetized form via Internet 220 and ISP 250. Using a name packet, primary name server 254 queries the root name server of the domain name system (DNS) for the address of **'4001.997.561.1.carrier.com'** in step 2. The name server for the DNS root returns **a reference to the name server for '.com'** in step 3...**This last reference contains the IP address of the desired gateway** which is then forwarded via Internet 220 and ISP 250 to WebPhone client 232 by name server 254 in step 12."

(*Id*. at 12:32–57 (emphasis added); *see also*, *id*. at 13:22–26 (disclosing call packet

to initiate a call to IP address of gateway).)

332.   Block 410 of Figure 8D of the '815 Patent states "Get ML ID from

E164 number." (EX1001 at Figure 8B.) The specification of the '815 Patent

209

explains that an "ML ID" is an identifier in a record located using portions of a
dialed E.164 number. (EX1001 at 23:40–50.) *Kelly* teaches a gateway selection
process where portions of an E.164 number are used to retrieve successive
references that identify name servers. (EX1006 at 11:50–12:57.) For example, a
caller dials the number "1-561-997-4001." (*Id*. at 11:54–59.) The number is then
reversed and a carrier domain name is appended to the reversed number to produce
"4001-997-561-1.carrier.com." (*Id*. at 12:7–15.) Portions of the number are then
used to retrieve references that identify name servers to resolve an IP address of a
carrier gateway. (*Id*. at 12:32–57.)

333. As discussed in Section XII.A, it would have been obvious to modify
the SLC of *Nadeau* to perform the gateway selection process taught in *Kelly*.
Thus, the SLC of *Nadeau* as modified by *Kelly* and *Vaziri* retrieves an ML ID
(identifier for a name server in a reference) from a dialed E.164 number (**block
410**).

334. Therefore, *Nadeau-Kelly-Vaziri* teaches this limitation under the
second structure because it teaches a processor programmed to implement blocks
257, 259, 261, 263, 269, 408, 410.

335. Furthermore, *Nadeau-Kelly-Vaziri* teaches a structure equivalent to a
processor programmed to implement blocks 257, 259, 261, 263, 269, 408, 410.

Generally, this algorithm performs three steps to prepare a call to be routed over the PSTN: (1) remove an IDD from the dialed number if it matches an IDD in a caller profile (blocks 257, 259, 261, 263); (2) determine that the formatted called number does not have a corresponding record in the system (block 269); (3) prepare for PSTN routing (blocks 408 and 410).

336. *Nadeau* teaches the SLC including a processor to perform the functions of the SLC. (EX1005 at 7:34–40.) *Vaziri* teaches removing an IDD from a dialed number if it matches an IDD in a caller profile to produce a formatted number (Country Code + City Code + Number). (EX1007 at 29:25–36, Figure 12.) *Nadeau* teaches the SLC determining that the number does not have a corresponding record in the caller profile. (EX1005 at 11:13–20.) *Vaziri* and *Kelly* teach preparing for PSTN routing because *Vaziri* teaches formatting the number to an E.164 number (EX1007 at 29:25–36, Figure 12) and *Kelly* teaches selecting a carrier and gateway to route the call (EX1006 at 11:50–12:67, 13:39–57.) As discussed in Sections XII.A and XIII.A, it would have been obvious to modify the SLC of *Nadeau* to perform the functions taught in *Kelly* and *Vaziri*.

337. Thus, *Nadeau-Kelly-Vaziri* discloses a processor that performs the recited function in substantially the same way as disclosed in the '815 Patent to

produce substantially the same result of a call that is prepared to be routed over the

PSTN. Therefore, *Nadeau-Kelly-Vaziri* teaches an equivalent structure.

6.   Limitation 28e: "means for classifying the call as a private network call when said match meets private network classification criteria"

338.   I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my opinion for this term using the structure "a processor programmed to implement one or more branches of the algorithm illustrated in Figure 8B that leads to the end of block 406 or block 279." I have not formed an opinion as to whether this structure is corresponding structure or whether the specification discloses corresponding structure for this term. These steps are shown below. (EX1001 at Figure 8B.)
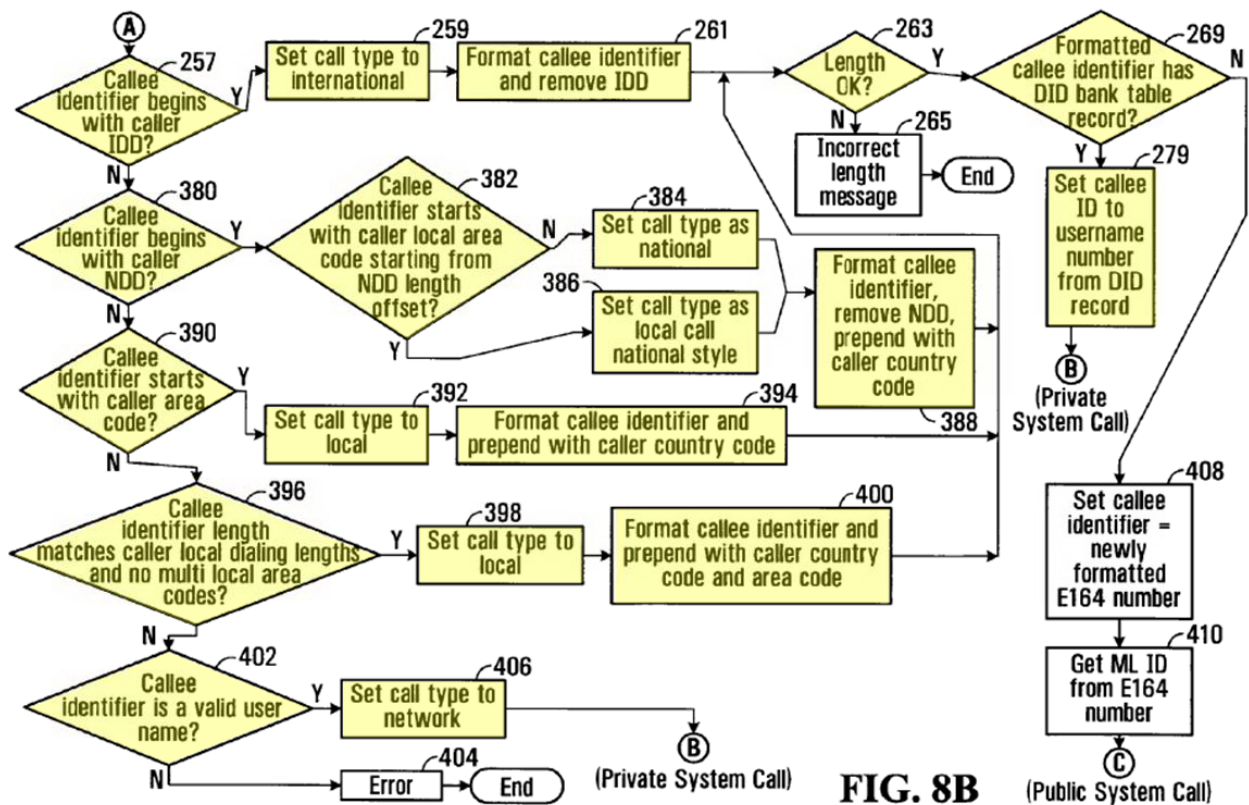
FIG. 8B

339. *Nadeau-Kelly-Vaziri* teaches Limitation 28e at least because it teaches a processor programmed to perform blocks 257, 259, 261, 263, 269, and 279.

340. As discussed for Limitation 28d, the SLC of *Nadeau* modified by *Kelly* and *Vaziri* processor performs at least blocks 257, 259, 261, and 263 of this algorithm, which results in a formatted callee identifier, such as a formatted telephone number.

341. The SLC can determine that a caller profile includes an entry for a particular callee based on the formatted callee identifier. A caller provides the

directory number of the callee to initiate a call with the callee. (EX1005 at 9:32–

40.) This directory number can be formatted to produce a formatted directory

number. *See* Limitation 28d. The formatted directory number can then be used to

determine whether there is an entry in the caller profile for a callee with that

directory number. (*Id*. at 9:66–10:2.)

> the directory itself which contains multiple entries, each
> entry including:
>
> name of the person, e.g. John Smith;
>
> **directory number**"

(*Id*. at 9:66–10:2 (emphasis added).) Therefore, the SLC can determine that a

formatted callee identifier, such as the callee's formatted telephone number, has a

DID bank table record, such as an entry in a caller profile (**block 269**).

342. The entry in the profile can include an IP address of the callee. (*Id*. at

9:55–10:3.)

> the directory itself which contains multiple entries, each
> entry including:...
>
> **IP address**...
>
> routing information;
>
> time of day routing;
>
> day of week routing;
>
> **least cost routing, such as:**

complete to VoIP if IP address available.”

(*Id*. at 9:55–10:20 (emphasis added).) The SLC can complete the call to that IP

address rather than to the formatted directory number. (*Id*. at 10:12, 12:59–61.)

> 8. The SLC 122 returns to the Internet **ACS GWFE 116**
> a **message** indicating to **route the call to the IP address**
> retrieved from the Internet domain.”

(*Id*. at 12:59–61 (emphasis added).) Thus, to complete the call, the SLC sets the

callee ID, such as the formatted directory number, to a username number, such as

the IP address, from the DID record, such as the entry in the profile (**block 279**).

343. Therefore, *Nadeau-Kelly-Vaziri* teaches this limitation.

7.   Limitation 28f: “means for producing a private network routing message for receipt by a call controller, when the call is classified as a private network call, said private network routing message identifying an address, on the private network, associated with the callee”

344. I have been informed that this term is governed by 35 U.S.C. § 112,

Paragraph 6. I have been instructed to provide my opinion for this term using two

alternative structures “a processor programmed to (i) produce a routing message

identifying an address on the private network with which the callee identified by

the contents of the callee ID buffer is associated OR (ii) implement the algorithm

illustrated in block 644 of Figure 8C” and “a processor programmed to implement

cell 350 of Figure 8A or cell 644 of Figure 8C.” I have not formed an opinion as

to whether any of these structures is corresponding structure or whether the specification discloses corresponding structure for this term.

(i) First Structure

345.   *Nadeau-Kelly-Vaziri* teaches this structure at least because it teaches a processor programmed to produce a routing message identifying an address on the private network with which the callee identified by the contents of the callee ID buffer is associated.

346.   As discussed for Limitation 28b, *Nadeau-Kelly-Vaziri* teaches a processor, such as the CPU, that performs the functions of the SLC.

347.   For an IP call, when the SLC determines that the call should be routed over the IP network, the routing instructions instruct the DPFE to route the call to an IP address of the callee. (EX1005 at 12:55–61.) "The primary goal of the SLC 122 is to provide the **DPFEs** with **call processing instructions**." (*Id*. at 7:22–23 (emphasis added).)   "**Upon reception of routing instructions** from the SLC through the GWFE, **the DPFE will resume call processing according to the received instructions** and route the incoming call **directly to a Delivery Point FE** or to the IP/PSTN GWFE 124 if needed." (*Id*. at 7:5–9.) "When a call stays inside the PSTN/Mobile or **IP network**, the call is **delivered directly to the called party terminal**." (*Id*. at 11:27–28 (emphasis added).)

7. The IP GKFE 118 returns to the SLC 122 **the IP
address** corresponding to this pseudo-address indicating
that **this person is currently connected to the Internet
and ready to receive VoIP calls**.

8. The SLC 122 returns to the Internet **ACS GWFE 116**
a **message** indicating to **route the call to the IP address**
retrieved from the Internet domain.

(*Id*. at 12:55–61 (emphasis added).)

348.   The callee is identified by a name or telephone number provided by

the caller. (*Id*. at 9:32–38.)

"In order to access the ACS system from a phone, the
user must dial into the system, using either a dedicated
DN or feature code, and inform the system of the
particular individual, listed in his/her subscriber
directory, to be reached, either by speaking **a name
(Voice-Activated Dialling or VAD)** or by entering **the
DN or any other code uniquely identifying the party
to be called**."

(*Id*. at 9:32–38 (emphasis added).)

In terms of the ACS service itself, an **ACS subscriber
first builds a directory of the individuals he/she
wishes to be able to reach**, prior to using the ACS
system. The directory must include some **routing
information for each entry, such as the individual's
directory number (DN) for the PSTN and an IP
address or pseudo-address for the Internet**.

(*Id*. at 9:18–23 (emphasis added).) Thus, the SLC produces a routing message,

such as routing instructions, identifying an address on the private network, such as

the callee's IP address, with which the callee identified by the contents of the

callee ID buffer, such as the name or telephone number provided by the caller, is
associated.

349. As discussed for Limitation 1e, one of ordinary skill in the art would
know that the routing instructions produced by the SLC must include the callee IP
address.

350. Moreover, as discussed for Limitation 1e, the SLC of *Nadeau* as
modified by *Kelly* produces routing instructions that include the callee IP address.
"The connection/information server then transmits to the calling party an
information packet containing the IP address of the callee party. Upon receipt
of the located IP address from the connection server, the calling party's WebPhone
**initiates a direct point-to-point communication link with the callee party by
sending a call packet directly to the IP address of the callee party**." (EX1006
at 7:56–8:1.)

351. Thus, *Nadeau-Kelly-Vaziri* teaches Limitation 28f under the first
structure.

(ii) Second Structure

352. The alternative structure is "a processor programmed to implement cell 350 of Figure 8A or cell 644 of Figure 8C" These steps are shown below. (EX1001 at Figures 8A, 8C.)

FIG. 8A

FIG. 8C
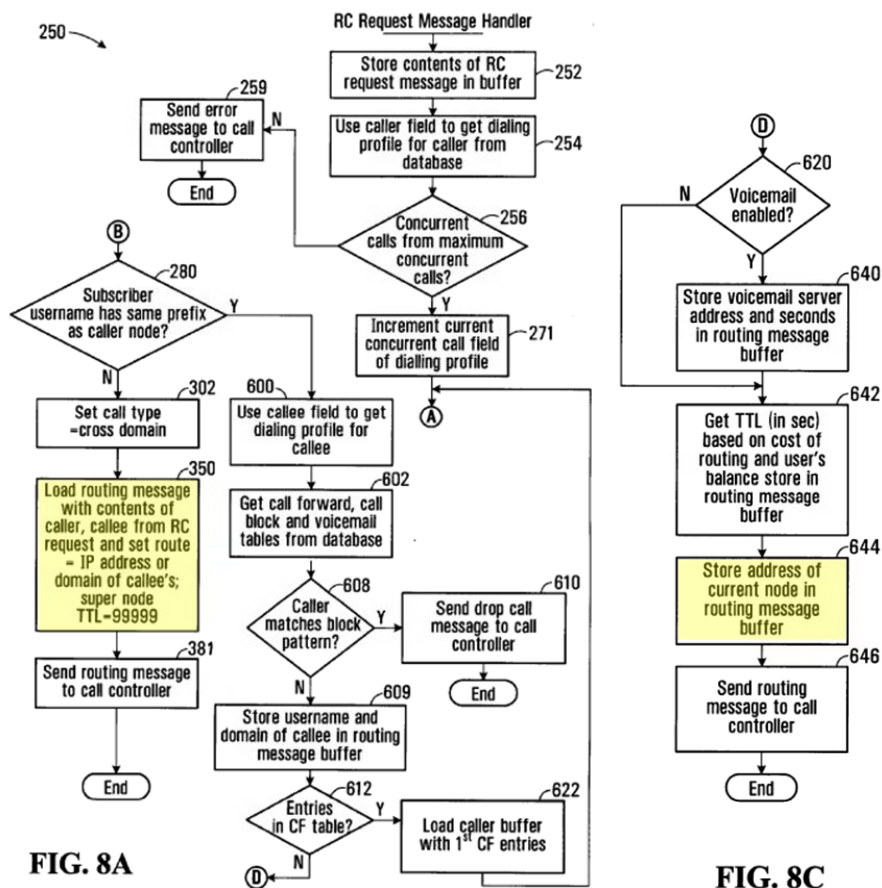
353. *Nadeau-Kelly-Vaziri* teaches this structure at least because it teaches a processor programmed to perform at least block 350, which states, "Load routing message with contents of caller, callee from RC request and set route=IP address or domain of callee's; super node TTL=99999." (EX1001 at Figure 8A.)

354. Although block 350 in Figure 8A states "set route = IP address or domain of callee's supernode," the specification of the '815 Patent states that block 350 merely requires that the route be set to "an identifier of a node on the private network with which the callee is associated." (EX1001 at Figure 8A, 20:39–48.) In other words, to perform the algorithm of block 350, the supernode's IP address need not be added to the routing message. Rather, it is sufficient for any identifier (e.g., an IP address) for any network node associated with the callee (e.g., the callee's multimedia PC) to be added to the routing message. Thus, the SLC performs this step of the algorithm when it produces routing instructions that include the IP address of the callee's multimedia PC.

355. As explained above in Limitation 28f(i), the SLC of *Nadeau* as modified by *Kelly* and *Vaziri* generates routing instructions that include an IP address for the callee. The IP address could be the IP address for a multimedia PC of the callee. (EX1005 at 9:1–4.)

> Finally, examples of an **Internet Delivery Point** FE 120 include:
>
> a multimedia PC with:
>
> a Voice-over-IP (VoIP) client

(*Id*. at 9:1–4 (emphasis added).) Therefore, the SLC sets route=IP address of callee's multimedia PC.

356. Although *Nadeau* does not explicitly disclose that the routing instructions include an identifier of the caller, one of ordinary skill in the art would understand that the routing instructions identify the caller in view of the disclosure that the routing instructions are for routing in an "IP network." (*Id*. at 7:43, 11:27.) "When a call stays inside the PSTN/Mobile or **IP network**, the call is delivered directly to the called party terminal." (*Id*. at 11:27–28; *see also*, *id*. at 7:41–44 (disclosing IP telephony network).)

357. As I discussed in the State of the Art, one of ordinary skill in the art would know that an IP message includes a header, depicted below. The header includes an IP address of the source of the message ("Source Address"). *See* ¶¶ 91–107 above.

3. SPECIFICATION

3.1. Internet Header Format

A summary of the contents of the internet header follows:

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Version|  IHL  |Type of Service|          Total Length         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Identification        |Flags|      Fragment Offset    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Time to Live |    Protocol   |         Header Checksum        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Source Address                          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                    Destination Address                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                    Options                    |    Padding    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
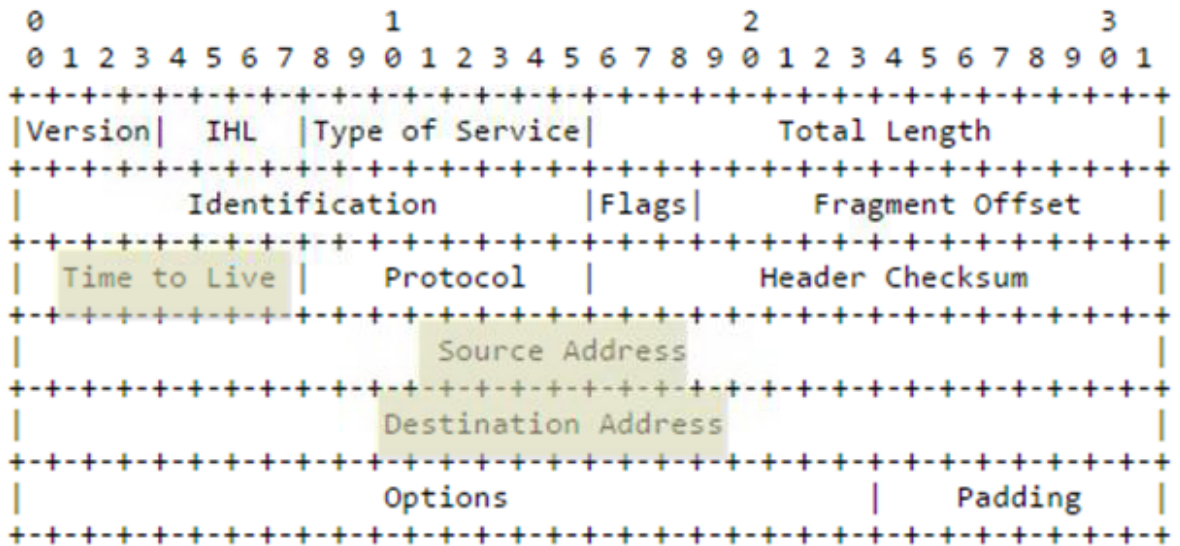
Example Internet Datagram Header

Figure 4.

Note that each tick mark represents one bit position.

358.   As a result, the teaching of routing instructions to route a call over an

IP network is a disclosure that the routing instructions identify the source of the

call, such as an IP address of the caller.

359.   Additionally, it would have been apparent to one of ordinary skill in

the art that the routing instructions include a caller identifier in light of *Nadeau*'s

disclosure that the network is an H.323 compliant network. (EX1005 at 7:41–47.)

As discussed in the State of the Art, one of ordinary skill in the art would have known that in an H.323 network, call setup requires communication of a message containing a calling party identifier and a called party identifier. *See* ¶¶ 156–158 above. These identifiers could be names, E.164 telephone numbers, private telephone numbers, email addresses, user IDs, etc. *See* ¶¶ 163–164 above.

360. Moreover, *Kelly* teaches including a caller identifier, such as a caller IP address, in a routing message. (EX1006 at 7:39–8:8.) "**The calling party transmits an on-line request packet** to a connection/information server upon connection to an IP-based network, e.g. the Internet or an Intranet. **The on-line request packet contains** configuration and settings information, a unique E-mail address and **a fixed or dynamically assigned IP address** for the WebPhone client." (*Id*. at 7:39–8:8.)

361. One of ordinary skill in the art could have easily modified the SLC of *Nadeau* to include the caller IP address in the routing instructions as taught by *Kelly* because this modification is merely a combination of prior art elements (SLC of *Nadeau* and the caller IP address of *Kelly*) according to known methods (this modification would require nothing beyond programming the SLC to add the caller IP address to the routing instructions) to yield predictable results (*Kelly* teaches the result: a routing message that includes the caller IP address). Furthermore, this

223

modification involves the application of a known technique (adding the caller IP
address to a routing message) to a known device (the SLC of *Nadeau*) ready for
improvement (this modification would require nothing beyond programming the
SLC to add a caller IP address to the routing instructions) to yield predictable
results (*Kelly* teaches the result: a routing message that includes the caller IP
address).

362.   Thus, the SLC of *Nadeau* as modified by *Kelly* and *Vaziri* "load[s]
routing message with contents of caller" by including a caller identifier in the
routing instructions.

363.   Although *Nadeau-Kelly-Vaziri* does not explicitly disclose that the
routing instructions identify the callee, one of ordinary skill in the art would
understand that the routing instructions identify the callee in view of the disclosure
that the routing instructions instruct a DPFE and ACS Gateway to route a call.
(EX1005 at 7:5–9, 12:59–61.) "**Upon reception of routing instructions** from the
SLC through the GWFE, **the DPFE will resume call processing according to the
received instructions** and route the incoming call **directly to a Delivery Point FE**
or to the IP/PSTN GWFE 124 if needed." (*Id*. at 7:5–9.) "8. The SLC 122 returns
to the **Internet ACS GWFE 116 a message indicating to route the call to the IP
address** retrieved from the Internet domain." (*Id*. at 12:59–61 (emphasis added).)

364. One of ordinary skill in the art would know that for the routing instructions to instruct another network element to route a call to a destination, the routing instructions must include an identifier for the call. In other words, the routing instructions must include an identifier for the call in order for the system of *Nadeau* to function properly. *Nadeau* teaches that a call can be initiated by a caller providing a callee's name or telephone number. (*Id.* at 9:32–38, 12:34–38.) The call is sent to a DPFE which requests routing instructions from the SLC. (*Id.* at 6:66–7:5.) The DPFE suspends call processing until it receives these routing instructions. (*Id.* at 7:1–9.) During the time that the call is suspended, the DPFE can receive other calls from other callers and suspend those calls while it awaits routing instructions for those calls. When routing instructions return for the first call, unless the routing instructions include some identifier for that first call, the DPFE will not know to which suspended call the routing instructions apply. Thus, the routing instructions must include an identifier for the call to which they apply. Because the caller already provided a name or telephone number of the callee that "uniquely identif[ies]" the callee, it would be obvious to use the callee name or telephone number as the identifier for the call. (*Id.* at 7:9:32–38.) As a result, the teaching of routing instructions to route a call is a disclosure that the routing instructions include the callee's network routable address such as an IP address or domain style IP network address, and other callee information such as a name or

225

telephone number. *See* ¶¶ 137–138, 158, 163–164 above. Thus, the SLC "load[s]
routing message with contents of callee."

365. Although *Nadeau-Kelly-Vaziri* does not explicitly disclose that the
routing instructions include a time to live (TTL), one of ordinary skill in the art
would understand that the routing instructions include a TTL in view of the
disclosure that the routing instructions are sent through an IP network. (*Id*. at 7:43,
11:27.) As I discussed in the State of the Art, one of ordinary skill in the art would
know that an IP message includes a header, depicted below. The header includes a
"Time to Live" ("TTL"). *See* ¶¶ 96–97 above. Additionally, it was well-known in
other IP related protocols and services to use a Time to Live field. *See* ¶¶ 96–97,
110–111, 136 above.

3. SPECIFICATION

3.1. Internet Header Format

A summary of the contents of the internet header follows:

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |Version|  IHL  |Type of Service|          Total Length         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         Identification        |Flags|      Fragment Offset    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |  Time to Live |    Protocol   |         Header Checksum        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                       Source Address                          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                    Destination Address                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                    Options                    |    Padding     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
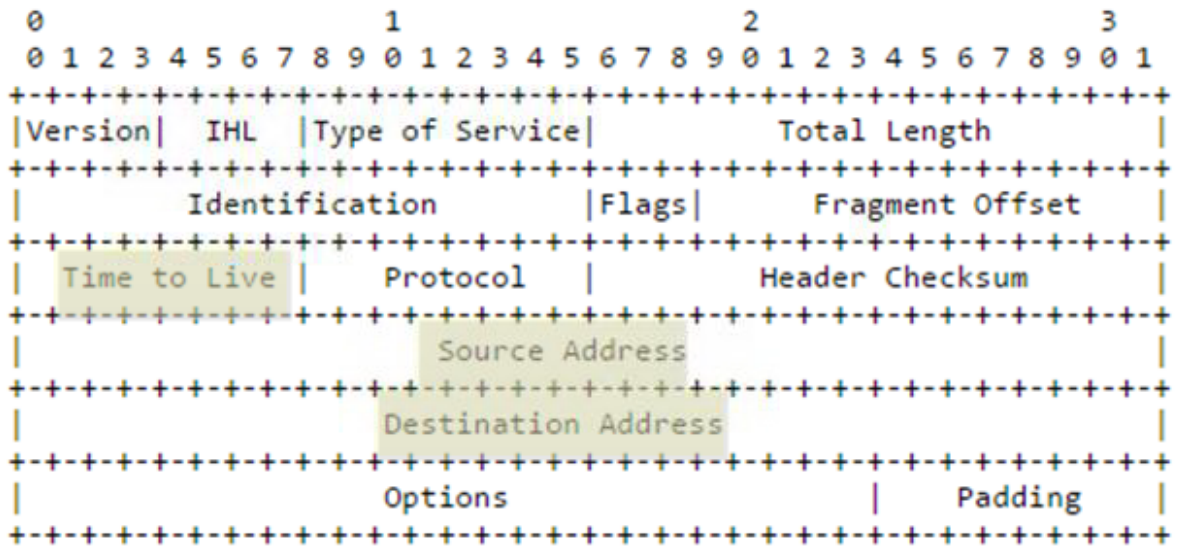
Example Internet Datagram Header

Figure 4.

Note that each tick mark represents one bit position.

366.   Although *Nadeau-Kelly-Vaziri* does not explicitly disclose a particular value for the TTL, one of ordinary skill in the art would understand that the TTL can be set to any desired value. As I discussed in the State of the Art, the TTL can be set to achieve different results depending on the particular application or implementation. *See* ¶¶ 96–94, 110–111, 136, 162 above. For example, in some implementations, the TTL was set to limit the number of network hops that an IP message may traverse before being discarded.   As another example, some

implementations set the TTL to limit the amount of time that the IP message stayed

alive or may be cached in the network. Therefore, one of ordinary skill in the art

could set the TTL to any desired value as a matter of design choice. Furthermore,

although block 350 states that the TTL is set to a value of 99999, the specification

of the '815 Patent makes clear that the TTL can be set to any value and that 99999

is merely an "example" value. (EX1001 at 20:39–43.)

367. As a result, the SLC sets a TTL in the routing instructions.

368. For at least these reasons, *Nadeau-Kelly-Vaziri* discloses Limitation

28f under the second structure.

8. Limitation 28g: "means for producing a public network routing message for receipt by a call controller, when the call is classified as a public network call, said public network routing message identifying a gateway to the public network."

369. I have been informed that this term is governed by 35 U.S.C. § 112,

Paragraph 6. I have been instructed to provide my opinion for this term using two

alternative structures "a processor programmed to implement the algorithm in

block 563 of Figure 8D" and "a processor programmed to implement the algorithm

illustrated in Figure 8D." I have not formed an opinion as to whether any of these

structures is corresponding structure or whether the specification discloses

corresponding structure for this term.

(i) First Structure

370.   *Nadeau-Kelly-Vaziri* teaches this structure at least because it teaches a processor programmed to implement the algorithm in block 563 of Figure 8D, which states "Load route field with route identifier." (EX1001 at Figure 8D.)

371.   As discussed for Limitation 28b, *Nadeau-Kelly-Vaziri* teaches a processor, such as the CPU, that performs the functions of the SLC.

372.   For an IP call, when the SLC determines that the call should be routed over the PSTN, the routing instructions instruct the DPFE and Internet ACS Gateway to route the call to an IP-PSTN Gateway. (EX1005 at 7:5–9, 8:39–42, 11:29–33.) "The primary goal of the SLC 122 is to provide the **DPFEs** with **call processing instructions**." (*Id*. at 7:22–23 (emphasis added).) "**Upon reception of routing instructions** from the SLC through the GWFE, **the DPFE will resume call processing according to the received instructions** and route the incoming call directly to a Delivery Point FE or **to the IP/PSTN GWFE** 124 if needed." (*Id*. at 7:5–9.) "[W]hen a call originating from one network has to terminate on the other, the ACS system forwards the call **to a PSTN/IP gateway for proper bridging**." (*Id*. at 11:27–28; *see also*, *id*. at 8:39–42 (the IP/PSTN gateway routes calls between network domains).)

373.   As discussed for Limitation 1f, one of ordinary skill in the art would know that the routing instructions must include an IP address of the IP-PSTN Gateway to complete the call.

374.   Moreover, *Kelly* teaches a gateway selection process that includes the IP address of the gateway in the routing instructions to "initiate a call session to the IP address of the gateway." (EX1006 at 12:32–35, 12:55–57, 13:22–26.) "**This last reference contains the IP address of the desired gateway** which is then forwarded via Internet 220 and ISP 250 to WebPhone client 232 by name server 254 in step 12." (*Id*. at 12:55–57; *see also*, *id*. at 12:32–35.) "After step 12 of FIG. 6, the **call packet** containing the entire telephone number domain name entry '4001.997.561.1.carrier.com' is then sent to initiate a call session to the **IP address of the gateway**, for example, gateway 218C, and the call is offered." (*Id*. at 13:22–26.)

375.   As discussed in Section XII.A, it would have been obvious to modify the SLC of *Nadeau* to perform the gateway selection process taught in *Kelly*. Thus, the SLC of *Nadeau* as modified by *Kelly* and *Vaziri* produces routing instructions that identify the IP-PSTN Gateway by including its IP address.

376. Therefore, *Nadeau-Kelly-Vaziri* teaches this structure because it teaches that the SLC loads a route field with a route identifier by including the IP address of the gateway in the routing instructions.

(ii) Second Structure

377. The alternative structure is "a processor programmed to implement the algorithm illustrated in Figure 8D." These steps are shown below. These steps are shown below. (EX1001 at Figure 8D.)
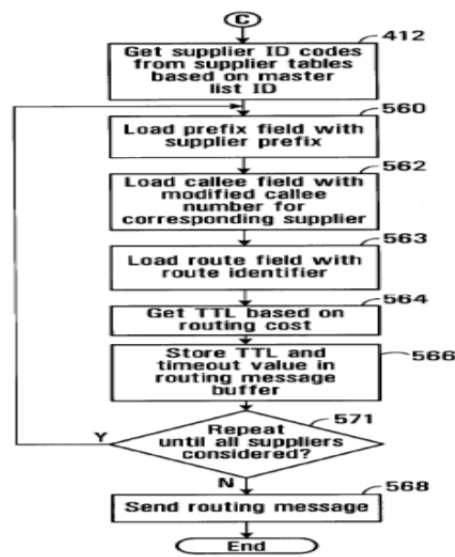

FIG. 8D

378. As with Limitation 28d, the modified SLC of *Nadeau-Kelly-Vaziri* performs a gateway selection process that retrieves ML IDs, such as references to name servers, from an E.164 number. This process eventually returns a supplier ID code, such as a reference to a carrier gateway. (EX1006 at 12:55–56.)

231

> Referring to FIG. 6, a **recursive process of resolving** the
> telephone number domain name previously entered into
> the WebPhone client to **the appropriate IP address of a
> gateway on a PSTN** is illustrated conceptually: In step 1,
> the WebPhone client 232 forwards the telephone number
> domain name to primary name server 254 in packetized
> form via Internet 220 and ISP 250. Using a name packet,
> primary name server 254 queries the root name server of
> the domain name system (DNS) for the address of
> **'4001.997.561.1.carrier.com'** in step 2. The name server
> for the DNS root returns **a reference to the name server
> for '.com'** in step 3...**This last reference contains the IP
> address of the desired gateway** which is then forwarded
> via Internet 220 and ISP 250 to WebPhone client 232 by
> name server 254 in step 12."

(*Id*. at 12:32–57 (emphasis added); *see also*, *id*. at 13:22–26 (disclosing call packet

to initiate a call to IP address of gateway).) Thus, the SLC uses ML IDs to get a

supplier ID code (**block 412**).

379. Also as discussed for Limitation 28d, the gateway selection process

produces routing instructions that include a carrier prefix such as "carrier.com."

(*Id*. at 13:22–26.) Thus, the SLC loads a prefix field with a carrier prefix (**block

560**).

380. Furthermore, as explained for Limitation 28d, the routing instructions

include a modified telephone number for the callee, such as "4001.997.561.1." (*Id.*

at 13:22–26.) A carrier identifier is appended to this number to generate a number

for that carrier, (e.g., "4001.997.561.1.carrier.com"). (*Id*. at 12:7–11.) Thus, the

SLC loads a callee field with a modified callee number for a supplier, such as
"4001.997.561.1.carrier.com" (**block 562**).

381.   Furthermore, as discussed for Limitation 28d, the routing instructions
include the IP address of the selected gateway, such as the IP-PSTN Gateway. (*Id*.
at 12:55–57, 13:22–26.)   Thus, the modified SLC loads a route field with a route
identifier, such as the IP address of the IP-PSTN Gateway (**block 563**).

382.   Additionally, as with Limitation 28f(ii), the SLC sets a TTL in the
routing instructions (**block 566**) and the TTL can be set to a value based on the
needs of an implementation or application.   Routing cost should be considered in
making determinations.   (*Id*. at 13:46–49; EX1005 at 10:8–16.)

> routing information;
>
> ...
>
> > **least cost routing, such as:**
> >
> > > complete to VoIP if IP address available;
> > >
> > > complete to called party directory number using IP
> > > through a terminating VOIP gateway;
> > >
> > > **complete to called party directory number
> > > using PSTN;**"

(EX1005 at 10:8–16 (emphasis added).)   "By utilizing the invention as previously
described, a gateway may be selected on a **least cost routing basis to minimize**

the toll charges on a traditional PSTN network." (EX1006 at 13:46–49

(emphasis added).) Thus, routing cost may be a need of an implementation or

application that affects the value of the TTL. Therefore, the SLC gets a TTL based

on routing cost (**block 564**).

383. Although, *Nadeau-Kelly-Vaziri* does not disclose setting a timeout in

the routing message, one of ordinary skill in the art would understand that the

routing message includes a timeout because the call is being routed to its

destination over the PSTN. (EX1005 at 6:16–24.) As discussed in the State of the

Art, one of ordinary skill in the art would have known that timeouts are set for

PSTN calls. *See* ¶¶ 161–163 above. These timeouts may be used to control call

processing, such as to try alternate routing paths when a switching system becomes

overloaded such that no response to a call request is received. Thus, that the

routing message is used to route a call over the PSTN is a disclosure that the

routing message includes a timeout for the call. (EX1005 at 6:16–24.) Because

the modified SLC set a timeout for the call and indicated that timeout in the routing

message, the SLC must have set the timeout in a buffer in memory before writing

it to the routing message. That buffer is the routing message buffer. Therefore, the

CPEDRE stores a timeout in the routing message buffer (**block 566**).

384. As part of the gateway selection process, the modified SLC considers multiple carriers and selects a gateway of a carrier (**block 571**). (EX1006 at 12:37.) "The WebPhone client may also be configured with a default or user selectable **PSTN carrier such as MCI, Sprint, AT&T, etc., such carrier will be referred to generically hereafter as 'carrier.com.'**" (*Id*. at 12:3–7 (emphasis added); *see also*, *id*. at 13:58–59 (disclosing overriding preferred carrier).)

385. Also, the SLC sends the routing instructions to a DPFE and ACS Gateway to route the call (**block 568**). (EX1005 at 7:5–9, 7:22–23, 12:55–61.) "The primary goal of the SLC 122 is to provide the **DPFEs** with **call processing instructions**." (*Id*. at 7:22–23 (emphasis added).) "**Upon reception of routing instructions** from the SLC through the GWFE, **the DPFE will resume call processing according to the received instructions** and route the incoming call directly to a Delivery Point FE or **to the IP/PSTN GWFE 124** if needed." (*Id*. at 7:5–9.)

386. Thus, *Nadeau-Kelly-Vaziri* discloses this limitation under the second structure.

387. Furthermore, *Nadeau-Kelly-Vaziri* teaches a structure equivalent to a processor programmed to implement the algorithm illustrated in Figure 8D. Generally, this algorithm performs three steps to produce a routing message: (1)

235

add carrier information to the routing message (blocks 412, 560, 563, 571); (2) add

call information to the routing message (blocks 562, 564, 566); (3) send the routing

message (block 568).

388. *Nadeau* teaches the SLC including a processor to perform the

functions of the SLC. (EX1005 at 7:34–40.) *Kelly* teaches adding carrier

information to a routing message. (EX1006 at 11:50–12:67; 13:22–26.) *Nadeau*

teaches adding call information to the routing message and sending the routing

message. (EX1005 at 7:5–9, 7:20–27, 12:32–65.) As discussed in Sections XII.A

and XIII.A, it would have been obvious to modify the SLC of *Nadeau* to perform

the functions taught in *Kelly* and *Vaziri*.

389. Thus, *Nadeau-Kelly-Vaziri* discloses a processor that performs the

recited function in substantially the same way as disclosed in the '815 Patent to

produce substantially the same result of producing a routing message. Therefore,

Nadeau-Kelly-Vaziri teaches an equivalent structure.

C.   Claim 34: "The apparatus of claim 28 further comprising formatting means for formatting said callee identifier into a pre-defined digit format to produce a re-formatted callee identifier."

390. I have been informed that this term is governed by 35 U.S.C. § 112,

Paragraph 6. I have been instructed to provide my opinion for this term using the

structure "a processor programmed to implement the algorithm illustrated in block

236

261, block 388, block 394, or block 400 of Figure 8B." I have not formed an opinion as to whether this structure is corresponding structure or whether the specification discloses corresponding structure for this term. These steps are shown below. (EX1001 at Figure 8B.)

FIG. 8B
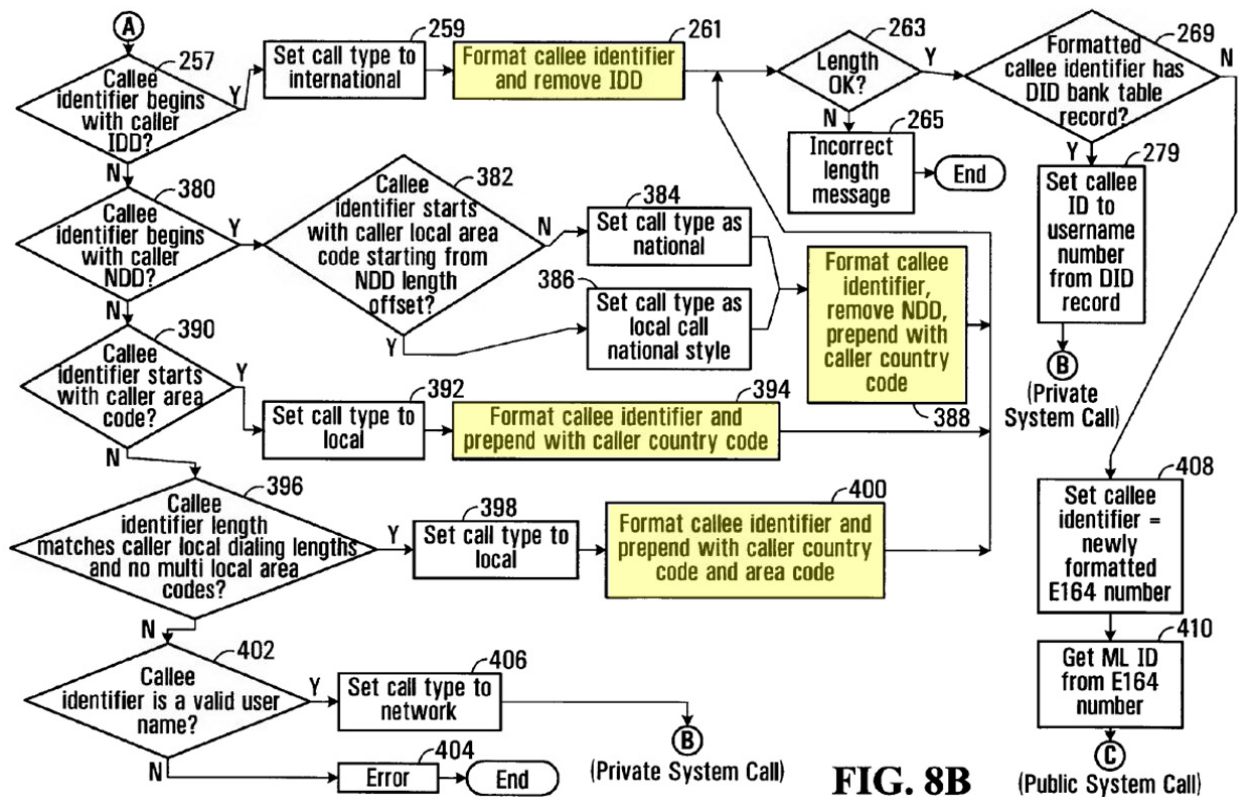
391. As with Limitation 28d, *Nadeau-Vaziri-Kelly* teaches a processor programmed to implement blocks 257, 259, 261, 263, 269, 408, and 410. Therefore, *Nadeau-Vaziri-Kelly* teaches this structure because it teaches a processor programmed to implement at least block 261.

D. Claim 93

392. The preamble of Claim 93 (a call routing controller apparatus "for establishing a call between a caller and a callee in a communication system") is substantially similar to the preamble of Claim 28 (a call routing apparatus "for facilitating communications between callers and callees in a system"). *Nadeau-Kelly-Vaziri* teaches Claim 93's preamble for at least the same reasons discussed for Claim 28's preamble. The corresponding structures for Claim 93's limitations are the same corresponding structures identified for Claim 28's limitations. Thus, the analysis for Claim 28's limitations is cross-applicable to Claim 93's limitations. (*See* Limitations 28b–28g.) One of ordinary skill in the art would understand the Service Logic **Controller** to be a controller apparatus. Additionally, *Nadeau-Kelly* explains that the primary goal of the SLC is to provide routing instructions to route a call. (EX1005 at 7:20–27.) Thus, one of ordinary skill in the art would understand that the SLC is a call routing controller apparatus.

E. Claim 111: "The apparatus of claim 93 further comprising means for causing the private network routing message or the public network routing message to be communicated to a call controller to effect routing of the call."

393. I have been informed that this term is governed by 35 U.S.C. § 112, Paragraph 6. I have been instructed to provide my opinion for this term using the structure "a processor programmed to implement the algorithm illustrated in block

381 of Figure 8A, block 646 of Figure 8C, and block 568 of Figure 8D." I have

not formed an opinion as to whether this structure is corresponding structure or

whether the specification discloses corresponding structure for this term. These

steps are shown below. (EX1001 at Figures 8A, 8C, 8D.) Each block recites the

same step: send a routing message to a call controller.

FIG. 8A   FIG. 8C   FIG. 8D
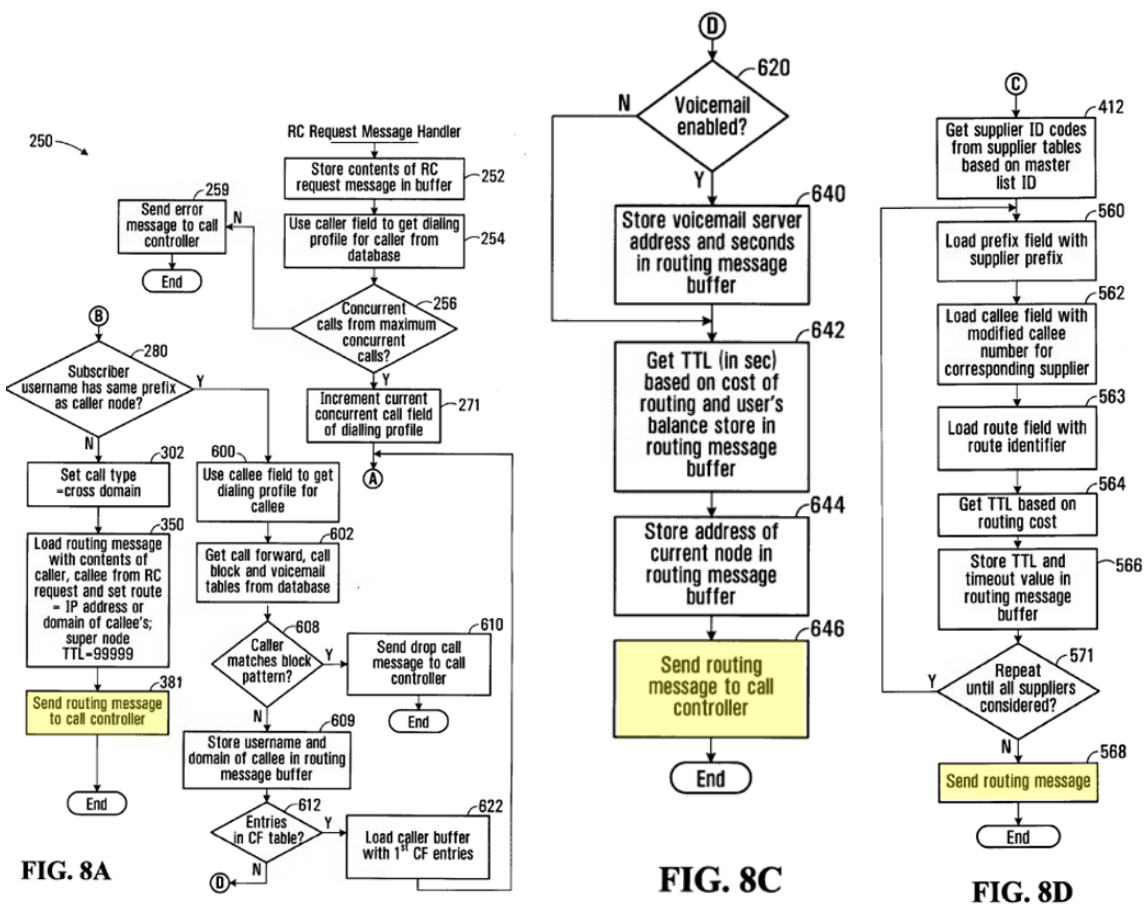
394. *Nadeau-Kelly-Vaziri* teaches this claim.

395.   As discussed for Limitation 28b, the SLC includes a processor, such as a CPU.

396.   The SLC sends the routing instructions to a DPFE or ACS Gateway to effect routing of the call. (EX1005 at 7:5–9, 7:22–23, 12:59–61.) "The primary goal of the SLC 122 is to provide the **DPFEs** with **call processing instructions**." (*Id*. at 7:22–23; *see also id*. at 12:59–61.)   "**Upon reception of routing instructions** from the SLC through the GWFE, **the DPFE will resume call processing according to the received instructions** and route the incoming call **directly to a Delivery Point FE or to the IP/PSTN GWFE 124** if needed." (*Id*. at 7:5–9.)

397.   Although *Nadeau-Kelly-Vaziri* does not explicitly refer to the DPFE and ACS Gateway as a "call controller," the DPFE and ACS Gateway form a call controller as described by the '815 Patent. The specification of the '815 Patent explains that a call controller receives a routing message from a routing controller and then completes a call according to the routing message. (EX1001 at 14:10–23.)

398.   The DPFE and ACS Gateway form a "call controller" as contemplated by the '815 Patent because the DPFE and ACS Gateway receive "routing instructions" from the SLC and then complete a call according to those "routing

240

instructions." (EX1005 at 7:5–9, 7:20–23, 12:59–65.) Thus, *Nadeau-Kelly-Vaziri* teaches the SLC sending a routing message, such as routing instructions, to a call controller, such as the DPFE and ACS Gateway.
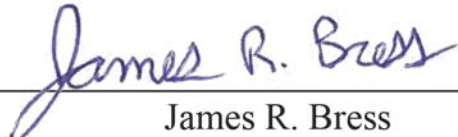
XIV. CONCLUSION

399. Based on the foregoing, it is my opinion that the Challenged Claims are invalid.

400. I may testify about any of the preceding topics at a deposition or hearing.

401. I reserve the right to respond to any declarations that are submitted by Digifonica's expert witnesses or to any testimony by Digifonica's fact or expert witnesses, whether at deposition or at trial.

402. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001.

James R. Bress

_____
James R. Bress

**James R. Bress
Curriculum Vitae**

Professional Summary

Mr. Bress has over 30 years of experience in the telecommunications industry. His work experience covers a broad range of disciplines including the development of requirements and standards for digital (VoIP), mobile, and analog telephone equipment, network systems and interfaces, product design consulting, user interfaces engineering, developing and operating telecommunications testing laboratories including VoIP, mobile, and analog equipment, design and development of testing systems including hardware and software development, software architectures and database system design, database system management, software code development, hardware architectures and development, new telecommunications services development, and the delivery of telecommunications training seminars (US and internationally).

Mr. Bress has in-depth knowledge and experience with telecommunications protocols and systems including SS7/AIN (Advanced Intelligent Network), PSTN, VoIP, Unified Communications (UC), mobile, and IMS.

Mr. Bress has over 10 years of experience in intellectual property matters including expert consulting and witnessing for patent litigation (plaintiffs and defendants), patent prosecution, testifying in court, testifying in deposition, development of expert reports and declarations for infringement, non-infringement, validity, and invalidity, claim charts analysis, claim construction, inter partes review (IPR), ex parte and inter partes re-examination, and the development of intellectual property and the filing of patents. Mr. Bress also has litigation experience related to the Telecommunications Consumer Protection Act (TCPA).

Mr. Bress has extensive experience working with multi-national engineering teams in the telecommunications product development process from design conception, software and hardware architectures, prototyping, design testing, production, and quality assurance.

Mr. Bress has in-depth experience with technologies related to hearing loss including interfacing with hearing loss special interest groups, amplified telephone equipment developers, manufacturers and suppliers, hearing aid manufacturers, and audiologists. Mr. Bress was the prime contributor to the ANSI/TIA-4953 standard for amplified telephone performance and this work has included consulting and presentations to state (PUC) and federal (FCC) agencies focused on accessibility and equipment for the hearing impaired.

Mr. Bress was (and continues to be) the chief architect for the development of several complex telecommunications device test systems including hardware, software, user interfaces, system integration, and networking protocol interfaces.

Mr. Bress is the named inventor for patents issued while at Bellcore, AST, and as a private consultant. He is the author of many Bellcore requirements and recommendations documents and the prime contributor to many American National Standards Institute / Telecommunication Industry Association (ANSI/TIA) standards. Mr. Bress has provided leadership at TIA continuously starting in 1998, and he is currently serving as chairman of the TIA TR-41 engineering committee for communications products performance and accessibility standards development.

Mr. Bress is a cum laude graduate of the University of North Carolina with a BS in Electrical Engineering, and a summa cum laude graduate of the California Institute of Technology with a MS in Electrical Engineering.

James R. Bress Curriculum Vitae

Employment Summary

Mr. Bress is currently the president of AST Technology Labs Inc. which he founded in 1995, providing product design consulting and testing services to internationally based customers including telephone service providers, product certification programs, and product and semiconductor manufacturers.

Prior to founding AST, Mr. Bress was employed from 1985 to 1995 at Bell Communications Research (Bellcore) as a Member of the Technical Staff (MTS) and Senior Systems Engineer. Mr. Bress's work at Bellcore was focused on new services development including prototype terminals (including smart phones) development, network signaling and protocols, operations, and features requirements, and the development and operation of telecommunications testing laboratories including hardware and software development.

Since 2005 Mr. Bress has been an expert consultant and expert witness for intellectual property litigation and prosecution cases.

Expertise

- Voice Over IP (VoIP) Signaling and Features
- Digital Telephony Signaling and Features
- Mobile Telephony Signaling and Features
- Analog Telephony Signaling and Features
- Computer Telephony Devices
- Unified Communications (UC) Technologies
- Caller-ID Technologies
- Voicemail Systems
- Telephone Answering Machines
- Acoustics and Audio Technologies
- Amplified Telephones and Hearing Loss
- Communications Accessibility
- Telephone Feature Implementation
- Telephone and Gateway Testing
- Webcam Testing
- Video Set-Top-Box Testing
- Telecommunications Standards
- Telecommunications Network Architectures
- US Telecommunications Infrastructure
- Telecommunications Services Development
- IP (SIP / SDP, IMS)
- Advanced Intelligent Network (AIN)
- ISDN
- ADSL
- POTS
- Electronics and Control Systems
- Communications Protocols
- Test Systems Design and Development
- Analog and Digital Hardware
- Product Development Processes
- RF Communications
- Software Architectures and Development
- User interfaces design
- Database Systems Development and Management
- Systems Development and Integration
- Product Design Specifications Development

Education - University

Year	College or University	Degree
1987	California Institute of Technology	M.S. Electrical Engineering (GPA: 4.0 / 4.0)
1985	University of North Carolina at Charlotte	B.S. Electrical Engineering (GPA: 3.6 / 4.0)

James R. Bress Curriculum Vitae	March 1, 2017

Education - Other

"Bellcore University" classes including:

- SS7 (Signaling System #7)
- Computer networking: Architectures
- Computer networking: Token Ring
- Computer networking: Ethernet / IP
- 'C' language programming (multiple classes)
- X.25 protocols

- OSI protocols
- ISDN
- Databases
- Multiple internal operations classes

Professional Experience

From: 2005
To: Present
Organization: James Bress
Title: Expert Witness and Expert Consultant
Summary: See separate section below: "Litigation and Intellectual Property Expert Experience"

From: 1995
To: Present
Organization: James Bress, Consultant
Title: Engineering Consultant and Expert
Summary: In addition to activities and responsibilities related to Mr. Bress's position as President and CTO at AST Technology Labs Inc. (see below), Mr. Bress has been a contractor / consultant for projects which are summarized below.

- Summary of project responsibilities
    - Analysis of telecommunications standards to support the development of product performance specifications and the development of related testing systems.
    - Technical consulting for the development of detailed product performance specifications, and the design and development of advanced telephony device prototypes.
    - Systems development including system architecture design, software and hardware development, system installation and training.
    - Field troubleshooting and consulting for customer's product issues.
    - Development of Intellectual Property (IP).
    - Development and delivery of technical training seminars regarding telecommunications product design and testing for North American and international customers.

- Projects highlights include:
    - VoIP telephone, gateway / Analog Terminal Adapter (ATA) test system.
        - Developed system architecture, hardware, software, and user interfaces including features for controlling and analyzing VoIP

sessions.

- Integration and provisioning of system hardware components.
- System features include control and analysis of:
    - SIP and SDP signaling for call set-up negotiation and signaling messages.
    - RTP for audio transmission and telephony event control.
    - Message headers, message field data, and message packet timing.
    - Analog port (FXS and FXO) signaling input/output.
- Test system used for call set-up analysis, feature analysis (e.g., caller-ID, VMWI, voicemail), end-to-end signaling, timing variations, and much more.

- o IMS (Internet Multimedia Subsystem) services.
    - Research and development of system designs and architectures for services delivery via IMS (Internet Multimedia Subsystem) based on 3GPP, IETF, and ITU standards and protocols including access, transmission, and billing.
        - Analysis of IMS architecture for the design of an audio enhancement feature.
        - Developed services concept for users connecting to an IMS network via SIP/SDP enabled devices to access service provided by application servers.
        - Application servers service logic used to enhance the audio of a VoIP session by inserting a custom media gateway feature in the media path to modify the audio based on the user's hearing impairment parameters.
        - Media gateway with added features to provide the audio enhancements applied to the speech signal coded in the transmission codec (voice coder).
    - Analysis and development of service delivery for mixed mode networks using IMS and AIN interfaces and components.
    - Analysis of service delivery to mobile devices including issues related to connections of the mobile circuit switched (CS) network to the IMS packet switched (PS) network.
    - Named inventor for US Patent No. 9,020,621 "Network Based Media Enhancement Function Based on an Identifier".
- o Microsoft's Skype for Business (fka: "Lync") device test lab.
    - Audio device testing program using AST's audio and acoustics test lab (see below).
    - Video camera test lab developed including integrating hardware, software, fixtures, and testing environment (controlled light room) for testing of video cameras (e.g. webcams).
- o Microsoft's "Response Point" IP-PBX system requirements and test lab.
    - Development of detailed performance and testing specifications, and the development of custom testing capabilities for each system component:
        - VoIP telephony devices (handset, headset, speakerphone).

- - VoIP gateways (FXO/PSTN and FXS/ATA-Analog).
    - System base controller (including SIP server, proxy, registrar, and voicemail server).
  - Microsoft's customer's installations troubleshooting and consulting.
- Audio and acoustics telephony test lab.
  - Integration of hardware, software, test fixtures, and physical testing environments.
  - Standard/basic tests including frequency response, amplitude, volume control, noise, distortion, stability.
  - Advanced tests including terminal coupling loss (TCLw), echo cancellation (line and acoustic), noise suppression / cancelation, speech quality.
  - Anechoic room and semi-reverberant room test environments set up and qualified.
  - Speech recognition testing (e.g. Cortana) for multiple device types (laptops, tablets, etc.).
  - Subjective testing.
- Thomson Consumer Electronics General Telephone Design Specifications
  - Drafted and updated complete library of Thomson's detailed feature, performance, and testing requirements provided to OEMs (1000's of pages).
  - Consulted with Thomson engineers and OEMs for product design details and testing requirements.
  - Comprehensive product performance testing services for Thomson's OEMs.
- TSA-6000® telephone signal recording and analysis system.
  - Developed system architecture, hardware, and software including features for signal recording and DSP analysis and reporting of telephony signals, events, states, and protocols.
  - Design of feature-rich graphical user interfaces.
  - Ongoing project operations include the manufacture and sale of TSA-6000® systems which started in 2003.
  - Named inventor for U.S. Patent No. 7,076,031 "System and Method for Telephone Signal Collection and Analysis."
  - Human factors testing for user interfaces.
- Automated Range Test (ART™) system.
  - Developed system architecture, hardware, software, and user interfaces.
  - System used to test the RF range of a cordless telephone by applying audio signals to the telephone's microphone (send path) and line (receive path) interfaces while varying the (simulated) distance between the cordless handset and its associated base.
  - Control of RF path attenuation using probes and computer controlled RF attenuators.
  - Separately analyze the telephone's transmit and receive audio signals in real time to determine a quality factor used to calculate when the simulated distance has caused the handset - base communications link to degrade below a configured threshold.

- Audio files are also recorded for subsequent analysis.
- ART™ used in house at AST and also sold to key AST customers including installation and on-site training.
- Human factors testing for user interfaces.
  o Automated Caller-ID test system (ATAS™)
    - Developed system architecture, hardware, software, and user interfaces.
    - Development and integration of:
      - DSP based signal simulations.
      - Telephone line simulation and control.
      - Vision system for automatic pass / fail analysis. Included OCR (optical character recognition), light indicator detection, and pattern matching.
      - Database for storing results and elaborate reporting.
    - ATAS™ used in house at AST and also sold to key AST customers including installation and on-site training.
    - Human factors testing for user interfaces.
  o Automated Stutter Dialtone Detection test system
    - Developed system architecture, hardware and software.
    - Development and integration of:
      - DSP based signal simulations.
      - Telephone line simulation and control.
      - Developed robotic interface for telephone push-button and switch-hook control using custom developed electrical / mechanical hardware and software control with feedback.
      - Interface and control of line conditions and computer controlled light sensor.
      - Database for storing results and elaborate reporting.
    - System used in house at AST.
  o ADSL test labs development and operation:
    - ADSL splitters and filters.
    - ADSL signaling impact on other out-of-band signaling equipment.
    - ADSL physical layer testing of integrated gateways (test plans).
  o Common-Mode Noise test system.
    - Developed system architecture, hardware and software.
    - Development and integration of:
      - DSP based signal simulations.
      - Telephone line simulation and control.
      - Test parameter configurations based on Bell System Technical Journal (BSTJ) published field test results.
    - System used in house at AST.
  o Network Call Generator system (for Telcordia)
    - Developed system architecture, hardware, software, and user interfaces.
    - Prototype to support demonstrations of Telcordia's:
      "1 Million Calls Per Minute" emergency notification project.
    - Integration of d telephone call control hardware and software and

**James R. Bress
Curriculum Vitae**

database.

- Delivered and installed system and trained Telcordia management and sales teams.

  o Telcordia Analog Display Services Interface (ADSI)
    - Development of a standardized interface between an ADSI telephone and a Computer Telephony Integration Signaling Unit (ACTISU).
    - ACTISU unit was designed to connect in the network and communicate with an AIN (Advanced Intelligent Network) node.
    - System designed to work in conjunction with class-5 end-office switching systems (e.g., AT&T 5-ESS and Nortel DMS-100) to support the development of new consumer telephony services.
    - Named inventor for US Patent No. 5,570,420 "Customer premise equipment network integrator."

  o Seminars delivered to multiple companies / organizations including:
    - Alcatel (Paris, France)
    - Belco Telecom Products (Seoul, Korea)
    - HLAA (Hearing Loss Association of America)
      (Delivered in multiple US sites)
    - Inventec Electronics (Penang, Malaysia; Nanjing China)
    - Motorola (Austin, TX)
    - NASRA (National Association for State Relay Administration) (Albuquerque, NM)
    - Nortel (Calgary, Canada)
    - Philips Semiconductors (Eindhoven, The Netherlands)
    - Rayson Electronics (Taipei, Taiwan)
    - TEDPA (Telecommunications Equipment Distribution Programs Association) (Delivered in multiple US sites)
    - Thomson Consumer Electronics (Paris, France; Indianapolis, IN)
    - Uniden (Tokyo, Japan)

From: 1995
To: Present
Organization: AST Technology Labs, Inc.
Title: President, Chief Technical Officer, and Founder
Summary: AST Technology Labs Inc. provides services to the telecommunications industry including product testing and reporting, product design engineering and development consulting, and systems development (including software and hardware).

               AST is also involved in standards development and provides leadership for the Telecommunications Industry Association (TIA).

               AST's list of clients includes telecommunications service providers, telephone equipment manufacturers, retail and institutional equipment buyers, semiconductor manufacturers, and other test labs.

> **James R. Bress**
> **Curriculum Vitae**

Mr. Bress's responsibilities include:

- Chairman of the Telecommunications Industry Association (TIA) TR-41 engineering committee (telephone performance standards) (2015 – Present) and chairman / vice-chairman of the TIA TR-41.3 sub-committee (telephone performance standards) (2000 – 2015). Responsibilities include management of standards development, officiate at meetings, and liaison to other telecommunications standards organizations including ETSI, ITU, IETF, and IEEE.

- Telephony test systems design and development including authoring of overall system architectures, software architectures, software, hardware, and user interfaces (GUI).

- Development and operation of telephone testing lab for VoIP telephone devices and computer telephony devices including audio and acoustics, interfacing and signaling, and feature operations.

- Development and operation of Unified Communications (UC) devices audio and video testing lab for computer telephony devices (handsets, headsets, speakerphones, tablets, mobile devices, and webcams). AST is an authorized test lab for Microsoft's "Optimized for Lync Logo" (now "Skype for Business") and Skype device certification program.

- Development and operation of mobile handset testing lab including audio and acoustics and feature operations. Testing GSM, CDMA, WCDMA (UMTS), and LTE (4G) devices. Integration of R&S CMU200 and R&S CMW500 base station simulators with audio and acoustics test system.

- Development and operation of VoIP telephone, gateway and Analog Terminal Adapter (ATA) test system.

- Development and operation of comprehensive analog telephone device testing lab including Caller-ID, telephone line electrical and signaling interfacing, audio and acoustics, environmental performance testing (ESD, lightning, drop, AC power), Radio Frequency Immunity (RFI), cordless telephone (range, battery charging, operations), and other specialized features performance testing.

- Development and operation of Set-Top-Box telephone interface testing lab specified by DirecTV for DirecTV's Set-Top-Box vendors.

- Development and operation of amplified telephone testing lab for device audio and acoustic and signaling performance.

- Development and operation of Hearing Aid Compatibility (HAC) telephone handset testing lab for signaling performance.

- Development and operation of comprehensive testing lab for telephone answering machines and IP based voicemail systems including signaling and features.

- Design and development of professional test reports for testing lab services.

- Development of telecommunications product specifications and prototypes.

- Field troubleshooting and consulting for AST customer's product issues.

- Technical consulting for the development of detailed product performance specifications, and the design and development of advanced telephony devices.

**James R. Bress
Curriculum Vitae**

- Protection of AST's intellectual property through patent development and applications.
- Business development, client development, contracts, personnel, and corporate systems.

AST's Services

AST provides services to telephone service providers, telephone designers and manufacturers, and semiconductor manufacturers. These services include:

- Testing and reports for conformance to standards including TIA, Bellcore, IEEE, ITU, ETSI, 3GPP, and others, for telephony products and interfaces
- Product design consulting with product engineering development support
- Development of custom test systems
- Development of custom testing methods and test reports
- Development of telephony product design specifications and requirements
- Development of product testing specifications and requirements
- Custom test systems on-site installation and training
- Development of product testing specifications for AST customers
- Development of product and system prototypes based on customer's requirements
    - o System architecture design
    - o User interface design (GUI) and software prototyping for customer approvals
    - o Software design, implementation, and test
    - o Hardware design, implementation, integration, and test

AST's Test Systems Development Projects

AST performs systems development including integration of vision systems, database systems, RF control systems, audio control systems, signaling and interface hardware and user interface controls (GUI). Test systems developed include:

- VoIP gateway signaling and features test system
- Unified Communications device testing labs (audio and video)
- Telephone acoustic test system (VoIP, Mobile, Analog)
- Automated Caller-ID testing system (ATAS)
- Automated Cordless Telephone Range test system (ART)
- Automated RFI (Radio Frequency Interference) test system (ARFI)
- Common-mode noise test system
- Automated Stutter Dialtone Detection test system
- Telephone signal capture and analysis system (TSA-6000®) (patented)

| James R. Bress |
| Curriculum Vitae |

From: 1985
To: 1995
Organization: Bell Communications Research (Bellcore) (now known as Telcordia)
Title: Senior Systems Engineer, Member of the Technical Staff (MTS)
Summary: <u>Caller-ID / ADSI / AIN Telephone Features Related Projects</u>

- Author of Bellcore Caller-ID and ADSI (Analog Display Services Interface) network signaling and telephone requirements and testing documents.

- Analysis of class-5 (end office) switching systems capabilities including the AT&T 5-ESS, Nortel DMS-100, and Siemens EWSD. Analysis was for the development of new telephony services.

- Screen phone (smart phone) requirements, system architectures, and software development including server-to-terminal protocols, signaling, and information display requirements (display mapping rules). The terminal display requirements were based on a "logical display" (vs. physical display) and "soft-keys" definition allowing for an open terminal display architecture including the use of hierarchical presentation of options.

- User interfaces prototyping and effectiveness analysis.

- Research and analysis of touch-screen technologies to select touch-screen type to be integrated in prototype screen phones (smart phones).

- Telephony features enabled by ADSI included Visual Voice Mail (VVM), context sensitive soft-keys to activate CLASS services (e.g., automatic recall, automatic callback), called party telephone directories, and access to information services.

- Managed and developed Bellcore's Caller-ID / ADSI conformance test lab including hardware and software development.

- Subject Matter Expert for Caller-ID / ADSI signaling and protocols.

- Developed and delivered Caller-ID / ADSI seminars to US and international telcos and telephone product manufacturers.

- Human factors testing for user interfaces and customer acceptance of tone levels, frequencies and call interruptions.

<u>Information Gateway Projects</u>

- Leader of the development team for the "Information Gateway" which defined protocols between network-based servers and terminals for access of information, display of the information, and user input methods.

- Developed demonstration of networked remote database access and transmission system for images stored with searchable characteristics parameters. Included development of data compression and error control used for transmission.

- Researched and reported on the current state of the art for terminal display and mapping (information display rules) protocols including France Minitel. NAPLPS, AT&T Smart Phone, VT-100, and other terminal protocols.

- Developed mass market and network service platform prototypes (software development and hardware integration) using PSTN, ISDN, X.25, and TCP/IP networks.

- Developed service architectures, requirements, and prototypes for Advanced Intelligent Network (AIN) services deployed in a Signaling System #7 (SS7) network.

- Developed, tested, and applied human factors analysis techniques to graphical user interfaces (GUI) for the display and access to distributed information (pre-cursor to web browsers).
- Developed software interfaces and protocols for a layered communications system architecture including layer-1 (physical), layer-2 (data link), and layer-3 (network) with emphasis on ISDN (Q.921 and Q.931) and Ethernet connectivity.
- Software development and hardware integration for integrated ISDN, X.25, and POTS messaging services.
- C-language software development under UNIX / Windows / DOS.
- Assembly language development.
- Developed hardware and software for PC based analog and digital test equipment.

Corporate Fax – Email Server Project
- Chief architect, project manager, and software developer.
- Developed integrated messaging platforms (architecture, software, database, hardware) for e-mail, fax, voice, and directory services.
- Developed new features for Bellcore's corporate fax / email server system. Included integration of fax-to-email and email-to-fax- for incoming and outgoing faxes through corporate email system.
- Human factors testing for user interfaces.

Bell Operating Company Operations Systems Development and Management
- Developer, tester, and analyst for the Bellcore ST&S (Software Technologies and Systems) business unit in the FACS (Facility Assignment and Control Systems) group including database management and configuration.
- Developed code and managed database system components for PREMIS (PREmise Information System), SOAC (Service Order Analysis & Control), and LFACS (Loop Facility Assignment and Control System) which are all components of the FACS.
- Managed and performed FACS systems communications network development and software installation and testing.
- RDBMS performance analysis and development.

From:	1990
To:	1993
Organization:	Sole Proprietor
Title:	Owner / Software and Systems Developer
Summary:	▪ Development of database system for entertainment/tour companies' customer databases including schema architecture and design, coding, report development, and remote access.
	▪ Developed system specifications, developed all code, and added features as requested by customers.

James R. Bress **Curriculum Vitae**	**March 1, 2017**

From: 1982
To: 1984
Organization: Process Systems Inc.
Title: Engineering Technician
Summary:
- Technical writing for energy management field located equipment and host system software and user manuals
- Developed test equipment and procedures for field located equipment and host systems

**James R. Bress
Curriculum Vitae**

Litigation and Intellectual Property Expert and Consultant Experience

- Patent Litigation: Expert witness and consultant
    - Infringement (plaintiff cases, and defendant cases).
    - Invalidity (supporting invalidity position cases, and defending validity cases).
    - Experience includes:
        - Trial testimony
        - Depositions
        - Expert reports and expert rebuttal reports
        - Declarations
        - Claim chart development and analysis
        - Prior art searches
        - Prior art analysis
        - Consulting with attorneys
        - 30 (b)(6) depositions support
        - Research
        - Systems analysis
        - Software code review and analysis

- Patent Prosecution Cases
    - Inter partes reviews (IPR)
    - Inter partes re-examination
    - Ex-parte re-examination
    - Experience includes:
        - IPR depositions.
        - Engagements with third party requesters and patent owners.
        - Multiple cases regarding telecommunications patents.
        - Expert declarations.
        - Analysis of prior art.
        - Search and identification of prior art (including patents and technical publications).
        - Claim chart development and analysis.
        - USPTO panel interview.
        - In-depth study into the technical and legal basis for obviousness including precedent setting cases and the MPEP (Manual of Patent Examining Procedures).

- TCPA (Telecommunications Consumer Protection Act) Litigation: Expert witness and consultant
    - Deposition.
    - Expert declaration development.
    - VoIP based telephone system analysis including operations, functions, and features.
    - Mobile telephone service call connections and billing records analysis of Call Detail Records obtained from a subpoena of plaintiff's AT&T mobile account.
    - Consulting regarding FCC rules and regulations related to the TCPA.

James R. Bress
Curriculum Vitae

- Pre-Litigation Support: Expert consultant for the analysis of patent claims and accused products
  - o Patent claims infringement review including evaluation and analysis of accused products and systems to determine operational features and methods.
  - o Patent claims validity evaluation including prior art searches.
  - o Consulting with attorneys to explain technical aspects of claims and patent specifications.
  - o Product analysis including disassembly, parts inspection analysis, software code review, and research.

- Vermont PUC (Public Utility Commission) VoIP Service Hearings
  - o Purpose: Determine if VoIP is a Telecommunications Service Vs. Information Service.
  - o Consulting and response to VT-PUC RFP questions.
  - o Analysis of VoIP services connectivity and configurations (e.g., Comcast VoIP service).
  - o Analysis of issues related to "Nomadic Vs. Fixed VoIP".
  - o Analysis of FCC telecommunications regulations and declaratory rulings.

<table>
<tr><td align="center">**JAMES BRESS**
LITIGATION AND PATENT PROSECUTION
CASES SUMMARY</td></tr>
</table>

- **CLOSED**
  - o Trial
    - 1 patent case to trial
  - o Deposition
    - 2 patent cases to deposition
    - 1 TCPA lawsuit defense (Telecommunications Consumer Protection Act) to deposition
  - o USPTO / PTAB
    - 4 IPRS
    - 1 inter partes reexam
    - 1 ex parte reexam
  - o Consulting
    - 5 patent cases as consultant
    - 1 product liability case as consultant
- **ACTIVE / STAYED**
  - o 1 patent case to expert reports (stayed before deposition)
  - o 1 patent case as consultant (stayed)

James R. Bress
Curriculum Vitae

**JAMES BRESS
LITIGATION AND PATENT PROSECUTION
CASE OVERVIEWS**

Patent non-infringement and invalidity to trial (closed)
- Metaswitch v Genband (Baker Botts) (Judge Gilstrap: Eastern District of Texas)
  - Expert for defendant (Genband)
  - Three patents (VoIP, telecommunications networks and features)
  - Non-infringement, invalidity, non-infringing alternatives, reports, depositions, trial testimony
  - Closed 2016 (no infringement found at trial)

Patent infringement and validity to depositions (closed)
- Lucent (v Dell et al), Kirkland & Ellis
  - Expert for plaintiff (Lucent)
  - Patent: Caller-ID signaling and receiver
  - Infringement, validity, reports, deposition
  - Closed 2007 (Case dismissed on MSJ: surrender in previous inter partes review)

Patent infringement to depositions (closed)
- Securus v GTL, Kellogg, Huber, Hansen, Todd, Evans & Figel, P.L.L.C.
  - Expert for counter-claim plaintiff (GTL)
  - Two patents: Telephone system features and call records analysis: prison applications
  - Infringement, non-infringing alternatives, reports, deposition, product analysis, site inspections
  - Closed 2015 (patents invalidated by PTAB as abstract)

TCPA lawsuit defense (Telecommunications Consumer Protection Act) to deposition (closed)
- Richard Newland v Rubio's Restaurants, Oliva and Associates
  - Expert for defendant (Rubio's Restaurants, Inc.)
  - TCPA / FCC rules related to Client's telephone system operations
  - Research, consulting, telephone system analysis, mobile telephone call records analysis, consulting on the FCC's TCPA related rules and Report & Order releases, site analysis
  - Reports / declaration, deposition
  - Closed 2014 (Settled)

Patent infringement to expert reports without deposition (stayed)
- GTL v Securus. Kellogg, Huber, Hansen, Todd, Evans & Figel, P.L.L.C.
  - Expert for plaintiff (GTL)
  - Infringement, non-infringing alternatives, reports, product analysis, site inspections
  - Three patents: VoIP telephone system access control and call recording: prison
  - Stayed 2015 for IPRs outcomes

James R. Bress **Curriculum Vitae**

JAMES BRESS
LITIGATION AND PATENT PROSECUTION
CASE OVERVIEWS

IPRs (depositions, declarations, petition review) (closed)
- Expert for petitioner: Genband
  - Metaswitch Patent: 8,687,640: VoIP SIP / IMS media gateway
  - Baker Botts
  - Closed 2016, trial instituted: all claims (minus one), all claims found unpatentable
- Expert for petitioner: Genband
  - Metaswitch Patent: 8,687,640: VoIP SIP / IMS media gateway
  - Baker Botts
  - Closed 2016, trial instituted: all claims (minus one), all claims (minus one) found unpatentable
- Expert for petitioner: GTL
  - Securus Patent: 8,135,115: VoIP telecommunications conferencing and recording systems
  - Sterne, Kessler, Goldstein & Fox P.L.L.C.
  - Closed 2016, trial instituted: all claims, all claims found unpatentable
- Expert for petitioner: GTL
  - Securus Patent: 7,961,860: Telecommunications event detection and processing
  - Sterne, Kessler, Goldstein & Fox P.L.L.C.
  - Closed 2015, trial not instituted

Inter partes reexam (declarations) (closed)
- Expert for patent owner: ClassCo
  - ClassCo Patent: 6,970,695: Audible Caller-ID
  - David Quinlan PA
  - Closed 2014 (all claims rejected)

Ex parte re exam (declarations) (closed)
- Expert for patent owner: ClassCo
  - ClassCo Patent: 6,970,695: Audible Caller-ID
  - David Quinlan PA
  - Interview with examiners (convinced examiner to reverse earlier decision and allow claims)
  - Closed 2012 (claims allowed)

Patent non-infringement and invalidity as expert consultant (stayed)
- {client confidential while case is active}, Jones Day
  - Expert for defendant ({confidential})
  - Patent: VoIP / Mobile: Instant messaging and call control
  - Consulted on patent and prosecution file histories, product analysis
  - Stayed 2017

**James R. Bress
Curriculum Vitae**

**JAMES BRESS
LITIGATION AND PATENT PROSECUTION
CASE OVERVIEWS**

Patent non-infringement and invalidity as expert consultant (closed)
- IAS LLC v XO Communications LLC, BakerHostetler
  - Expert for defendant (XO Communications)
  - Patent: Protocols related to V.90 modems, modem standards, product analysis
  - Research, consulting, standards analysis, product analysis
  - Settled 2015
- Reese v Samsung Telecommunications L.P., et al, Kirkland & Ellis
  - Expert for defendant (Samsung Telecommunications L.P., et al)
  - Patent: Telephone features, Caller-ID
  - Research, consulting, product analysis
  - Settled 2007
- Reese v RIM, Howrey
  - Expert for defendant (RIM)
  - Patent: Telephone features, Caller-ID
  - Research, consulting, product analysis
  - Settled 2006
- Reese v Atlinks Inc., Sacco & Associates P.A.
  - Expert for defendant (Atlinks Inc.)
  - Patent: Telephone features, Caller-ID
  - Research, consulting, product analysis
  - Settled 2006

Patent infringement and validity as expert consultant (closed)
- MagicJack VocalTec Ltd. (Y-Max) v NetTalk.com, Inc., Fenwick & West LLP
  - Expert for plaintiff (MagicJack VocalTec Ltd. (Y-Max))
  - Patent: VoIP telephone gateway
  - Research, consulting, product analysis, product inspections
  - Settled 2012

1 product liability case (closed)
- Barry vs. Audiovox, Don, Galleher & Saliman
  - Expert for defendant (Audiovox)
  - Mobile handset acoustic limiting and safety: Complaint for damage to hearing due to potential unsafe / improper design of a cellular telephone handset's audio and acoustics.
  - Product testing, standards analysis
  - Settled 2008

James R. Bress
Curriculum Vitae

JAMES BRESS LITIGATION AND PATENT PROSECUTION CASE DETAILS (REVERSE CHRONOLOGICAL)		
Case Information	**Services Provided**	**Status and Case Outcome**
Non-infringement / Invalidity {client confidential: active case} Jones Day Patent: VoIP / Mobile: Instant messaging and call control	**Expert for defendant** ({confidential}) • Patent prosecution analysis • Product analysis • Standards analysis • Consulting	**STAYED** (January 2017)

Non-infringement / Invalidity Metaswitch v Genband Baker Botts Nick Schuneman, Clarke Stavinoha, Chad Walters
 	
2:14-cv-744 3 Patents:
1. 8,687,640 (SIP / IMS media gateway)
2. 8,611,522 (IP/CS networks call processing)
3. 8,488,768 (Unified voicemail box)
	Expert for defendant (Genband)
	• Trial testimony
	• Trial related demonstratives
	• Deposition #1: (2015-10-07)
	• Deposition #2: (2015-10-08)
	• Expert reports:
	  ○ Invalidity
	  ○ Non-infringement (rebuttal)
	  ○ Non-infringing alternatives
	• Evidence research / analysis:
	  ○ Standards analysis
	  ○ Product analysis
	  ○ Prior art
	• Consulting
		CLOSED (March 2016)
		
		• Trial completed
		• Judge Gilstrap: Eastern Dist. TX
		• Jury found non-infringement for all 3 patents

Inter partes review (IPR) Baker Botts Nick Schuneman, Clarke Stavinoha, Chad Walters
 	
IPR2015-01456 Metaswitch Patent: 8,687,640 (SIP / IMS media gateway)
	Expert for petitioner (Genband)
	• Deposition (2016-04-19)
	• Expert declaration
	• Petitions review
	• Evidence research / analysis:
	  ○ Prior art
	  ○ Product analysis
	• Consulting
		CLOSED (December 2016)
		
		• PTAB instituted trial on all but one claim (13)
		• All claims found unpatentable

James R. Bress
Curriculum Vitae

JAMES BRESS LITIGATION AND PATENT PROSECUTION CASE DETAILS (REVERSE CHRONOLOGICAL)		
Case Information	**Services Provided**	**Status and Case Outcome**
Inter partes review (IPR) Baker Botts Nick Schuneman, Clarke Stavinoha, Chad Walters IPR2015-01457 Metaswitch Patent: 8,687,640 (SIP / IMS media gateway)	**Expert for petitioner** (Genband) • Deposition (2016-04-20) • Expert declaration • Petitions review • Evidence research / analysis: ○ Prior art ○ Product analysis • Consulting	**CLOSED** (December 2016) • PTAB instituted trial on all but one claim (14) • All claims (minus claim 10) found unpatentable
Inter partes review (IPR) Sterne, Kessler, Goldstein & Fox P.L.L.C. Lauren C. Schleh, Michael Specht IPR2015-01226 Securus Patent: 8,135,115 (telephone conferencing and recording systems)	**Expert for petitioner** (GTL) • Deposition (2016-02-17) • Expert declaration • Petitions review • Claim construction consulting • Prior art research / analysis • Consulting	**CLOSED** (December 2016) • PTAB instituted trial on all claims • All claims found unpatentable
Inter partes review (IPR) Sterne, Kessler, Goldstein & Fox P.L.L.C. Azin Neishaboori, Nicholas J. Nowak, Michael Specht IPR2015-01223 Securus Patent: 7,961,860 (telecommunications event detection and processing)	**Expert for petitioner** (GTL) • Expert declaration • Petitions review • Claim construction consulting • Prior art research / analysis • Consulting	**CLOSED** (December 2015) • PTAB denied trial institution

James R. Bress
Curriculum Vitae

JAMES BRESS LITIGATION AND PATENT PROSECUTION CASE DETAILS (REVERSE CHRONOLOGICAL)		
Case Information	**Services Provided**	**Status and Case Outcome**

Infringement
Securus v GTL (counter-claim)
Kellogg, Huber, Hansen, Todd, Evans & Figel, P.L.L.C.
Evan Leo, J.C. Rozendaal, Nic Hunter, Chris Funk, Jean Paul (Yugo), Nagashima, Courtney S. Elwood
 	
3:13-CV-3009-K
2 Patents:
1. 7,039,171
(telephone system call records analysis)
2. 7,085,359
(telephone system call records analysis)
	Expert for counter-claim plaintiff
	(GTL)
	• Deposition (2015-07-31)
	• Expert report (infringement)
	• Non-infringing alternatives
	• Claim construction consulting
	• 30 (b)(6) deposition support
	• Evidence research / analysis:
	  o Product analysis
	  o Site inspection
	• Consulting
		CLOSED
		(November 2015)
		
		• Patents invalidated: abstract

Infringement
GTL v Securus
Kellogg, Huber, Hansen, Todd, Evans & Figel, P.L.L.C.
Evan Leo, J.C. Rozendaal, Nic Hunter, Chris Funk, Jean Paul (Yugo), Nagashima, Courtney S. Elwood
 	
3:14-CV-00829-K
3 Patents:
• 7,551,732
(VoIP telephone system with recording call: prison)
• 7,783,021
(VoIP telephone system with access control: prison)
• 7,853,243
(VoIP telephone system with access control: prison)
	Expert for plaintiff
	(GTL)
	• Expert report (infringement)
	• Non-infringing alternatives
	• Claim construction consulting
	• 30 (b)(6) deposition support
	• Evidence research / analysis:
	  o Product analysis
	  o Site inspection
	• Consulting
		STAYED
		(August 2015)
		
		7,551,732 IPR: claims 1–8 and 11–27: unpatentable.
		Asserted claims: 1, 2, 5, 6, 8, **10**, 12, 15, 17, 20, 22, 23
		
		7,783,021: IPR: **Denied institution**
		Asserted claims: 1, 4, 5, 7, 13, 15, 16, 17, and 18
		
		7,853,243: IPR: claims 1-6 found to be **patentable**
		Asserted claims: 1, 3, and 4

James R. Bress
Curriculum Vitae

JAMES BRESS LITIGATION AND PATENT PROSECUTION CASE DETAILS (REVERSE CHRONOLOGICAL)		
Case Information	**Services Provided**	**Status and Case Outcome**
Non-infringement / Invalidity IAS LLC v XO Communications LLC BakerHostetler John (Jack) P. Corrado, Charles (Chuck) C. Carson, Brian Saunders 1:14-cv-00754-RGA Patent: 6,072,825 (Protocols related to V.90 modems)	**Expert for the defendant** (XO Communications LLC) • Evidence research / analysis: ○ Prior art ○ Standards analysis ○ Product analysis • Consulting	**CLOSED** (2015) • Settled
Inter partes re-exam David Quinlan PA David Quinlan Control No. 95/002,109 ClassCo Patent: 6,970,695 (Audible Caller-ID)	**Expert for Patent Owner** (ClassCo) • Expert declarations • Prior art research / analysis • Consulting	**CLOSED** (January 2014) • All claims rejected
TCPA lawsuit defense Richard Newland v Rubio's Restaurants, Inc. Oliva and Associates Stephen F. Yurcich 37-2013-00062892-CU-MC-NC (Superior Court for the State of California 2 for the County of San Diego - North County Division)	**Expert for defendant** (Rubio's Restaurants) • Deposition • Expert declaration • Research and consulting • On-site telephone system analysis • Mobile telephone service call records analysis • Consulting on FCC's TCPA rules and Report & Order releases	**CLOSED** (October 2014) • Settled

James R. Bress
Curriculum Vitae

JAMES BRESS LITIGATION AND PATENT PROSECUTION CASE DETAILS (REVERSE CHRONOLOGICAL)		
Case Information	**Services Provided**	**Status and Case Outcome**
Ex parte re-exam David Quinlan PA David Quinlan Control No. 90/011,679 ClassCo Patent: 6,970,695 (Audible Caller-ID)	**Expert for Patent Owner** (ClassCo) • Expert declarations • Prior art research / analysis • Consulting • Participated in interview with patent examiners at the USPTO providing information critical to the examiner's decision making.	**CLOSED** (June 2012) • All claims allowed
Infringement / Validity MagicJack VocalTec Ltd. (Y-Max) v NetTalk.com, Inc. Fenwick & West LLP Saina S. Shamilov, Elizabeth J. White 9:12-cv-80360-DMM Patent: 6,731,751 (VoIP: telephone gateway)	**Expert for the plaintiff** MagicJack VocalTec Ltd. (Y-Max) • Expert declarations • Evidence research / analysis: ○ Prior art ○ Product analysis ○ Product physical inspection • Consulting	**CLOSED** (December 2012) • Settled
Infringement / Validity Lucent vs. Dell and Gateway Kirkland & Ellis James Marina 02-CV-2060 B (CAB) Patent: 4,582,956 (Caller-id receiver)	**Expert for the plaintiff** (Lucent) • Deposition • Expert report (infringement) • Expert rebuttal report (validity) • Evidence research / analysis: ○ Prior art ○ Standards analysis ○ Product analysis ○ Software inspection ○ Product testing • Consulting	**CLOSED** (2007) • Case dismissed on MSJ • Due to surrender in previous inter partes review

James R. Bress
Curriculum Vitae

JAMES BRESS		
LITIGATION AND PATENT PROSECUTION		
CASE DETAILS (REVERSE CHRONOLOGICAL)		
Case Information	**Services Provided**	**Status and Case Outcome**

Non-infringement / Invalidity
 Reese v Samsung Telecommunications L.P., et al
 Kirkland & Ellis
 Richard Koehl, Paul Bondor, Andrew Heinz
 	
 2:05-CV-00415-DF
 Patent: 6,427,009
 (Telephone features, Caller-ID)
	Expert for defendant
	 (Samsung Telecommunications L.P., et al)
	 • Evidence research / analysis:
	    o Prior art
	    o Standards analysis
	    o Product analysis
	 • Consulting
		CLOSED
		 (2007)
		
		 • Settled

Product liability Barry vs. Audiovox Don, Galleher & Saliman Shelley B. Don Mobile handset acoustic limiting and safety. Complaint for damage to hearing due to potential unsafe / improper design of a cellular telephone handset's audio and acoustics.	**Expert for defendant** (Audiovox) • Product testing and reporting (acoustic performance of cellular telephone handsets) • Standards analysis • Consulting	**CLOSED** (2008) • Settled

Non-infringement / Invalidity
 Reese v RIM
 Howrey
 Peter J. Chassman, Tyler Van Houtan
 	
 Patent: 6,427,009
 (Telephone features, Caller-ID)
	Expert for defendant
	 • Evidence research / analysis:
	    o Prior art
	    o Standards analysis
	    o Product analysis
	 • Consulting
		CLOSED
		 (2006)
		
		 • Settled

Non-infringement / Invalidity
 Reese v Atlinks Inc.
 Sacco & Associates P.A.
 Duane Morris LLP
 	
 Patent: 6,427,009
 (Telephone features, Caller-ID)
	Expert for defendant
	 • Evidence research / analysis:
	    o Prior art
	    o Standards analysis
	    o Product analysis
	 • Consulting
		CLOSED
		 (2006)
		
		 • Settled

**James R. Bress
Curriculum Vitae**

Intellectual Property (IP) Consulting

Research and documentation to prepare patent applications to protect the intellectual property of a start-up company: Audigence Inc. Patent applications were in the fields of telecommunications and improvements for hearing and speech technologies.

Professional Affiliations

- Chairman (2015 to present), Telecommunication Industry Association (TIA) TR-41 engineering committee for standards related to communications product performance and accessibility.
- Chairman (2000 to 2007), and from 2011 to 2015, TIA TR-41.3 engineering sub-committee for standards related to communications product performance and accessibility.
- Vice-Chairman (2007 to 2011) TIA TR-41.3 engineering sub-committee for standards related to communications product performance and accessibility.
- Member: IEEE
- Tau Beta Pi

James R. Bress
Curriculum Vitae

Patents & Publications

US Patent No.   Title
5,519,774   Method and system for detecting at a selected station an alerting signal in the presence of speech
5,570,420   Customer premise equipment network integrator
7,076,031   System and Method for Telephone Signal Collection and Analysis
9,020,621   Network Based Media Enhancement Function Based on an Identifier

TIA Publications (Chairman, Editor, or Major Contributor)

1. TIA-4953-A-2015 *Telecommunications – Telephone Terminal Equipment – Amplified Telephone Measurement Procedures and Performance Requirements* (**Accessibility**)

2. TIA-810-B-2006 *Telecommunications – User Premises Equipment – Transmission Requirements for Narrowband Digital Telephones* (**VoIP – Narrowband**)

3. TIA-920.110-A-2011 *Telecommunications Telephone Terminal Equipment Transmission Requirements for Wideband Digital Wireline Telephones with Handset* (**VoIP – Wideband**)

4. TIA-920.120-A-2011 *Telecommunications Telephone Terminal Equipment Transmission Requirements for Wideband Digital Wireline Telephones with Speakerphone* (**VoIP – Wideband**)

5. TIA-920.130-A-2011 *Telecommunications Telephone Terminal Equipment Transmission Requirements for Wideband Digital Wireline Telephones with Headset* (**VoIP – Wideband**)

6. ANSI/TIA-1083-B-2015 *Telecommunications – Telephone Terminal Equipment – Handset Magnetic Measurement Procedures and Performance Requirements* (**Accessibility: Hearing Aid Compatibility**)

7. ANSI/TIA-1063-A-2015 *Telecommunications – User Premises Equipment – Analog Telephone Port Requirements for Packet-based User Premises Terminal Adapters* (**VoIP – Gateways**)

8. ANSI/TIA-777-A-2003 *Telecommunications - Telephone Terminal Equipment – Caller Identity and Visual Message Waiting Indicator Equipment Performance Requirements* (**Caller-ID**)

9. ANSI/TIA-855-A-2011 *Telecommunications Telephone Terminal Equipment – Stutter Dial Tone Detection Device Performance Requirements*

10. ANSI/TIA-470.310-D-2010 *Telecommunications – Telephone Terminal Equipment – Cordless Telephone Range Measurement Procedures*

11. ANSI/TIA-470.320-C-2006 *Telecommunications – Telephone Terminal Equipment – Cordless Telephone Operation and Feature Performance Requirements*

12. ANSI/TIA-470.330-C-2012 *Telecommunications – Telephone Terminal Equipment – Digital Telephone Answering Device Performance Requirements*

13. ANSI/TIA-470.110-D-2014 *Telecommunications – Telephone Terminal Equipment – Handset Acoustics Performance Requirements for Analog Telephones*

14. ANSI/TIA-470.120-C-2011 *Telecommunications – Telephone Terminal Equipment – Transmission Requirements for Analog Speakerphones*

15. ANSI/TIA-470.130-C-2009 *Telecommunications – Telephone Terminal Equipment – Transmission Requirements For Analog Telephones with Headsets*

16. ANSI/TIA-470.210-E-2013 *Telecommunications – Telephone Terminal Equipment – Resistance and Impedance Performance Requirements for Analog Telephones*

17. ANSI/TIA-470.220-D-2014 *Telecommunications – Telephone Terminal Equipment – Alerter Acoustics Performance Requirements for Analog Telephones*

18. ANSI/TIA-470.230-C-2005 *Telecommunications – Telephone Terminal Equipment – Network Signaling Performance Requirements for Analog Telephones*

Bellcore Publications (Authored or Co-Authored)

1. Bellcore SR-3363 (Issue 1, 1995) *Testing Guidelines for Switches and Servers With Analog Type 1, 2, and 3 Interfaces as Described in SR-INS-002726*
   [Caller-ID / ADSI Server (Screen Phone / Smart Phone) Network Testing Recommendations]

2. Bellcore SR-3004 (Issue 2, 1995) *Testing Guidelines for Analog Type 1, 2, and 3 CPE as Described in SR-INS-002726*
   [Caller-ID / ADSI CPE (Screen Phone / Smart Phone) Testing Recommendations]

3. Bellcore GR-30-CORE (Issue 1, 1994) *LSSGR: Voiceband Data Transmission Interface Section 6.6*
   [Caller-ID / ADSI CPE (Screen Phone / Smart Phone) Network Signaling Requirements]

4. Bellcore TR-NWT-001401 (Issue 1, 1993) *Visual Message Waiting Indicator Generic Requirements*

5. Bellcore SR-TSV-002568 (Issue 1, 1993) *Speech Test Tapes for Customer Premises Equipment Signal Detectors*
   [Bellcore Caller-ID Speech Test Tapes]

6. Bellcore SR-TSV-002578 (Issue 1, 1993) *A Method and Apparatus for Detecting a Dual Tone Signal in the presence of Speech*

7. Bellcore SR-INS-002726 (Issue 1, 1993) *Classes of Customer Premises Equipment*

8. Bellcore TR-NWT-001273 (Issue 1, 1992) *Generic Requirements for an SPCS to Customer Premises Equipment Data Interface for Analog Display Services*
   [ADSI Network Signaling and Server Interface Requirements]

9. Bellcore SR-INS-002461 (Issue 1, 1992) *Customer Premises Equipment Compatibility Considerations for the Analog Display Services Interface*
   [ADSI Telephone Terminal (Screen Phone / Smart Phone) Signaling and User Interface Display Mapping Rules Recommendations]

10. Bellcore SR-TSV-002476 (Issue 1, 1992) *Customer Premises Equipment Compatibility Considerations for the Voiceband Data Transmission Interface*
    [Caller-ID / ADSI Screen Phone / Smart Phone Signaling Recommendations]

Telecommunications Essentials

The Complete Global Source
for Communications Fundamentals,
Data Networking and the Internet,
and Next-Generation Networks

Lillian Goleniewski

Chapter 5

The PSTN

This chapter talks about the public switched telephone network (PSTN). It talks about what comprises the PSTN, what sorts of technologies have been used to complete the connections, how the signaling systems operate, and what the basic backbone architectures entail in terms of components and transmission capacities. This chapter also discusses intelligent networks (INs) and what they promise in terms of service logic and feature availability. Finally, this chapter describes some of the trends in the evolution of the PSTN that will support the new generation of applications.

■ The PSTN Infrastructure

Our views about what a network should be designed to support and what the infrastructure should be comprised of have changed quite a bit over the years, as applications and technology have changed. Before discussing what is needed in a network today, this chapter takes a look at how the PSTN infrastructure evolved and where it is today.

The traditional PSTN infrastructure was specifically designed to support only voice communications. At the time this infrastructure was being designed, we had no notion of data communications. Initially the traffic type the PSTN was designed to support was continuous real-time voice.

Another variable that's important to the design of the PSTN has to do with the length of calls. Most voice calls are quite short, so the circuit switches in the PSTN are engineered for call durations of three minutes or less. The average Internet

113

session, on the other hand, lasts around an hour. This means that increased Internet access through the PSTN has, in some locales, put a strain on the local exchanges. If a circuit switch is blocked because it is carrying a long Internet session, people may not be able to get a dial tone. There are several solutions to this problem. For example, as discussed in Chapter 10, "Next-Generation Networks," we can apply intelligence in front of some exchanges so that calls destined for ISPs can be diverted over a packet-switched network to the ISP rather than being completed on a circuit-switched basis through the local exchange.

Yet another variable that's important to the design of the PSTN has to do with what it was designed to support. The capacities of the channels in the PSTN are of the narrowband generation—they are based on 64Kbps channels. The worldwide infrastructure to accommodate voice communications evolved to include a series of circuit switches. Different switches are used based on the locations to which they're connecting. The switches have a high degree of intelligence built into them, both for establishing the communications channels and for delivering the service logic to activate a growing array of features. In the traditional framework, the monolithic switches in the network had all the smarts. The switch manufacturer and the carrier worked together very closely, and the carrier was not able to introduce new features and services into a particular area until a software release was available for the switch platform through which the neighborhood was being serviced. Thus, carriers were often unable to roll out new services and features because they hadn't yet received the new software releases from the switch manufacturers. Over time, we have separated the functions of switching and connection establishment from the functions involved in the intelligence that enables various services and features to be activated.

The traditional PSTN is associated with highly developed, although not necessarily integrated, operational support systems (such as billing systems, provisioning systems, network management systems, customer contact systems, and security systems). These systems have very well-developed business processes and techniques for managing their environments. But the various systems' databases cannot yet all speak to one another to give one comprehensive view. (But at least those systems exist, unlike in the public Internet, where the operational support systems are only now beginning to emerge to help manage that environment.)

The backbone of the traditional PSTN was largely based on a generation that we call the Plesiochronous Digital Hierarchy (PDH), which includes the T-carrier, E-carrier, and J-carrier standards. The local loop of the PSTN was provisioned as a twisted-copper-pair analog subscriber line.

Service Providers

Many abbreviations and acronyms are used to define the various players and the parts of the network in which they play. Some telcos can and do fulfill more than

one of these functions; the extent to which they can or do fulfill more than one of these functions partly depends on the policy, regulatory, and licensing conditions that prevail in different countries. The following terms are largely used in the United States, but they are important to the discussion in this chapter because they illustrate the functions service providers are addressing:

- **PTO**—PTO stands for *public telecommunications operator*, which is the name for an incumbent carrier in places other than the United States.

- **VAN**—VAN stands for *value-added network provider*. This term originated around 1970 and was applied to companies that were competing to provide telecommunications services, specifically with offerings focused on data communications and data networking. VANs provided more than a simple pipe from Point A to Point B. They provided some additional intelligence in the network, to, for example, perform error detection and correction, or to convert protocols or languages that different computers speak so that you could have interoperability across the network.

- **LEC**—In the local environment we use the acronym LEC for *local exchange carrier*. There was originally no competition among LECs, but as soon as competition in the local loop picked up, LECs were segmented into ILECs, CLECs, and DCLECs.

- **ILEC**—The ILEC is the *incumbent local exchange carrier*, the original common carrier that either once had, or in some countries still has, monopoly rights in the local loop. For most residents in the United States, this would be one of the four "baby Bells"—Qwest Communications International, SBC Communications, BellSouth Corporation, and Verizon Communications.

- **CLEC**—The CLEC is the *competitive local exchange carrier*. CLECs came about as a result of the Telecommunications Act of 1996, which opened up competition in the local loop. The CLEC is the competitor to the ILEC. Although the decline of the telecommunications economy in 2000 and 2001 forced several CLECs out of business, there are still some CLECs in the United States, and they currently focus on delivering dial tone to business customers.

- **DCLEC (or DLEC)**—DCLEC stands for *data competitive local exchange carrier*. The DCLEC is a company that is specifically focused on supporting data services (for example, providers that offer DSL services to end users).

- **ELEC**—ELEC stands for *Ethernet local exchange carrier*. The ELEC specializes in providing Ethernet solutions in the local loop and metro area.

- **IXC**—The *interexchange carrier* (IXC) is the carrier for long-distance and international communications. AT&T Corporation, WorldCom, Sprint, Qwest, and Verizon are the primary IXCs in the United States. Unless certain

stringent requirements imposed by the Federal Communications Commission are met, an IXC cannot offer long-distance services in the areas where it is also the ILEC.

- SP—Because so many lines are being blurred today by bundled services and bundled territories of operation, the basic term *service provider* (SP) is commonly used to refer generically to providers of different types of services.

Network Access

Figure 5.1 is a simple diagram of network access. On the left-hand side is the customer environment, which includes residences (single-line instruments being served by an access line) and business premises (with onsite telephone systems such as private branch exchange [PBXs] or key telephone systems—smaller site systems for installations where there are 50 or fewer employees). Those in the customer environment are connected to the PSTN via access lines. The *access network*, or the *local loop* we so often talk about, includes whatever equipment resides at the customer premise (that is, the customer premises equipment [CPE]), the access line leading to the local exchange, the components at the local exchange on which those access lines terminate (that is, the distribution cross-connects), and the logic used to help control the flow of traffic over the access lines. In the United States, competition is allowed in the local loop, and a myriad of players are interested in owning the local loop (for example, Internet service providers [ISPs], wireless operators, cable TV companies, power utilities). However, worldwide, the incumbent local providers continue to dominate the local loop, and, as usual, politics and economics are principal factors in delaying the mass deployment of high-speed residential access.

The local exchange, in the center of Figure 5.1, is the backbone, or the core, of the network. From the local exchange, we can establish connections into the other providers, such as IXCs for long distance, international carriers for overseas calls, cellular providers, and ISPs.

Services Beyond the Local Loop

Traditionally, we have thought of the local loop as leading to the home or to the business and ending there. But the need for additional bandwidth and capability is now shifting: We need these things within the premise, as well as on the local loop. It is therefore a logical extension for the service provider to not only give you access lines and termination, but also to provide you with the home area networking facilities you need in order to have an end-to-end broadband package. Chapter 15, "The Broadband Home and HANs," talks more about this.
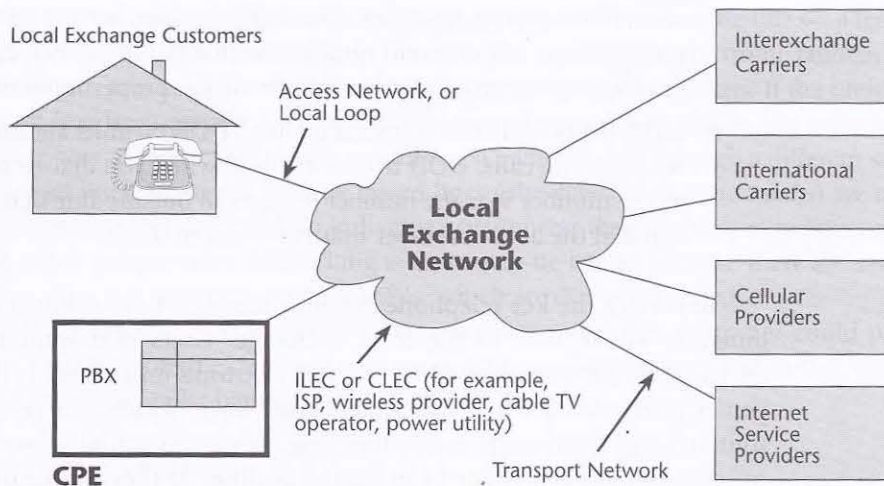
Figure 5.1 Network access

The underlying network access facilities can be either analog or digital loops, and they connect the exchanges to the customer premises. At the customer premises there are the network interfaces, CPE, premises distribution systems where wiring is cross-connected, and network interfaces. The equipment for providing switch access services includes line-termination cards, carrier and multiplexer equipment, and local exchange switching capabilities that support addressing, supervisory alerting, call progress, and other signaling functions.

Access Services

The main categories of access services are trunks, business lines for key telephone systems, centrex service, leased lines, and residential subscriber lines.

Trunks are used to provide connections into the PBX environment. There are three subcategories of trunks:

- **Two-way local exchange trunks**—On these trunks, traffic flows in both the incoming and outgoing directions.

- **DID trunks**—Direct inward dialing (DID) trunks are designed for only incoming calls. A benefit of DID trunks is that they enable the dialed number to ring directly on a user's phone rather than having to go through a centralized attendant. If the population knows whom they want to call directly, and if you want to ease the process of connecting the call, this can be a very useful feature. Another benefit of DID trunks is that they make it

seem like a private line goes directly to the user, but with DID you can support perhaps 100 different numbers with a group of only 25 to 35 trunks (traffic engineering is used to determine the proper number of trunks).

▪ **DOD trunks**—Direct outward dialing (DOD) trunks are used specifically for outgoing calls. DOD trunks are used when you dial an access code such as the number 9 or the number 8 to get an outside-line dial tone before you can dial the actual number that you want to reach.

To service the key telephone systems, business lines connect the network termination at the user to the local exchange. Users that want to use the local exchange as if it were their PBX rent centrex trunks on a monthly basis. Large companies often access the network via leased lines, which can be a very expensive solution, and home users access the network via residential subscriber lines.

Access lines can either be in analog facilities or they can be digital carrier services. Analog transmission is often called *plain old telephone service* (POTS for short). Three main types of digital services are offered by using twisted-pair cable. The first type of digital services involves T-1 access (at 1.5Mbps), E-1 access (at 2.048Mbps), and J-1 access (at 1.544Mbps). The second type of digital services is narrowband ISDN (N-ISDN) services, including Basic Rate Interface (BRI) for residences and small businesses and Primary Rate Interface (PRI) for larger businesses. The third type of digital services is the xDSL subscriber lines and high-speed digital subscriber lines that enable the all-important applications of Internet access and multimedia exploration. (Chapter 3, "Transmission Media: Characteristics and Applications," describes the digital services in more detail.)

Transport Services

Transport services are the network switching, transmission, and related services that support information transfer between the originating and terminating access facilities. The underlying facilities include local exchanges and tandem switches, toll and transit switches, international gateways, and interoffice transmission equipment. Transport services include switched services, nonswitched services, and virtual private networks (VPNs).

Switched Services

There are two main types of switched services: public and private.

Switched public services include local calling, long-distance calling, toll-free calling, international calling, directory assistance, operator assistance, and emergency services.

Switched private services can be switchable either because they are deployed within the CPE or because they are deployed on a carrier basis. With CPE-based ser-

vices, you can add capabilities to the telephone systems onsite in the PBXs—a feature called *electronic tandem networking*. For example, you can use electronic tandem networking to gain some flexibility in routing around congestion points: If the preferred leased line from Switch A to Switch B is occupied or not available, the switch can decide how to reroute that traffic to still reach Switch B, but through a different series of leased lines. However, because leased lines (also referred to as *tie trunks*) are mileage sensitive and dedicated to individual customers, they are very expensive; thus, not much private voice networking is done over tie trunks because there are several more attractive solutions, such as VPNs, which are discussed shortly.

With carrier-based switched private services, a centrex customer could partition and implement extensions across multiple local exchanges and in this way be able to switch traffic between those locations.

Nonswitched Services

Nonswitched services include leased lines, foreign exchange (FX) lines, and off-premises exchanges (OPXs). With leased lines, two locations or two devices are always on, using the same transmission path.

FX lines allow you to make a toll call appear to be a local call. For example, you might have a dedicated leased line that runs from your customer premise to a local exchange in a distant area where you call large numbers of customers. When anyone behind your PBX dials a number associated with that foreign local exchange, the PBX automatically selects the FX line. The dial tone the caller receives is actually coming from the distant local exchange, and the call proceeds as if it were a local call. The tradeoff with FX lines is that although you are not charged per call for your long-distance calls to the specified exchange, you pay a flat monthly fee for the leased line and you have to apply some traffic engineering to ensure that you're not making people wait for the FX line to become available. So with FX lines, you need to find the right balance point between reducing costs and ensuring a high level of service.

OPXs are used in distributed environments, such as a city government. Say that the city government has public works stations, libraries, fire stations, and parks and recreation facilities that are too far from the PBX to be served by the normal cabling. The city uses an OPX setup: It leases a circuit from the PBX to the off-premise location and ties it in as if it were part of that PBX. City government employees can then call one another, using their normal extension plan, their call accounting information can be accumulated so that cost allocations can be performed, and the employees can have access to the full suite of features that a business PBX offers.

VPNs

Although you might think that VPNs are related to the Internet or to Internet Protocol (IP) and are a somewhat new development, they actually originated in the circuit-
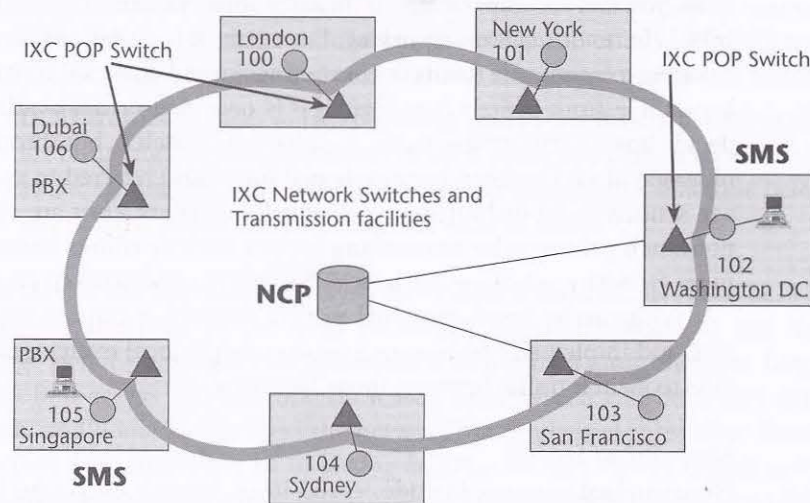
Figure 5.2 An example of a VPN

switched network environment, with AT&T's software-defined network (SDN) in the early 1980s. A VPN is a concept, not a technology platform or a set of networking techniques. A VPN defines a network in which customer traffic is isolated over shared-service provider facilities, so as more customers share the same facilities, their costs go down. The purpose of a VPN, then, is to reduce the high cost of leased lines, while still providing high quality of service and guaranteeing that private traffic has capacity between locations. Figure 5.2 shows an example of a VPN.

The underlying facilities of a VPN include the carrier public network, augmented by network control points and service management systems. Under computer control, the traffic is then routed through the public network in a manner that makes the VPN service seem like a facilities-based private network. Access to the VPN can occur via dedicated access, leased lines, or carrier-switched access, using either an analog or a digital carrier.

The network control point represents a centralized database that stores a subscriber's unique VPN information. The network control point screens every call and then applies call processing in accordance with the customer-defined requirements. A common-channel signaling network connects the various network elements so that they can exchange information with each other in real-time. (Common-channel signaling is discussed later in this chapter, in the section "Signaling Systems.")

A service management system is used to build and maintain the VPN database. It allows customers to program specific functions to accommodate their particular

business applications. It transmits information to the network control points, with important instructions on a customer-by-customer basis. Thus, VPNs introduce to the realm of the PSTN a lower-cost alternative to building a private voice network.

PSTN Architecture

The PSTN includes a number of transmission links and nodes. There are basically four types of nodes: CPE nodes, switching nodes, transmission nodes, and service nodes.

CPE Nodes

CPE nodes generally refer to the equipment that's located at the customer site. The main function of CPE nodes is to transmit and receive user information. The other key function is to exchange control information with the network. In the traditional realm, this equipment includes PBXs, key telephone systems, and single-line telephones.

Switching Nodes

Switching nodes interconnect transmission facilities at various locations and route traffic through a network. They set up the circuit connections for a signal path, based on the number dialed. To facilitate this type of switching, the ITU standardized a worldwide numbering plan (based on ITU E.164) that essentially acts as the routing instructions for how to complete a call through the PSTN. The switching nodes include the local exchanges, tandem exchanges (for routing calls between local exchanges within a city), toll offices (for routing calls to or from other cities), and international gateways (for routing calls to or from other countries). Primary network intelligence is contained in the Class 4 switches (that is, toll offices switches) and Class 5 switches (that is, local exchange switches). The Class 4 toll switches provide long-distance switching and network features, and the Class 5 switches provide the local switching and telephony features that subscribers subscribe to. Figure 5.3 shows where the types of telephone exchanges are located.

The Local Exchange   The local exchange (also called the Class 5 office or central office) is where communications common carriers terminate customer lines and locate the switching equipment that interconnects those lines. This class office represents the local network. Every subscriber line location in a local exchange is assigned a number, generally seven or eight digits. The first three (or four) digits represent the exchange and identify the local exchange switch that serves a particular telephone. The last four digits identify the individual line number, which is a circuit that is physically connected from the local exchange to the subscriber. The traditional local exchange switch can handle one or more exchanges, with each
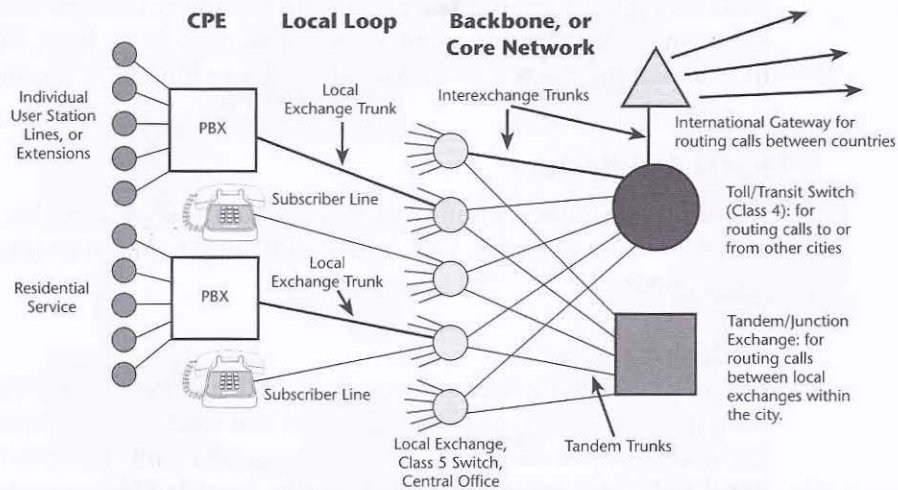
Figure 5.3   Types of telephone exchanges

exchange capable of handling up to 10,000 subscriber lines, numbered 0000 to 9999. In large metropolitan areas, it is common to find one local exchange building housing more than one local exchange switch and for each switch to handle five or more exchanges. These offices are sometimes referred to as *multi-entity buildings*.

The Tandem Office   The tandem office, or junction network, is an exchange that is used primarily as a switching point for traffic between local exchanges in a metropolitan area. It is an office that is used to interconnect the local end offices over tandem trunks in a densely settled exchange area where it is not economical for a telephone company to provide direct interconnection between all end offices. The tandem office completes all calls between the end offices but is not directly connected to subscribers.

The Toll Office   The toll office (also called the trunk exchange or transit switch) is a telephone company switching center where channels and toll message circuits terminate—in other words, where national long-distance connections are made. This is usually one particular exchange in a city, but larger cities may have several exchanges where toll message circuits terminate.

The International Gateway   An international gateway is the point to and from which international services are available in each country. Protocol conversion may take place in the gateway; in ITU terminology, this is called a *centre de transit* (CT). C1 and C2 international exchanges connect only international circuits. CT2

exchanges switch traffic between regional groups of countries, and CT1 exchanges switch traffic between continents. CT3 exchanges connect switch traffic between the national PSTN and the international gateway.

Transmission Nodes

Transmission nodes are part of the transport infrastructure, and they provide communication paths that carry user traffic and network control information between the nodes in a network. The transmission nodes include the transmission media discussed in Chapter 3, as well as transport equipment, including amplifiers and/or repeaters, multiplexers, digital cross-connects, and digital loop carriers.

Service Nodes

Service nodes handle *signaling*, which is the transmission of information to control the setup, holding, charging, and releasing of connections, as well as the transmission of information to control network operations and billing. A very important area related to service nodes is the ITU standard specification Signaling System 7 (SS7), which is covered later in this chapter.

The Transport Network Infrastructure

The transport network includes two main infrastructures. The first is the PDH, also known as T-carrier, E-carrier, and J-carrier wideband transmission standards. This infrastructure was first introduced in the early 1960s. The second infrastructure of the transport network is the Synchronous Digital Hierarchy (SDH; ITU terminology), also known as Synchronous Optical Network (SONET; ANSI terminology), which was first formalized and standardized in 1988. SDH/SONET is the second generation of digital hierarchy, and it is based on a physical infrastructure of optical fibers.

PDH and SDH/SONET are voice-centric circuit-switched network models that switch millions of 64Kbps circuits between various switching points. Each circuit is multiplexed numerous times for aggregation onto transmission facilities. Aggregation occurs at many points in the network: in the access network, within the local exchange, and throughout the interexchanges. Hence, a significant portion of the cost of a network goes to the equipment that performs this aggregation—the multiplexers and cross-connects in both the PDH and SDH/SONET environments.

The PDH Infrastructure

The term *Plesiochronous* makes PDH sound like a dinosaur, and in a way, it is—it's an outdated architecture from the standpoint of the data rates it offers. But the word *Plesiochronous* means "minute variations in timing," and that refers to the fact that

the PDH is an *asynchronous infrastructure*. Each network element—that is, each exchange, multiplexer, cross-connect, repeater, and so on—gets its clocking pulse from a different clocking source, and even though those clocking sources are synchronized, there are minute fluctuations in timing. To differentiate the beginning and the end of a conversation, we have to channelize conversations.

PDH was the first system designed to use digitized voice transmission. It was born of the telcos' desire to better use their cable facilities and to enhance the quality of calls. PDH was first used by telcos as a means of aggregating multiple voice channels into a single high-speed digital backbone. Standards that are used today for all-digital switching and transmission come from the original PDH specifications.

PDH defines several things: First, it's an integrated digital network, so it can carry a range of traffic, as long as that traffic is being presented in a digital manner. Therefore, PDH represented the first opportunity for users and carriers to combine voice and data traffic over the same pipes. Second, it specifies the different transmission levels or data rates, some of which are available for customers to subscribe to and others of which are used by operators internally within the backbones. Third, it defines within each of the transmission levels how many channels can be made available.

The T-, E-, and J-Carrier Standards

T-carrier, E-carrier, and J-carrier are PDH standards that are followed in different regions of the world: J-carrier is followed throughout Japan; T-carrier is followed throughout North America; and E-carrier is followed throughout Europe and the majority of other locations throughout the world, including large parts of Asia, Latin America, and Africa. Figure 5.4 compares these three standards. They all share one increment as a common denominator: 64Kbps. But each of the three standards multiplexes together a different number of these 64Kbps channels to derive higher transmission rates.

Having three separate standards—T-, E-, and J-carrier—means that we have to cross between systems that use different standards, and in doing so, we incur additional overhead.

Elements of the PDH Infrastructure

As shown in Figure 5.5, the following are the key elements of the PDH infrastructure:

- Transmission media
- Repeaters
- Channel service units (CSUs)
- Multiplexers
- Digital loop carriers (DLCs)
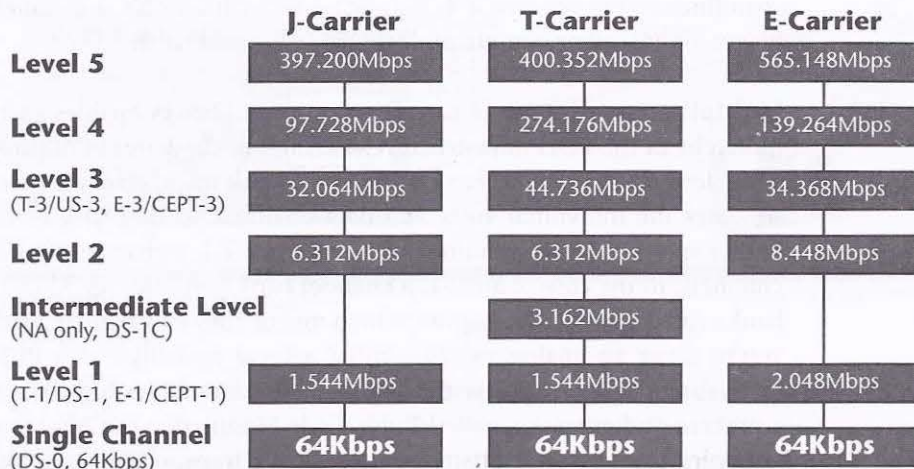- Digital cross-connect systems (DCSs)

	J-Carrier	**T-Carrier**	**E-Carrier**
Level 5	397.200Mbps	400.352Mbps	565.148Mbps
Level 4	97.728Mbps	274.176Mbps	139.264Mbps
Level 3 (T-3/US-3, E-3/CEPT-3)	32.064Mbps	44.736Mbps	34.368Mbps
Level 2	6.312Mbps	6.312Mbps	8.448Mbps
Intermediate Level (NA only, DS-1C)		3.162Mbps	
Level 1 (T-1/DS-1, E-1/CEPT-1)	1.544Mbps	1.544Mbps	2.048Mbps
Single Channel (DS-0, 64Kbps)	**64Kbps**	**64Kbps**	**64Kbps**

Figure 5.4   T-carrier, E-carrier, and J-carrier standards

Termination equipment (channel banks, multiplexers, digital cross-connect PBXs). — DSU/CSU — Digital transmission media (twisted copper pair, coaxial cable, microwave radio fiber) — DSU/CSU — Termination equipment (channel banks, multiplexers, digital loop carriers, digital cross-connects).

Customer Premises   **Local Exchange**
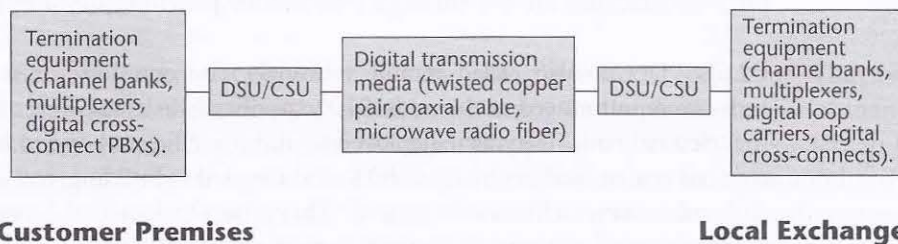
Figure 5.5   PDH components

Transmission media   PDH can include a wide variety of transmission media, and the type you use is contingent on the bandwidth you want to be able to support. You could use copper pairs to provision T-1, E-1, or J-1 services, but if you wanted to get into the higher-bandwidth capacities afforded under T-3, E-3, or J-3, you would deploy a higher-bandwidth medium, such as coax, microwave, or fiber. PDH operates on four-wire circuits, which means it operates in full-duplex and you can communicate in both directions simultaneously.

CSUs   A CSU terminates each end of a T-, E-, or J-carrier facility. It equalizes the received signal, filters the transmitted and received wave forms, and interacts with customers' and carriers' test facilities. You use a CSU to perform diagnostic tests on

span lines and to set up a T-1, E-1, or J-1 line with a PBX, a channel bank, a multiplexer, or any other compliant data terminal equipment.

Multiplexers   A series of time-division multiplexers enables us to move up the hierarchy of the PDH infrastructure. The first in the series of multiplexers is generally referred to as *channel banks*. A channel bank has several purposes. First, it consolidates the individual voice and data channels so that they can travel over the higher-speed transmission line. In the case of a T-1, a channel bank consolidates 24 channels; in the case of an E-1, a channel bank consolidates 32 channels. Channel banks can accept analog inputs, which means they can digitize analog voice. So, if you're using an analog switch—either a local exchange or a PBX—the channel bank should be equipped with the codecs that run an analog voice stream through a process of digitization called Pulse Code Modulation (PCM) to convert the analog voice into a digital bitstream that can be transported over the digital carrier. (Codecs are discussed in Chapter 2, "Telecommunications Technology Fundamentals," and PCM is discussed later in this chapter.)

Beyond the channel bank, the multiplexing hierarchy steps through the individual transmission levels. In the case of T-carrier, the levels are T-1 through T-4; for E-carrier, they are E-1 through E-5; and for J-carrier, they are J-1 through J-5.

DLCs   DLCs—also called remote terminals, concentrators, or remote concentrators—were introduced in the mid-1970s, specifically as a way to economically expand the telco network. They were deployed to improve efficiency and to lower costs. DLCs reduced analog facilities by up to 80%, and they led to building, real estate liquidation, and maintenance efficiencies as well. They also eliminated the need for load coils, which are used to improve transmission on wire pairs for distances greater than 3.4 miles (5.5 kilometers). DLCs also reduced the number of pairs of copper wires required between the local exchange and the subscriber; they did this by sharing pairs or transmission facilities among many multiplexed conversations. Essentially, the DLC architecture, shown in Figure 5.6, reduces the loop lengths and makes more effective use of high-capacity trunks from a neighborhood into the local exchange.

DLCs continue to evolve, and as they do so, they become smaller systems. The original DLCs were built so that an individual system could service around 600 subscribers, but these boxes achieved only about a 50% fill ratio, which meant that half of the capacity was not being used. Now, given the distribution and density of neighborhoods and populations, smaller DLCs are being created. These systems service up to about 96 subscribers, and utilization is at around a 90% level. These smaller DLCs allow for faster service rollout and a shorter payback period for the deployment. They also facilitate quick response to growth in services and competition.
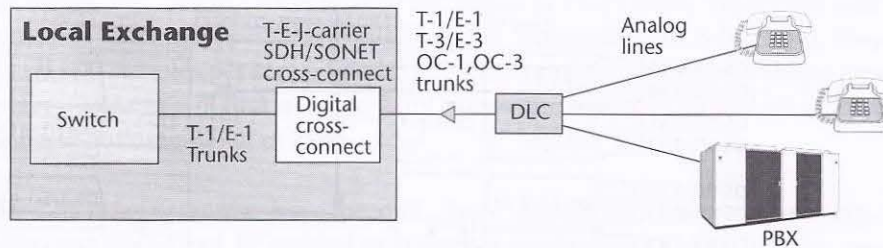
Figure 5.6 DLC architecture

With ever-increasing interest in high-speed broadband access, DLCs could be a tool for shortening loop length, thereby bringing more bandwidth to the customer. Consequently, some of the additional changes that have occurred with the newer generations of DLCs also provide interfaces for SDH/SONET or optical fibers. However, bear in mind that the vast majority of DLCs deployed are incompatible with the xDSL services. It is imperative that the proper generation of DLC be deployed in order to meet the customer's demand for broadband residential access via twisted-pair.

DCSs   DCSs were developed in 1981 and officially introduced in 1985. They basically automated the process of circuit provisioning and replaced the use of manual patch panels. The key feature of DCSs is called drop and insert. This refers to the capability of the cross-connect to exchange channels from one facility to another. It is used to implement appropriate routing of traffic, to reroute around congestion or failure, and to allow customers to dynamically reconfigure their own networks. Generally it keeps communications paths in place for continuous use over a period of months, or sometimes even years, but it does allow change as demand warrants.

Essentially, a DCS is a computer system with a variety of software databases that describe first-choice routes and alternate routes (see Figure 5.7). If Channel 7 normally goes out over Line 1 and then goes out over Trunk 1, but Trunk 1 fails, the digital cross-connect can consult its alternate routing table, which might say to reroute that particular line over Trunk 2. A reconfiguration can take place in a matter of minutes.

Digital cross-connects provide for four levels of switching. You can switch between DS-3s and DS-3s or between E-3s and E-3s. You can switch between DS-1s and DS-1s or between E-1s and E-1s. You can switch between DS-0s and E-0s, and you can also potentially switch below that level by using submultiplexed data streams within the DS-0 channel. Some of the individual intelligent multiplexers, such as T-1/E-1 muxes and T-3/E-3 muxes, also offer this capability.

The fact that reconfigurations can be implemented in a matter of minutes—and that customers can implement this capability on their own private networks—is the most
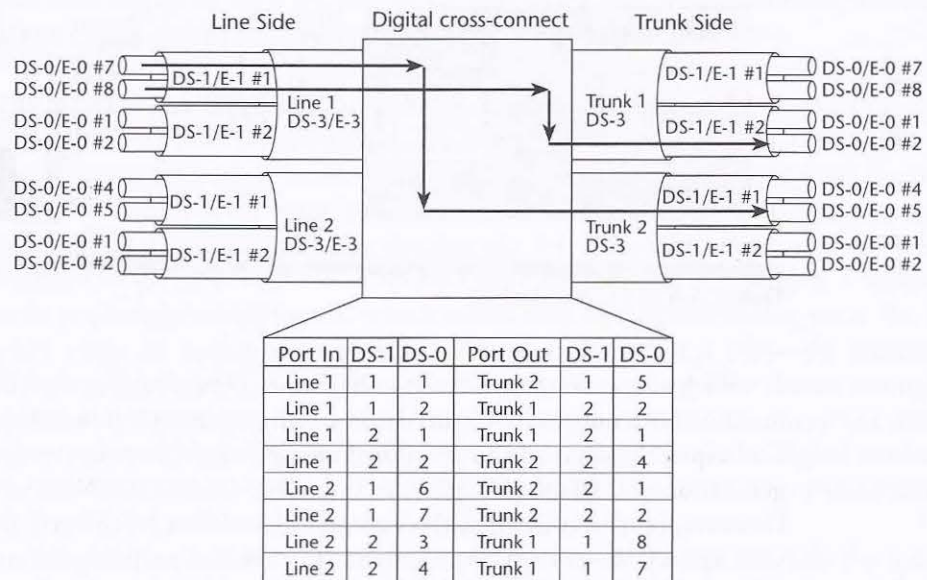
Figure 5.7 The DCS

important and favorable characteristic of the DCS. The main applications for cross-connects are to provide disaster recovery, to bypass a system during maintenance without affecting traffic flows, to reconfigure the network to address peak traffic demands, and to implement a temporary application that can be reconfigured as needed.

Voice Compression Standards

Let me take a moment to talk about how voice was digitalized to carry over the PSTN under the original sampling theorem.

PCM   When PCM was developed, we lived in an environment that was largely analog. Therefore, in designing a digitization scheme, it was important to consider that voice would have to undergo many conversions between analog and digital as it was transmitted through the numerous switching nodes and components of a network. And if it had to go through a number of conversions, it could withstand only so many conversions before it began to lose toll quality. Therefore, the sampling theorem that was developed suggested that in order to reproduce voice in toll-quality manner, you have to sample that voice at twice the rate of the highest frequency carried. The highest frequency being carried in the telephone channel was 4,000Hz, so we needed a sampling rate of 8,000 samples per second. Every time we take a sample, we're measuring the amplitude, or voltage, of the signal at

that point. Say that the amplitude of the signal is +1.25 volts. We would take that amplitude value and convert it into a binary expression, an 8-bit word. Now we have 8,000 samples per second and 8 bits per sample, resulting in 64Kbps required to carry voice in a digital manner. This is how the 64Kbps channel was derived as the basic building block of PDH.

ADPCM As networks have become more digitalized, fewer conversions take place, and voice can be carried at a higher quality over fewer bits per second. Another standard that is used in the PSTN is Adaptive Differential PCM (ADPCM), which essentially carries digital voice at 32Kbps. ADPCM does something wonderful for an end user. Say you have a traditional T-1 line with PCM channel banks. Over that one T-1, you can extract 24 channels, each of which carries 64Kbps. But your traffic increases, and you need more channels to carry voice traffic. You have two options: You can add another T-1 line, which means a substantial monthly investment, or you can put ADPCM channel banks on the T-1 that you already have, which gives you 48 channels of 64Kbps each. In essence, you can double the capacity of the network without having to add more subscriber lines.

Needless to say, voice compression continues to be applied, and not just in the PSTN. For instance, in wireless networks such as cellular networks, where spectrum is at a premium, we compress voice down to 8Kbps so that we can support more callers within each of the cells.

T-Carrier and E-Carrier Signal Hierarchy

Because competition has entered the marketplace, different operators in an area have often bought equipment from different manufacturers, which means there are a number of standards to deal with. Even if a country once followed ITU standards, new companies may have entered the country with North American–standard

DS-*x* Versus TX-*x* and CEPT-*x* Versus E-*x*

Technically, the DS-*x* and CEPT-*x* terminology (DS-1, DS-3, CEPT-1, CEPT-3, and so on) indicates a specific signal level (and thus usable bandwidth), as well as the electrical interface specification. T-*x* and E-*x* terminology (T-1, T-3, E-1, E-3, and so on) indicates the type of carrier—a specific physical implementation of a DS-*x*/CEPT-*x*. Today, however, the terms DS-*x* and T-*x* are often used interchangeably. For example, someone might use the term DS-1 and another person might use the term T-1 to refer to the same thing—a digital transport that can carry 1.544Mbps over a total of 24 channels. The same applies to the use of the European designation: E-1 is the same as CEPT-1, and so on.

equipment and interfaced with the existing ITU-based equipment. Thus, you really need to be familiar with all the standards. This section covers the signal hierarchy for both T-carrier and E-carrier standards.

The T-Carrier Digital Signal Hierarchy Table 5.1 lists the levels in the T-carrier digital signal hierarchy, the basic building block of which, DS-0, is the 64Kbps channel.

Table 5.1 The T-Carrier Digital Signal Hierarchy

Digital Signal Level	Bit Rate	DS-0 Channel	Number of T-1 Lines
DS-0 (T-0)	64Kbps	1	—
DS-1 (T-1)	1.544Mbps	24	1
DS-2 (T-2)	6.312Mbps	96	4
DS-3 (T-3)	44.736Mbps	672	28
DS-4 (T-4)	274.176Mbps	4,032	168

The first subscriber level, Digital Signal Level 1 (DS-1), provides 1.544Mbps and a total of 24 channels. The DS-2 level is not a subscriber level, nor is it used very frequently in the PSTN. You might see it installed on some campus networks, or perhaps to bundle some DS-1s out of a tandem exchange to a toll exchange.

DS-3 is a high-bandwidth alternative for subscribers, and it is used for interexchange trunks. Both users and carriers get 44.736Mbps with DS-3, which is a total of 672 channels that can carry combined voice, data, fax, and image traffic.

T-Carrier and J-Carrier: Stealing Bits for Signaling

In the T-carrier and J-carrier system, the signaling for each conversation flows in the same channel as the conversation. Thus, for voice purposes, we have the full 64Kbps channel, and every now and then we steal one of the bits of digital voice and replace it with the proper signaling bit. This does not affect the understandability or voice quality of the message. However, if a data stream were traveling through that channel and we went about stealing bits, we would obviously be changing the meaning of the content. Therefore, we accommodate 56Kbps of data within each channel, leaving a little bit of room for the signaling bits to be inserted as needed.

The DS-4 level is used only within the telco, again on interexchange trunks. DS-4 offers roughly 274Mbps and 4,032 channels.

With each of these levels, you must go through a separate multiplexing level. Remember that each of the muxes is driven by a different clocking source, so they each bundle their channels in a slightly different framework. In building the 64Kbps channels up to a T-1 and then building those T-1s up to T-2s and those T-2s up to T-3s, everything is fine unless somewhere along the way one customer decides to extract some capacity to drop off that allocation midway. Say, for example, that you're in Washington, DC, and you need to connect to San Francisco. In Washington, DC, you'd have a T-1 coming into the local exchange, along with multiple other customers in the neighborhood. The local exchange might bundle those T-1s onto a T-2 to pass off to the tandem, and the tandem would bundle them up into T-3s to send to the toll center. The toll center would bundle them up for T-4s to pass across the long haul to San Francisco. This works great, but then you need to add an office in Kansas City. So you need to add a T-4 mux to break it down to all the respective T-3s. Then you need to break down the T-3s into their T-2s, and then break down the T-2s into all their T-1s, and then find your T-1 so that you can extract the channels you want to drop off. Then you need to bundle them all back up onto the T-1 and go back up the scale again. This strict hierarchy requires you to go through all the changes—you can't jump steps as you bundle and unbundle traffic. Therefore, the PDH hierarchy is characterized by a lot of back-to-back multiplexing and demultiplexing in order to drop and add payload. That is one of the highest-cost components of this generation of the PSTN.

The E-Carrier Digital Signal Hierarchy As shown in Table 5.2, E-carrier signals are often called CEPT levels (for Common European Postal and Telegraphy); 64Kbps is the basic increment in E-carrier. CEPT-1 (or E-1) operates at 2.048Mbps and is delivered over 32 channels.

CEPT-2, like T-2, is not used much. CEPT-3, the high-bandwidth alternative, offers 34Mbps and 512 channels. CEPT-4 and CEPT-5 are largely used within telco

E-Carrier: Separate Signaling Channels

The E-carrier system is different from the T-carrier and J-carrier systems in an important way: In the E-carrier system, the signaling information travels in separate channels from the voice and data traffic. Two of the 32 channels are devoted to carrying signaling and control information, and the other 30 channels are available to carry customer payload at 64Kbps. In T-carrier and J-carrier, because the signaling information flows in the conversation channel, voice channels are 64Kbps, but data channels are 56Kbps, with the remaining capacity reserved for signaling.

Table 5.2   The E-Carrier Digital Signal Hierarchy

CEPT Signal Level	Bit Rate	E-0 Channel	Number of E-1 Lines
CEPT-0 (E-0)	64Kbps	—	—
CEPT-1 (E-1)	2.048Mbps	32	1
CEPT-2 (E-2)	8.488Mbps	128	4
CEPT-3 (E-3)	34.368Mbps	512	16
CEPT-4 (E-4)	139.246Mbps	2,048	64
CEPT-5 (E-5)	565.148Mbps	8,192	256

networks, again for their interexchange trunks. Like T-carrier, E-carrier has a strict hierarchy of multiplexers.

The SDH/SONET Infrastructure

SDH/SONET, created in the mid-1980s, is the second generation of digital hierarchy. Whereas PDH involves a lot of overhead because it includes three standards throughout the worldwide, SDH/SONET uses one common standard that applies to networks worldwide. SDH is the ITU standard and followed throughout the parts of the world where ITU standards dominate; SONET is the ANSI standard, which is part of SDH, and it is used in North America and Japan. SDH/SONET was created to be an industry standard for high-speed transmission over optical fiber. It was actually part of a much bigger standard in the works at that time—Broadband ISDN. Broadband ISDN was envisioned for use with advanced applications (for example, tele-education, telesurveillance, telegambling, the ability to collaborate, HDTV). Two technologies were required in order to support such applications—a transport infrastructure that had the significant bandwidth needed to support them (SDH/SONET) and a switching technology (ATM) that could ensure that latencies could be controlled and kept very low. Consequently, SDH/SONET and ATM, as modern broadband technologies, were both born out of the Broadband ISDN standard and a desire to be able to deliver advanced applications.

SDH/SONET is a family of transmission standards designed to achieve compatibility between different fiber-optic transport products, as well as to provide compatibility with the existing digital hierarchy, PDH. A lot of fiber-optic systems have been deployed in the past 16 or more years, but they're not all compatible with

one another. They use different forms of cables with different diameters, and they use different types of light sources. And where there are physical incompatibilities, you can't achieve *midspan meet*—where two carrier services have to come together. A railroad analogy can be used here. Think back to when people had just begun to build railroads. Oftentimes, one provider was building tracks going east to west that were a certain width and another provider was building tracks going west to east that were a different width. When the providers met in the middle, their cars couldn't cross each other's tracks. The same thing happens when there's a lack of physical compatibility in fiber-optic transport, and that means you lose the ability to carry network management information on an end-to-end basis. You may not be able to do end-to-end monitoring and control of a network that is multivendor or multicarrier in nature if the vendors or carriers use incompatible physical fiber-optic equipment.

It's always important to develop and have available very strong network management tools. The goal of network management is not to *eliminate* downtime—because we know that would be impractical; rather, it is to *minimize* the resolution time. So the ability to do end-to-end testing remotely is very critical to quick recoverability. SDH/SONET provides the physical layer (that is, Layer 1) framework for broadband applications. It provides a standardized list of optical parameters that define the types of cables and light sources that are allowed. It defines a new table of data rates that are much higher than older transmission rates. It redefines how the multiplexing process occurs as you move within the different transmission levels. It also affords very robust operations capabilities, such as service restoration.

The SDH/SONET specifications define a *frame format*—that is, how the bits are packaged together to be transported over the fiber. As mentioned earlier, they define the nature of the physical interfaces (for example, couplers, light sources). They define the optical carrier line rates, or transmission levels, and they define the sorts of messages that are exchanged in order to support operations, administration, maintenance, and provisioning.

An important aspect of SDH/SONET is that it introduced the notion of a ring operation to address network survivability by handling rapid restoration. With SDH/SONET, we use a dual-counter-rotating ring. Imagine that you have four network nodes. As shown in Figure 5.8, with a dual-counter-rotating ring, you link each of these four network nodes together by using one pair of fibers; that pair of fibers becomes the primary fiber, and information will flow over it in a clockwise manner. You run another pair of fibers, which may actually be housed in the same cable as the first pair of fibers, to join the four nodes together. The second pair of fibers become the protect fiber, which is designed to carry information in a counter-clockwise manner. In theory, if a cable is cut between Node A and Node B, you can still move a message from A to B by reversing the information flow and going from A to D to C to B. This enables you to recover immediately—within 50 milliseconds—from outages that occur, for example, because a construction crew
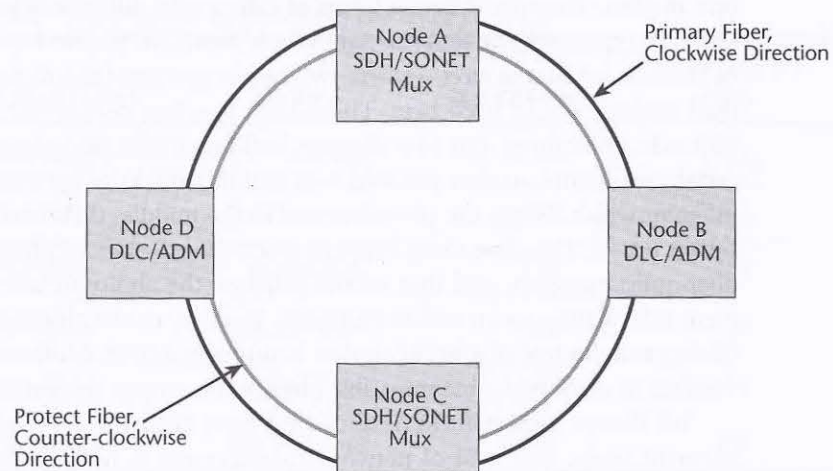
Figure 5.8 SDH/SONET ring architecture

has cut a cable. Obviously, if a major earthquake hit and all the streets were broken up, a counter-rotating ring wouldn't necessarily ensure survivability, but for smaller-scale problems, it can very adequately handle a backup. This is one of the greatest strengths of SDH/SONET and will likely keep it operational in networks for another 10 to 20 years. But these types of capabilities are also being introduced in the new generations of standards, such as WDM, and when that occurs, we will start to move away from SDH/SONET because SDH/SONET is a TDM system that does not take advantage of the fact that light can be spatially multiplexed, allowing multiple wavelengths to be carried over one fiber pair.

SDH/SONET is also important because it grooms and routes traffic. *Grooming* means that SDH/SONET selectively removes channels from a digital facility for routing to a designated remote location via another digital facility; basically, it enables you to drop and add payload flexibly. SDH/SONET also provides for performance monitoring so that you can understand the performance of the network, its components, and the congestion levels.

The SDH/SONET Signal Hierarchy

The SDH/SONET signal hierarchy deals with *optical carrier levels*, which refer to the optical aspect of the transmission—the optical pulse as it travels through the fibers. These optical pulses go through electronic muxes, and when the signal is going through these network elements, the bits are packaged in a frame for transport across the fiber. In the case of SONET, this frame is called the Synchronous Transport Signal (STS), and in SDH, the frame is called Synchronous Transport

Module (STM). Two types of rates are important in the realm of SDH/SONET: The *payload rate* refers to the capacity available to carry customer content, and the *data rate* refers to the total capacity available for customer content as well as network management information.

Table 5.3 shows the SDH/SONET signal hierarchy. You don't have to memorize all these levels, but you'll consistently encounter four or five of them in your readings that you should commit to memory.

Table 5.3 The SDH/SONET Signal Hierarchy

OC Level	SONET	SDH	Data Rate (Mbps)	Payload Rate (Mbps)
OC-1	STS-1	STM-0	51.48	50.840
OC-3	STS-3	STM-1	155.52	150.336
OC-9	STS-9	STM-3	466.56	451.008
OC-12	STS-12	STM-4	622.08	601.344
OC-18	STS-18	STM-6	933.12	902.016
OC-24	STS-24	STM-8	1,244.16	1,202.688
OC-36	STS-36	STM-12	1,866.00	1,804.032
OC-48	STS-48	STM-16	2,488.32	2,405.376
OC-96	STS-96	STM-32	4,876.64	4,810.752
OC-192	STS-192	STM-64	9,953.28	9,621.504

The levels of the SDH/SONET signal hierarchy that are most important to be familiar with are OC-1, OC-3, OC-12, OC-48, and OC-192:

- OC-1—OC-1 offers about 51Mbps and is generally used as customer access lines. Early adopter types of customers—such as universities, airports, financial institutions, large government agencies, and ISPs—would use OC-1.

- OC-3—OC-3 provides about 155Mbps. End users such as companies in the aerospace industry and high-tier ISPs would need this extensive level.

- OC-12—OC-12 provides about 622Mbps. It is another capacity toward which high-tier ISPs are moving. It was originally deployed for the metropolitan area

fiber rings built out across cities worldwide, although those rings are now moving to OC-48.

- OC-48—OC-48 offers about 2.5Gbps. This capacity has been deployed for backbone, or core, networks. Today the metropolitan area rings are moving from OC-12 to OC-48, and the backbone links are moving from OC-48 to OC-192.
- OC-192—OC-192 supports about 10Gbps and is being used for backbone networks.

There are more levels in the SDH/SONET signal hierarchy, but the ones discussed here are the ones for which equipment is currently being manufactured. We are in early stages of building new muxes that can also operate at OC-768 and that will support 40Gbps. Some people feel that electronic muxes really are not suitable for the higher data rates and that we should concentrate on moving to all-optical muxes and switches.

How do the high optical-carrier levels relate to all the lower-level signals out there—such as those from a 1.5Mbps T-1 or a 2Mbps E-1? There are mechanisms that enable us to map signal levels below DS-3 (that is, below 45Mbps) into what SDH calls *virtual containers* or what SONET calls *virtual tributaries*. A virtual container or tributary basically defines the data structure for the transport and switching of sub-51Mbps network services such as DS-1, E-1, DS-2, and E-3. Table 5.4 shows the various line rates that are supported and what existing standard each refers to. For most people, this type of detail won't make or break success in the industry, but it's important to know that a virtual tributary or virtual container can provide a highway for lower-rate data signals to coexist in high-speed optical pipes.

Table 5.4 Virtual Container/Virtual Tributary Line Rates and Standards

Virtual Container/ Virtual Tributary Level	Line Rate	Standard
VC-11/VT-1.5	1.728Mbps	DS-1/E-1
VC-2/VT-2	2.304Mbps	E-1
VT-3	3.456Mbps	DS-1C
VC-2/VT-6	6.912Mbps	DS-2
VT-6-N	$n \times 6.9$Mbps	(future)
async DS-3/VC-3	44.736/34.368Mbps	DS-3/E-3
VC-4	139.264Mbps	DS-4/E-4

In contrast to PDH, SDH/SONET is a *synchronous* infrastructure. This means that each of the network elements draws its clocking pulse from one clocking source—so everybody is marching to the beat of the same drummer. Instead of using special framing bits to delineate channels, SDH/SONET uses a special pointer bit in front of each conversation that essentially says "start of a new conversation." When it's time to drop that channel off at a customer premise, we can identify it by its pointer bit and extract it without having to disturb any of the other traffic. This reduces the overhead associated with multiplexers by a factor of 10.

SDH/SONET Muxes and Cross-Connects
SDH/SONET was built for and largely relies on fiber-optic transmission media. It also includes a variety of multiplexers and cross-connects, as well as equipment that could be placed at the customer premise. There are two main categories of SDH/SONET multiplexers (see Figure 5.9):

- **Terminal muxes**—Terminal muxes enable signals to move through the hierarchy of optical carrier levels. They act as access nodes and support current services by accepting electrical interfaces and lower-level signals, including DS-1/E-1, DS-2, and DS-3/E-3. They concentrate one or more optical carrier signals and represent one of the optical carrier levels.
- **Add/drop muxes (ADMs)**—ADMs facilitate easy dropping and adding of payload and are therefore the building blocks of the SDH/SONET network.
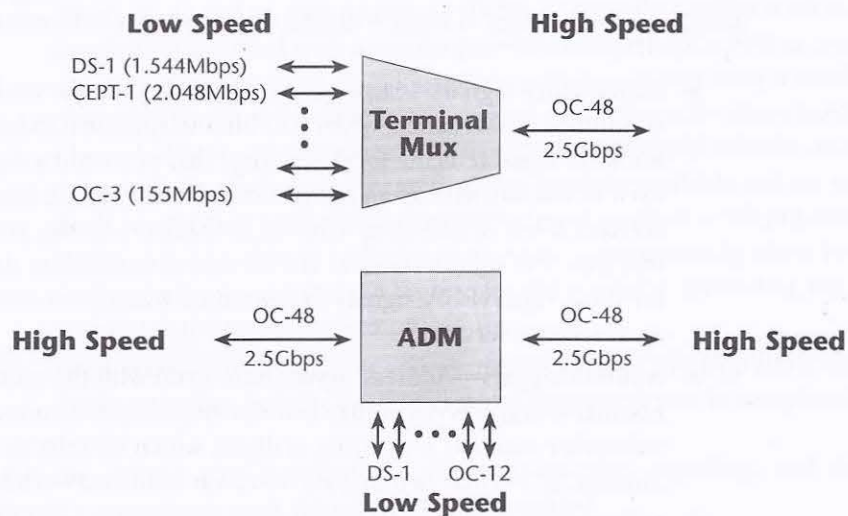
Figure 5.9 Terminal muxes versus ADMs

An add/drop mux converts one or more lower-level signals, such as T-1 or E-1 signals, into and from one of the optical carrier levels. It can drop lower-rate signals to be transported on different facilities, or it can add lower-rate signals into the higher-rate optical carrier levels, and basically it allows telcos to add and drop traffic easily and conveniently all along the network.

There are also two categories of SDH/SONET cross-connects:

- **Wideband digital cross-connects**—These terminate SDH/SONET and DS-3/E-3 signals. Switching occurs at the DS-0, DS-1/E-1, and VT/VC levels.

- **Broadband digital cross-connects**—Broadband digital cross-connects interface at the various SDH/SONET signal levels as well as the legacy DS-3/E-3 levels, but they then switch at the optical carrier levels. They can make cross-connections at DS-3/E-3, OC-1, and concatenated levels (that is, where you combine several frames of an OC-1 together). Generally, a broadband digital cross-connect is used as an SDH/SONET hub that grooms the optical carrier levels for broadband restoration purposes or for routing traffic.

■ Signaling Systems

This section discusses the nervous system of the network: the signaling system. A great deal of information needs to be passed back and forth between the network elements in the completion of a call and also in the servicing of specialized features. Four main types of signals handle this passing of information:

- **Supervisory signals**—Supervisory signals handle the on-hook/off-hook condition. For instance, when you lift a telephone handset (that is, go off-hook), a signal tells the local exchange that you want a dial tone, and if you exist in the database as an authenticated user, you are then delivered that service; when you hang up (that is, go back on-hook), you send a notice that says you want to remove the service. A network is always monitoring for these supervisory signals to determine when someone needs to activate or deactivate service.

- **Address signals**—Address signals have to do with the number dialed, which essentially consists of country codes, city codes, area codes, prefixes, and the subscriber number. This string of digits, which we refer to as the telephone number, is, in effect, a routing instruction to the network hierarchy.

- **Information signals**—Information signals are associated with activating and delivering various enhanced features. For instance, a call-waiting tone
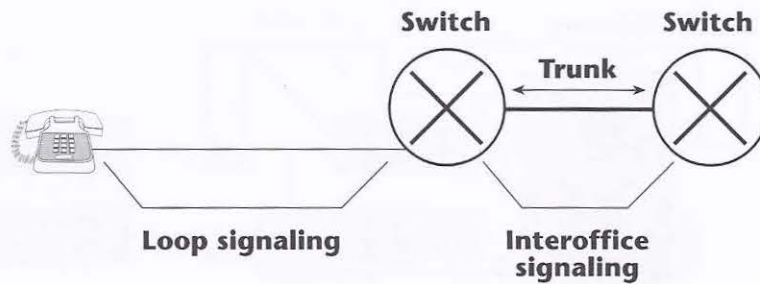
Figure 5.10   Customer loop and interoffice signaling

is an information signal, and pressing *72 on your phone might send an information signal that tells your local exchange to forward your calls.

- **Alerting signals**—Alerting signals are the ringing tones, the busy tones, and any specific busy alerts that are used to indicate network congestion or unavailability.

Signaling takes place in two key parts of the network: in the access network, where it's called *loop signaling*, and in the core, where it's called *interoffice signaling* (see Figure 5.10).

With analog loop signaling, two types of starts exist:

- **Ground start**—*Ground start* means that when you seize that line, it's immediately grounded so that no other call can potentially conflict with it. Ground start is used with a contentious system, perhaps a PBX at a corporate enterprise, to avoid collisions. For example, say you seize a trunk and place a call, and now you're in the ringing state. There are short periods of silence between ringing tones. The local exchange could mistake one of these periods of silence to mean that that trunk is available and try to send a call in over that same trunk that you're trying to place a call out over; this would cause a collision (referred to as *glare*). Consequently, when you're dealing with systems and contention for the resource, grounding the trunk up front is the most efficient procedure.

- **Loop start**—Pay telephones and residential phones use *loop start,* which means that the circuit is grounded when the connection is completed.

There are various start standards for digital subscriber signaling, and they are defined in accordance with the service being provided.

Interoffice signaling has been through several generations of signaling approaches. In the first generation, called per-trunk signaling, the complete path—
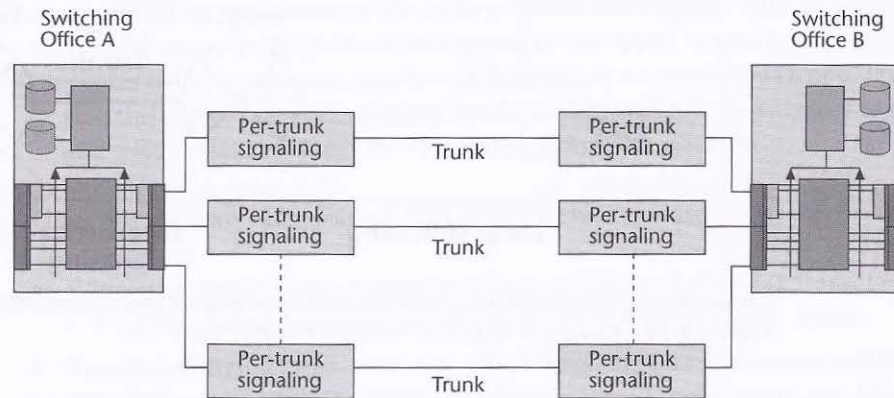
Figure 5.11 Per-trunk signaling

all the way to the destination point—is set up in order to just carry the signaling information in the first place (see Figure 5.11). This method uses trunks very inefficiently; trunks may be put into place to carry 20 or 30 ringing tones, but if nobody is on the other end to take that call, the network trunk is being used but not generating any revenue. Also, when a call is initiated and begins to progress, you can no longer send any other signaling information over that trunk; being able to pass a call-waiting tone, for instance, would not be feasible.

We have moved away from the per-trunk signaling environment to what we use today—common-channel signaling (see Figure 5.12). You can think of common-channel signaling as being a separate subnetwork over which the signaling message flows between intelligent networking components that assist in the call completion and assist in the delivery of the service logic needed to deliver the requested feature. Today, we predominantly use the ITU-T standard for common-channel signaling: SS7.

SS7 Architecture

SS7 is critical to the functioning and operation of the modern network. With SS7, a packet data network overlays and controls the operation of the underlying voice networks; signaling information is carried on an entirely different path than voice and data traffic. Signaling doesn't take a great deal of time, so we can multiplex many signaling messages over one channel, and that's why the signaling system is a packet network. The signaling system takes advantage of the efficiencies of statistical multiplexing for what is essentially bursty data. The SS7 signaling data link is a full-duplex digital transmission channel that operates at
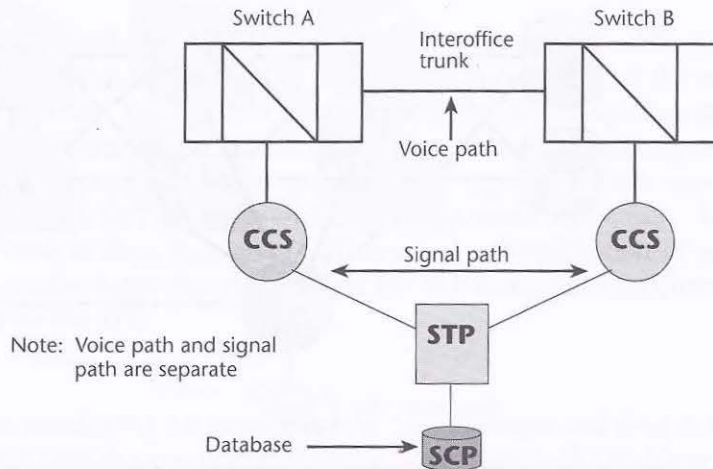
Figure 5.12 Common-channel signaling

either 56Kbps or 64Kbps, depending on the standards under which the network is operating (for example, T-carrier and J-carrier operate at 56Kbps, E-carrier operates at 64Kbps).

SS7 is an entire architecture that performs out-of-band signaling (that is, signaling in which the conversation and the signaling take place over different paths) in support of the information-exchange functions that are necessary in the PSTN, such as call establishment, billing, and routing. Database access messages convey information between toll centers and centralized databases to permit real-time access to billing-related information and other services. The SS7 architecture defines the procedures for the setup, ongoing management, and clearing of a call, and it allows you to pass along customer-related information (for example, the identity of the caller, the primary carrier chosen) that helps in routing calls. The efficiency of the network also results in faster call setup times and provides for more efficient use of the circuits when carrying the voice or data traffic. In addition, SS7 supports services that require signaling during a call as it is occurring—not in the same band as the conversation.

SS7 permits the telephone company to offer one database to several switches, thereby freeing up switch capacity for other functions, and this is what makes SS7 the foundation for INs and advanced intelligent networks (AINs). It is also the foundation for network interconnection and enhanced services. Without SS7, we would not be able to enjoy the level of interoperability we have today. SS7 is also a key to the development of new generations of services on the Internet, particularly those that support traditional telephony services. To be able to accommodate
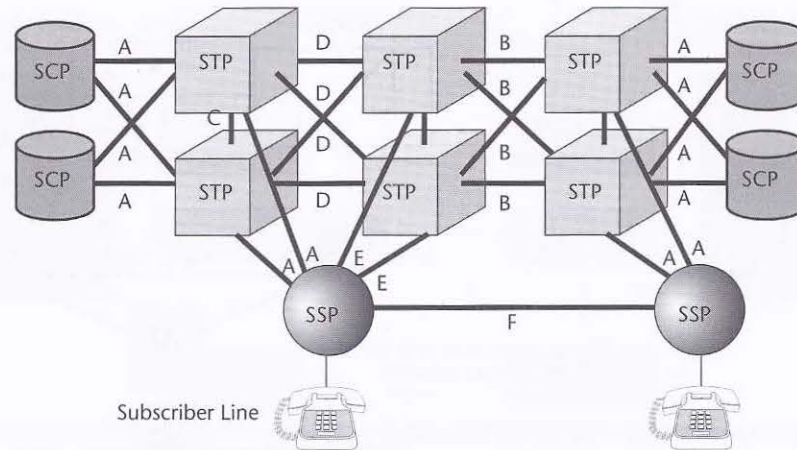
Figure 5.13 An SS7 network

features such as call forwarding, call waiting, and conference calling, you must be able to tap into the service logic that delivers those features. Until quite recently, the Internet has not been able to do this, but the year 2000 saw the introduction of SS7 gateways, which allow an interface between circuit-switched networks (with their powerful SS7 infrastructure) and the emerging packet-switched networks that need to be capable of handling the more traditional type of voice communications on a more cost-effective basis.

As Figure 5.13 shows, there are the three prerequisite components in the SS7 network: service switching points (SSPs), service control points (SCPs), and signal transfer points (STPs).

SSPs

SSPs are the switches that originate and terminate calls. They receive signals from the CPE and perform call processing on behalf of a user. The user, by dialing particular digits, triggers the network to request certain services. For instance, if you preface a number with a toll-free prefix, that toll-free arrangement triggers the local exchange, or SSP, to initiate a database lookup to determine the physical address of that toll-free number (that is, where it resides in the network). The SSP reaches into the network to find the database that can translate the toll-free number into a physical address in order to then complete the toll-free call. The SSP does this by interacting with a device called the SCP, which is discussed shortly.

SSPs are typically implemented at local exchanges, access tandem offices, or toll centers that contain the network-signaling protocols. The SSP serves as the source and destination point for the SS7 messages.

SCPs

The second key component of SS7 is SCP. This is the network element that interfaces with the SSP as well as the STP. Most importantly, the SCP is the network element that contains the network configuration and call-completion database; in other words, it contains the service logic to act on the types of calls and features the users are requesting. SCPs are centralized nodes that contain service logic—basically software and databases—for the management of the call. They provide functions such as digit translation, call routing, and verification of credit cards. The SCPs receive traffic from the SSP via the STP and return responses, based on that query, via the STP.

STPs

The STP is responsible for translating the SS7 messages and then routing those messages between the appropriate network nodes and databases. Notice in Figure 5.13 that the SCPs and the STPs are both redundant, and that the links running between them are also redundant.

SS7 and the Internet

If a network loses its signaling system, it loses the capability to complete calls, as well as to do any form of billing or passing along of management information. This makes SS7 critical. The SS7 signaling data link, as mentioned earlier in the chapter, is a full-duplex digital transmission channel that operates at either 56Kbps or 64Kbps. A variety of other SS7 links are defined as well, and each has specific uses within the signaling network:

- **A (access) links**—An A link interconnects an STP with either an SSP or an SCP. The SSP and SCP, collectively, are referred to as the *signaling endpoints*. A message sent to and from the SSPs or SCPs first goes to its home STP, which, in turn, processes or routes the message.

- **B (bridge) links, D (diagonal) links, and B/D links**—A B link connects an STP to another STP. Typically, a quad of B links interconnect peer (or primary) STPs (for example, the STPs from one network to the STPs of another network). The distinction between a B link and a D link is rather arbitrary, and such links may be referred to as *B/D links*.

- **C (cross) links**—C links interconnect mated STPs.

- **E (extended) links**—E links provide enhanced reliability by providing a set of links from the SSP to a second STP pair.

- **F (fully associated) links**—F links are links that directly connect to signaling endpoints.

■ Intelligent Networks

The ITU's standardization of SS7, in 1980, began the evolution toward the concept of intelligent networking. An IN includes a set of nodes that rely on widespread distribution of call-handling functions and capabilities (see Figure 5.14). Before the advent of INs, customers could have only the services and features available from their local exchanges. Their ability to demand and achieve new services from the operator was very much tied to the generation of software in the local exchange and whether it had yet incorporated the feature of interest. With INs, you can centrally place this type of service and feature logic on a node (such as an SCP), and then any switch can reach it and make use of that feature. The objective of the IN initially was to ease the introduction of new services into the network. It also provided a foundation for complex services that would be required and desirable on a networkwide basis, such as the automation of the operator-assistance function. Because of the IN and specialized peripherals—again, computing systems loaded with specific software—we no longer have to use operators to place a credit card call or a collect call.

Intelligent networking gives carriers the capability to directly develop network functionality on outboard processors connected to the switches, instead of having to be tied to their switch manufacturer and having to rely on the internal software. A main feature developed for the IN during the early and mid-1980s was *digit translation*, which was applied to toll-free number translation and VPNs. Customers could develop a unique calling plan that identified their location. They could invent their own numbering plan so that they could dial numbers that were easy
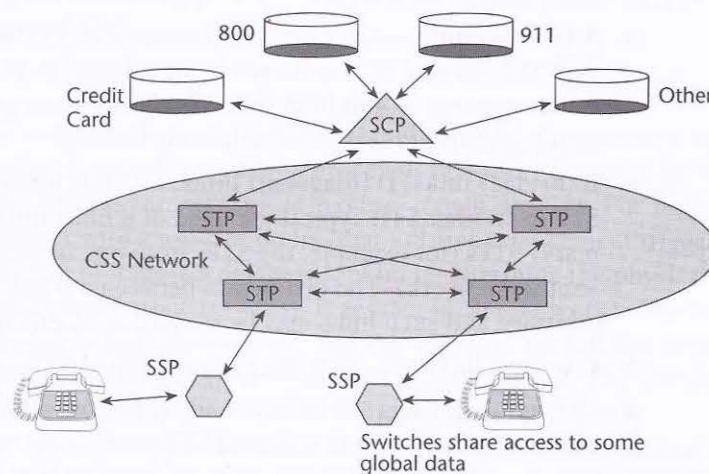
Figure 5.14 An IN

for them to remember, and in the network, the IN infrastructure would translate these private numbers into network physical addresses (for example, country code, city code, area code).

The IN also enables operator-assistance features such as eliminating credit card calling and collect calling as manual fulfillment processes. The IN also enables the identification of primary carriers (where competition exists), so that customers can select their primary carriers. *Local number portability*—which allows you to keep your own telephone number when you move to a new location—is a rather new concept that can be delivered thanks to the sophistication of this IN infrastructure. With local number portability, although your physical address will be different at your new location, you may want to keep your old phone number so your friends and colleagues can easily recall it. But for calls made with your old number to reach your new physical address, there must be translation tables in the network that can identify your correct physical address and properly route incoming calls to you.

AINs

Around the mid-1980s, Bellcore (which is now Telcordia) pioneered the second generation of INs, which we call AINs (see Figure 5.15). AINs move the service logic outside the switch and onto an independent SCP. An AIN is a service-independent network architecture that allows carriers to create and uniformly support telecom services and features via a common architectural platform, with the objective of allowing for rapid creation of customizable telecommunication services.
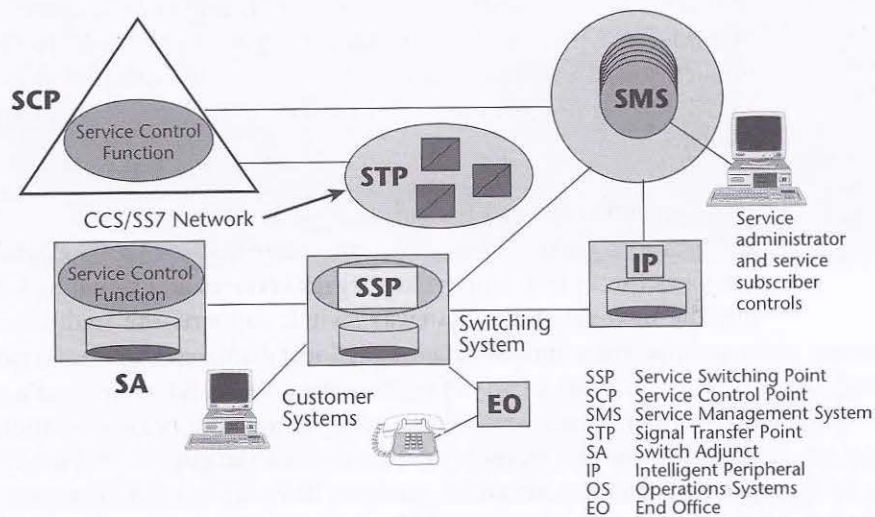
Figure 5.15 AIN architecture

An AIN is composed of intelligent nodes that are linked via SS7 to support a variety of services and advanced call-handling features across multiple vendor domains. With the introduction of the AIN architecture, a few additional components were needed. First, the service management system is a service-creation environment that facilitates the technical and customer service representatives' interface with the provisioning and network management systems. Second, intelligent peripherals are computing platforms that serve a very specific purpose but have a very widespread demand across the network (for example, voice recognition and voice synthesis capabilities to process third-party-assisted calls).

AINs can be used for a number of applications, including intelligent call routing, visitor location registration, virtual number service, voice-activated dialing, voice response, speech recognition, and text-to-speech conversion. The AIN infrastructure is critical in mobile communications. The reason you can roam across cellular networks is that IN databases are able to log whether you are present in your home network or in a visitor network, and they can identify whether you're authenticated to use the network. If you are authenticated to use the network, IN databases can identify which services should be made available to you. Virtual number services are also an important application of AINs; for example, a 700 number can identify and locate you within a footprint, rather than requiring you to be at a specific telephone to receive a call.

Next-Generation Networks

The SS7 network acts as the backbone for the AIN—it provides access to the AIN features, allows for efficient call setup and teardown, and interconnects thousands of service providers under one common signaling network. The capability to communicate with SS7 networks is essential for all service providers because SS7 networks give next-generation local exchange carriers access to an existing base of service features.

Next-Generation Network Equipment

SS7 uses new genres of equipment to ensure that packet-based telephony switching gateways can in fact support key legacy services and signaling features. For example, the next-generation gateway switch supports the traditional Class 4, or toll switch, services and the Class 5, or local exchange switch, services. It is designed to support a wide variety of traffic—data, voice, fax, multimedia, and other emerging sensory forms—over a data backbone. The next-generation gateway switch provides seamless interoperability between the circuits that network the PSTN and packet-switching networks, such as IP backbones, ATM networks, Frame Relay networks, and emerging MPLS networks. We can use these gateway switches to connect with the SS7 network and to handle the IP services that are so popular
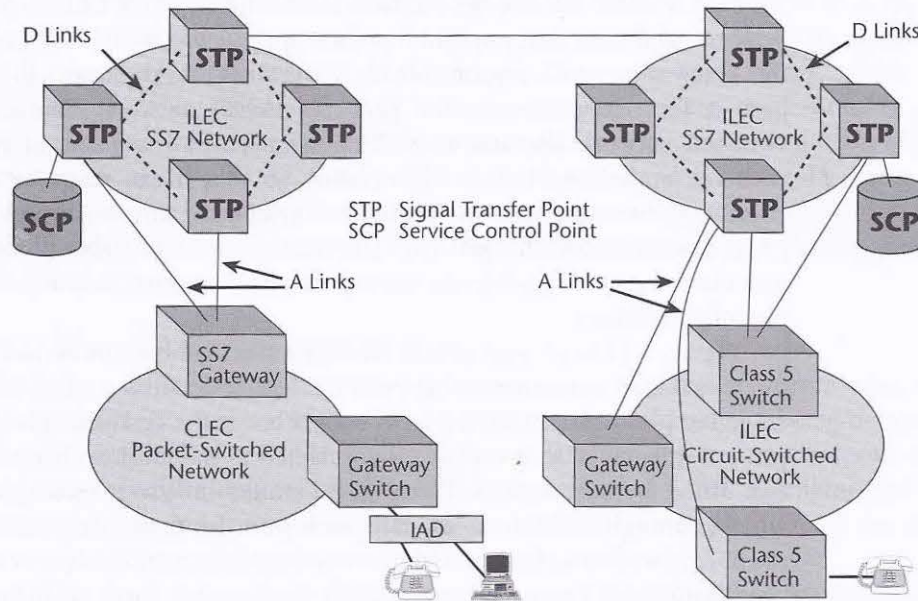
Figure 5.16   Next-generation gateway switches

Telephony Signaling Protocols and SS7

A number of telephony signaling protocols are currently used, and we don't know yet which will become the standard. Today, H.323 is found most frequently and offers the greatest range of vendor interoperability. Session Initiation Protocol (SIP), which is an Internet Engineering Task Force (IETF) standard, has a lot of support from the Internet community, and it is being included on more devices all the time. Over the next few years, we will be better able to determine which will be the dominant protocols, although IETF's SIP protocol is gaining popularity and supplanting H.323. (Signaling protocols are discussed in detail in Chapter 11, "Next-Generation Network Services.")

today. These gateway switches support a variety of telephony signaling protocols (for example, H.323, Session Initiation Protocol [SIP], Media Gateway Control Protocol [MGCP]) for communicating with the underlying SS7 architecture.

As shown in Figure 5.16, there are different forms of these next-generation gateway switches for different purposes. In the bottom right of Figure 5.16 is an ILEC and its resident circuit-switched network, which is a series of Class 5 offices at the perimeter. These Class 5 offices are connected to the SS7 network or the

STPs via A links. These Class 5 offices then connect into a CLEC's packet-switched network, and their first point of interface is a gateway switch. Among other things, this gateway switch is responsible for digitalizing and packetizing the voice to prepare it for transport over the packet-switched network. The CLEC's packet-switched network also has an SS7 gateway, which is capable of communicating with the underlying ILEC's SS7 network so that it can map the appropriate IP addresses associated with the destination telephone number, which is served by a given destination media gateway. The next-generation gateway switch, therefore, provides a means to seamlessly interoperate between two very important and existing infrastructures.

Figure 5.17 is an end-to-end view of a next-generation network. It shows an interconnected environment between the legacy circuit-switched network and the emerging packet-based networks. A subscriber at the customer premise (for example, a residence, a business site) is connected to the local exchange, known as the end office, by access lines. From there, trunks link to a media gateway switch, which, through SS7 interfaces, can reach into the underlying intelligence within the SS7 network and further add the necessary information to process the call as it's been requested. The call then goes out on a packet basis throughout a series of switches or routers (depending on what the provider is using as the backbone) and reaches a destination media gateway switch that unpackages the voice, undigitalizes it, and delivers it to the destination phone.
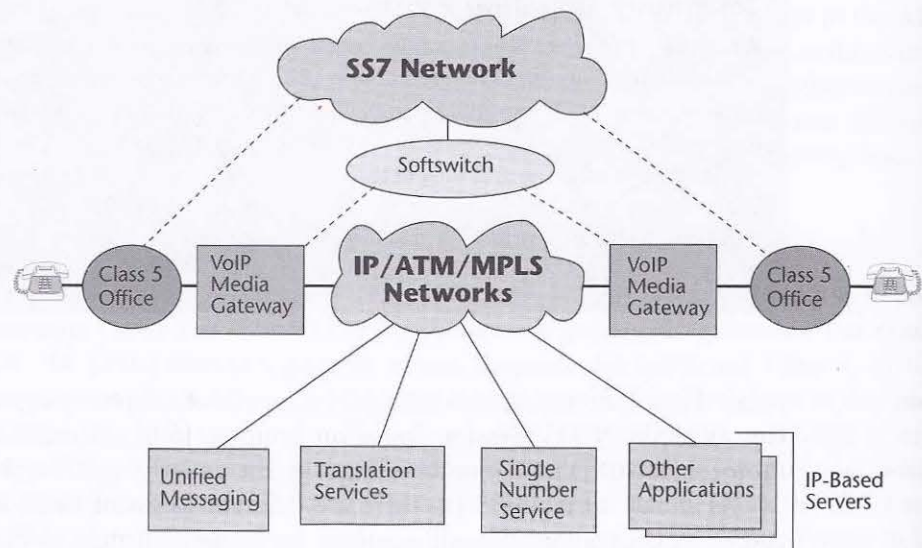
Figure 5.17   Next-generation networks

Although tremendous amounts of time and money have been spent in developing the intelligence that provides the telephony features we know today, there are still many new applications to be developed. These new applications, which are increasingly being developed for IP, include unified messaging, single-number service, and a network-type Rolodex that houses all kinds of contact and other information about people. We will be able to use databases to service calls when we have an integration or an interconnection between two networks. We will be able to provide traditional voice telephony features and introduce new generations of IP-based services.

Next-Generation Networks Versus the PSTN

The characteristics of next-generation networks are very different from what the traditional PSTN was aiming at. Next-generation networks are not being designed for just voice, data, or video. They're being designed for multimedia, and this requires capacities that are broadband in nature, networks that are engineered for extremely low and controllable latencies, and infrastructures that provide the ability to administer quality of service on a very granular level.

This book has talked about the explosion of bandwidth that's occurring because of developments in optics. As you have more and more bandwidth, it becomes cheaper and cheaper. When bandwidth becomes very inexpensive or free, a carrier needs to find other ways to generate revenue, such as by offering a large variety of value-added services (for example, reliability, priority, customer service, and encryption or security). But to administer all these services and to provide differentiated pricing, which can result in handsome revenue streams, there must be mechanisms for controlling, monitoring, and billing.

The following are important features of the next-generation network infrastructure that are covered in detail in later chapters:

- It has very fast packet switching, with capacities that we're beginning to need to measure in terabits per second (Tbps) and soon in petabits per second (1Pbps =1,000Tbps), and on its heels, in exabits per second (1Ebps = 1 billion Gbps). (See Chapter 10.)

- It places great emphasis on optical networking elements, to take advantage of the abundant bandwidth that's inherent in the visible light spectrum. (See Chapter 12, "Optical Networking.")

- Multiservice access is being created, so we will not have separate devices for voice and data as we do today, but we'll have nodes that can accommodate any traffic type. We are also creating intelligent edges; we're displacing the smarts for processing service requests, delivering features, and accommodating advanced applications by deploying them at the edge. This allows for more rapid introduction, as well as more customization of the feature sets. The core

also has to be multiservice, but it also needs to be able to differentiate between the requirements of the different traffic streams. (See Chapter 10.)

■ Next-generation telephony is very important for new entrants, particularly because of the costs of deploying normal local exchanges. A regular local exchange costs in the neighborhood of US$3 million to US$5 million, whereas a media gateway will be on the order of US$100,000. For those seeking to become competitors in the local loop environment, next-generation telephony offers a very cost-effective means of gaining entry. (See Chapter 11.)

■ Intelligent networking is being applied to the public data infrastructure as well as the Internet. (See Chapter 10.)

■ Network operators are introducing video and multimedia elements, video servers, media farms, video compression, and decompression devices, all of which become part of what constitutes the entire communications network. (See Chapter 10.)

■ Access is moving toward the broadband realm on both a wired and a wireless basis. (See Chapter 13, "Broadband Access Solutions.")

For more learning resources, quizzes, and discussion forums on concepts related to this chapter, see www.telecomessentials.com/learningcenter.

Telecommunications Essentials

The Complete Global Source for Communications Fundamentals, Data Networking and the Internet, and Next-Generation Networks

Lillian Goleniewski

Chapter 11

Next-Generation Network Services

This chapter investigates traditional Internet services, as well as new generations of applications and the network platforms that support those applications. It discusses virtual private networks (VPNs), security, various uses of Voice over IP (VoIP) networks, and developments in the streaming media arena and emerging applications.

■ Traditional Internet Applications

Traditional Internet applications are called *elastic applications* because they can work without guarantees of timely delivery. Because they can stretch in the face of greater delay, they can still perform adequately, even when the network faces increased congestion and degradation in performance. The following are the most widely used elastic applications:

- **E-mail**—The most widely used of the Internet applications, generating several gigabytes of traffic per month, is e-mail. Because there is a standardized convention for the e-mail address—*username@domainname*—various companies can interoperate to support electronic messaging.
- **Telnet**—Telnet is one of the original ARPANET applications. It enables remote login to another computer that's running a Telnet server and allows

329

you to run applications present on that computer, with their outputs appearing in the window on your computer.

- **File Transfer Protocol (FTP)**—FTP allows file transfers to and from remote hosts. That is, you can use FTP to download documents from a remote host onto your local device.

- **The World Wide Web**—Key aspects that identify the Web are the use of the uniform resource locator (URL) and the use of Hypertext Transfer Protocol (HTTP)—the client/server hypermedia system that enables the multimedia point-and-click interface. HTTP provides hyperlinks to other documents, which are encoded in Hypertext Markup Language (HTML), providing a standardized way of displaying and viewing information contained on servers worldwide. Web browsers are another important part of the Web environment—they interpret the HTML and display it, along with any images, on the user's local computer. The ease of using the Web popularized the use of URLs, which are available for just about any Internet service. (The *URL* is the syntax and semantics of formalized information for location and access of resources via the Internet. URLs are used to locate resources by providing an abstract identification of the resource location.)

So, how are people actually using the Internet? Greenfield Online conducts polls online. In November 2000, Greenfield Online (www.greenfieldonline.com) reported that the Internet was being used as follows:

- 98% of Internet users went online to check their e-mail.

- 80% of Internet users were checking for local information, such as movie schedules, weather updates, or traffic reports.

- 66% of Internet users were looking for a site that provided images and sounds.

- 66% of Internet users wanted to shop at sites that provided images of the products they were interest in.

- 53% of Internet users downloaded some form of a large file.

- 37% of Internet users listened to Internet radio.

This shows that increasingly there is interest in imagery, multimedia, and entertainment-type aspects of the Internet. These are advanced real-time applications that are highly sensitive to timely data delivery. Therefore, any application that includes VoIP, audio streaming, video streaming, or interactive multimedia needs to be addressed by the administration of Quality of Service (QoS). The lack

of control over QoS in the public Internet is preventing the deployment of these new applications at a more rapid pace.

Today's flat-rate pricing for Internet access is compatible with the Internet's lack of service differentiation, and it is partially responsible for that structure as well. The main appeal of a flat-rate pricing scheme is its simplicity. It means predictable fees for the users, and it means providers can avoid the administrative time and cost associated with tracking, allocating, and billing for usage. It also gives companies known expectations for payments, facilities planning, and budgeting. However, as QoS emerges within the Internet, the ability to differentiate services will result in differentiated pricing, thereby allowing revenue-generating service levels and packages—and that's extremely important. As we've discussed several times so far in this book, developments in optical networking and in wireless networking are providing more and more bandwidth. Hence, the cost—the cents per minute that you can charge for carrying traffic—is being reduced. If network operators are going to continue to make money in the future, they will need to do so through the administration of value-added services, differentiated performance, and tiered pricing. Therefore, the QoS aspect is very important to the materialization of new revenue-generating services.

Key applications from which service providers are expected to derive revenues include e-commerce, videoconferencing, distance learning and education networks, Webcasting, multiplayer gaming, unified messaging, call centers, interactive voice response, and IP-based centrex systems. Evolving next-generation networks—such as VPNs, VoIP and Packet over IP, streaming audio and video, multimedia collaboration, network caching, application hosting, location-based online services, software downloads, and security services—are introducing a variety of Class of Service (CoS) and QoS differentiators.

■ VPNs

A big driver of interest in VPNs is that customers increasingly need to communicate with people outside their enterprise, not just those inside the enterprise. As mentioned in Chapter 6, "Data Communications Basics," in the 1980s, about 80% of the information that was used within a given address of a business came from within that address. Only 20% was exchanged outside the walls of that location. Today, the relationship has reversed. As much as 80% of information exchanged is with points outside a given business address.

Another reason for interest in VPNs is that customers want to quickly and securely change their access points and needs as changes occur in their businesses. Many strategic alliances and partnerships require companies to exchange messages quickly. Some of these are temporary assignments—for example, a contractor
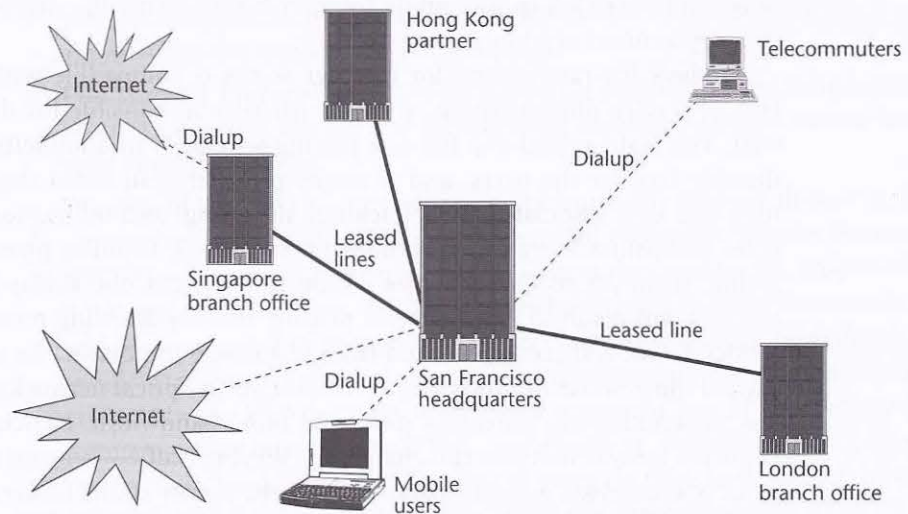
Figure 11.1 An enterprise network based on leased lines

building out a fiber-optic loop or an applications developer building a new billing system—that might last a few months, during which time the individuals involved need to be incorporated into the network. Leased lines are infamous for requiring long waits for provisioning—often 6 months to 18 months! VPNs allow rapid provisioning of capacity where and when needed.

What we see emerging is a requirement for networks that can be very quickly provisioned and changed in relationship to organizational structures. This results in a steady migration of traffic away from the traditional networks, based on leased lines (see Figure 11.1), to public networks. As a result, we're seeing a steady growth in the pseudoprivate realm of the VPN (see Figure 11.2). A *VPN* is a logical network that isolates customer traffic on shared service provider facilities. In other words, the enterprise's traffic is aggregated with the traffic of other companies. VPNs have been around for quite some time—since X.25 closed user groups on the packet-switched network, and with the AT&T Software-Defined Network (SDN) on the circuit-switched networks. A VPN looks like a private network, but it runs across either the public circuit-switched network or public packet-switched data networks. Thus, VPNs are not just a solution within the IP realm—a VPN is a concept, not a specific set of technologies, and it can be deployed over a wide range of network technologies, including circuit-switched networks, X.25, IP, Frame Relay, and ATM.

A VPN uses a shared carrier infrastructure. It can provide additional bandwidth on demand, which is an incredible feat, as compared to the weeks that it normally takes to add bandwidth to dedicated networks. Carriers build VPNs with
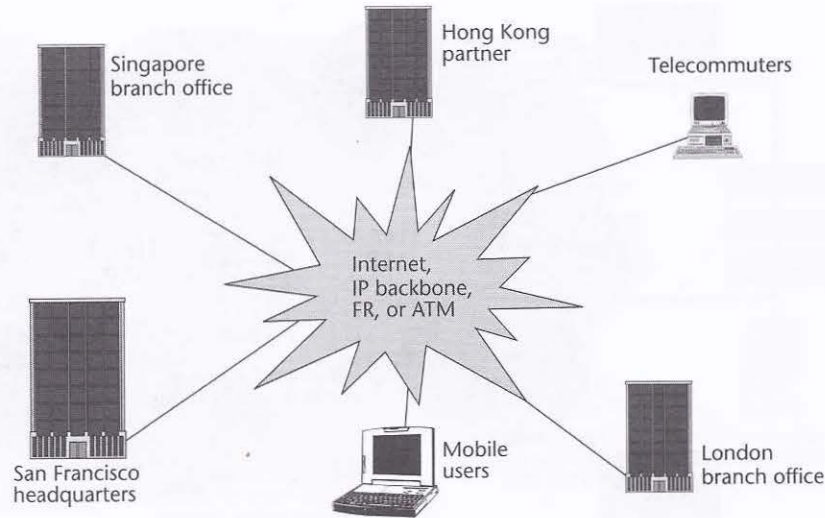
Figure 11.2 An enterprise network using a VPN

advanced survivability and restoration capabilities, as well as network management tools and support, so that QoS can be considered and service-level agreements (SLAs) can be administered and met.

Two basic VPN deployment models exist: customer based and network based. In *customer-based VPNs*, carriers install gateways, routers, and other VPN equipment on the customer premises. This is preferred when customers want to have control over all aspects of security. In *network-based VPNs*, the carrier houses all the necessary equipment at a point of presence (POP) near the customer's location. Customers that want to take advantage of the carrier's VPN economies of scale prefer this type of VPN.

VPN Frameworks

Contemporary VPNs can be described as belonging to one of two categories: the Internet-based VPN and the provisioned VPN.

Internet-Based VPNs

In an *Internet-based VPN* (see Figure 11.3), smaller ISPs provide local access services in defined geographical regions, requiring an enterprise to receive end-to-end services from multiple suppliers. An Internet-based VPN uses encryption to create a form of closed user group, thereby isolating the enterprise traffic and providing acceptable security for the enterprise across the public shared packet network. However, because
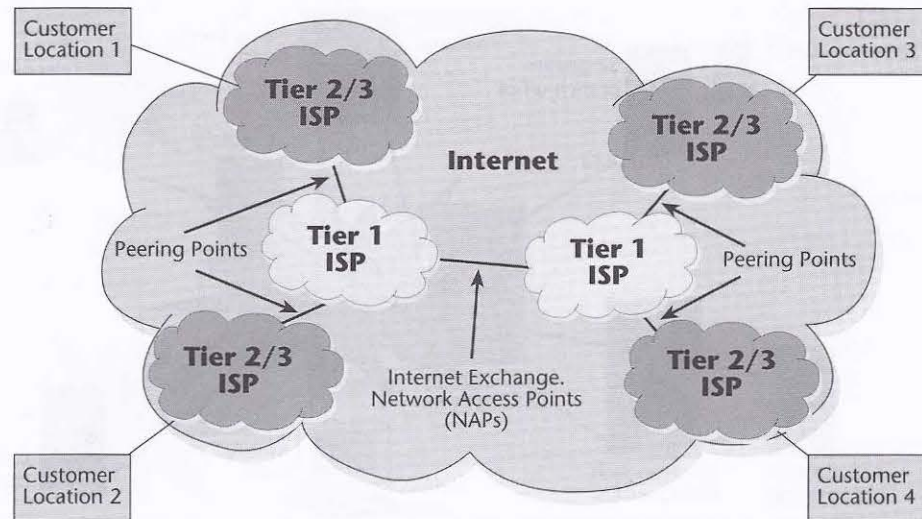
Figure 11.3 An Internet-based VPN

it involves multiple ISPs in the delivery of the VPN, the performance is unpredictable. The biggest problem of having multiple suppliers is the inability to define and meet consistent end-to-end bandwidth or performance objectives.

Figure 11.4 shows what is involved in providing an Internet-based VPN. The customer would have on the premises a wide variety of servers that dish up the corporate content, the finance systems, the customer service systems, and so on. A VPN is responsible for the encapsulation of the information and hence the security aspects. *Remote Authentication Dial-in User Services* (RADIUS), an authentication and access control server, is used for purposes of authenticating whether a user is allowed access into the corporate resources. The RADIUS server connects to a firewall, which is used to determine whether traffic is allowed into or out of the network. The router selects the optimum path for the messages to take, and the circuit physically terminates on a channel service unit/data service unit (CSU/DSU). A private line interfaces with the Internet provider's POP. From that point, the VPN either uses the public Internet that's comprised of multiple ISPs, or it relies on IP backbones provided by a smaller group of providers. Users who are working on mobile devices would have laptops equipped with the client and VPN services necessary for encapsulation and the administration of security.

Provisioned VPNs

VPNs rely on the capability to administer preferential treatment to applications, to users, and so on. The public Internet does not support preferential treatment
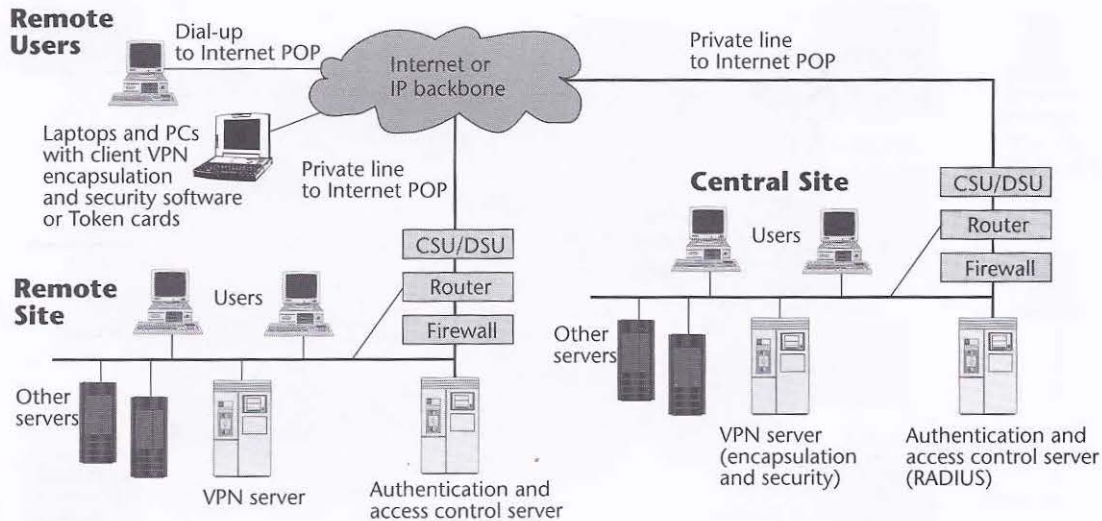
Figure 11.4   The parts of an Internet-based VPN

because it is subject to delay, jitter, and loss; it is therefore unsuitable for next-generation services that require high performance. In most cases, to accommodate business customers that are interested in such advanced services and who demand SLAs, the underlying transport is really Frame Relay or ATM. These Frame Relay and ATM VPNs offer greater levels of QoS and can fulfill the SLAs that customers and vendors agree to. They do, however, require that the customer acquire an integrated access device (IAD) to have on the premises, which can increase the deployment cost significantly. IADs enable the enterprise to aggregate voice, data, and video traffic at the customer edge.

A *provisioned VPN* (see Figure 11.5) is a packet-switched VPN that runs across the service provider's backbone, generally using Frame Relay or ATM. This type of VPN is built on OSI model Layer 2 virtual circuits, such as those used by Frame Relay, ATM, or Multiprotocol Label Switching (MPLS), and it is provisioned based on customer orders. Virtual circuits based on predetermined locations create closed user groups and work well to carve out a VPN in a public shared network, by limiting access and usage to the provisioned VPN community. However, encryption is still required to securely protect the information from theft or modification by intruders.

The provisioned VPN is differentiated from the IP VPN by its ability to support multiple protocols and by the fact that it offers improved performance and management. These VPNs are characterized as having excellent performance and security, but the negative is that a single vendor offers both reach and breadth in terms of service offerings.
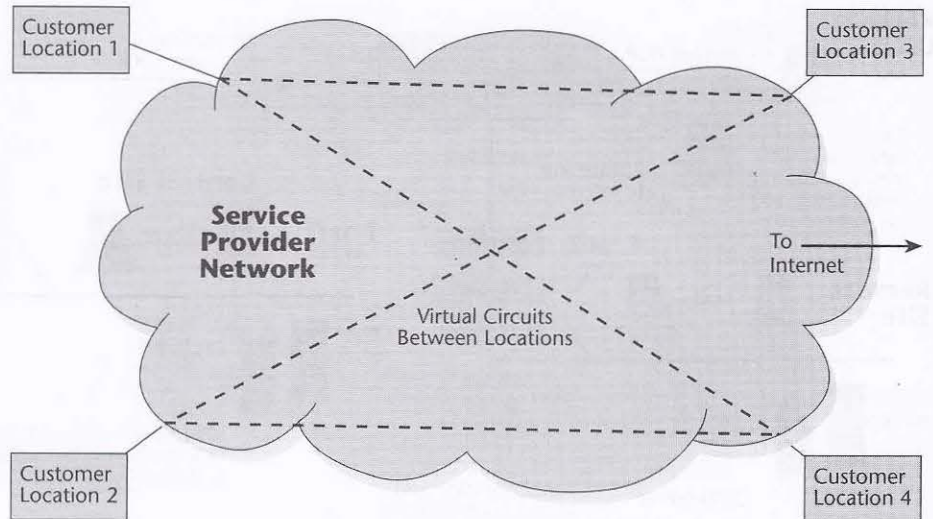
Figure 11.5 A provisioned VPN

Figure 11.6 shows what the equipment would like look at a customer premise in support of a Frame Relay- or an ATM-based VPN. The customer would have an IAD that would allow voice and data to be converged at the customer premise. The IAD would feed into the data communications equipment, over which a circuit would go to the service provider's POP. At the service provider's POP would be a multiservice access device that enables multiple protocols and interfaces to be supported and that provides access into the service provider's core network, which would be based on the use of Frame Relay or ATM. To differentiate Frame Relay- and ATM-based VPNs from Internet-based VPNs, service providers stress that multiple protocols are supported and that they rely on the use of virtual circuits or MPLS labels to facilitate the proper path, thereby ensuring better performance and providing traffic management capabilities.

To further differentiate Frame Relay- or ATM-based VPNs from regular Frame Relay or ATM services, additional functions—such as packet classification and traffic isolation, the capability to handle multiple separate packet-forwarding tables and instances of routing protocols for each customer—reside at the edge.

VPN Applications

A VPN is an architecture, a series of products and software functions that are tied together and tightly calibrated. Managing a VPN entails dealing primarily with two issues: security policies and parameters and making sure that applications function within the latency requirements.
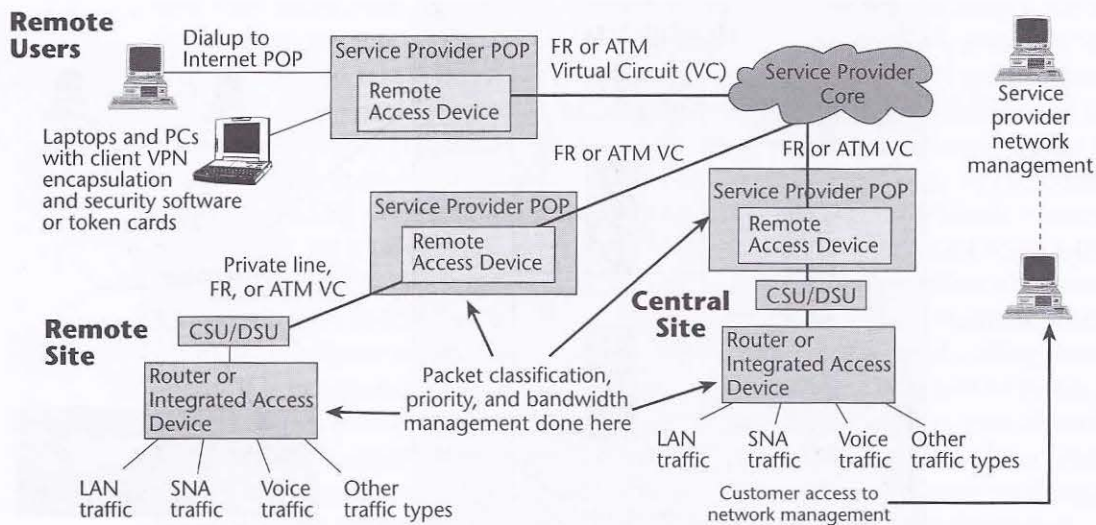
Figure 11.6 A Frame Relay- or ATM-based provisioned VPN

VPN applications provide maximum opportunities to save money and to make money—by substituting leased lines with Internet connectivity, by reducing costs of dialup remote access, and by stimulating new applications, using extranets. These savings can be substantial. According to TeleChoice (www.telechoice.com), in the realm of remote access, savings over customer-owned and maintained systems can range from 30% to 70%; savings over traditional Frame Relay services can range from 20% to 60%; savings over leased lines or private lines can range from 50% to 70%; and savings over international private lines can be up to 90%.

It is important to be able to effectively and easily manage the VPN environment. You need to consider the capability to track the tunnel traffic, the support for policy management, the capability to track QoS, the capability to track security infractions, and the support for public key certificate authorities (CAs).

The one-stop-shopping approach to VPNs—managed VPN services—is designed to lock in users and to reduce costly customer churn, but with this approach, interoperability is very restricted. Managed VPNs provide capabilities such as IP connection and transport services, routers, firewalls, and a VPN box at the customer site. Benefits of this approach include the fact that it involves a single service vendor, SLAs, guaranteed latency and bandwidth, and the security of traffic being confined to one network. Approximately one-third of VPN users opt for such a managed service.

There are three major applications of VPNs—intranets (that is, site-to-site VPNs) remote access, and extranets—which are examined in the following sections.
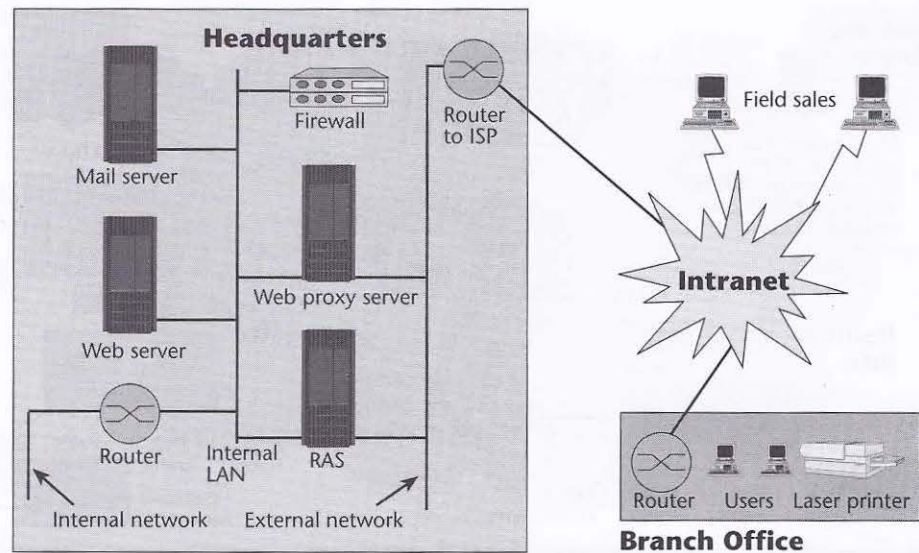
Figure 11.7 An intranet-based VPN

Intranet VPNs

Intranet VPNs are site-to-site connections (see Figure 11.7). The key objective of an intranet VPN is to replace or reduce the use of leased-line networks, traditional routers, and Frame Relay services. The cost savings in moving from private networks to Internet-based VPNs can be very high, in the neighborhood of 50% to 80% per year. Remember that Internet-based VPNs allow less control over the quality and performance of applications than do provisioned VPNs; this is a bit of a deterrent, and many clients still want to consider the Frame Relay- or ATM-based ATMs, which would provide better QoS. The savings might drop a bit, but the cost of a provisioned VPN would be substantially less than the cost of using leased lines.

There are a few key barriers to building out more intranets based on VPNs:

■ No standardized approach to encryption

■ Variance between vendors' products, which leads to interoperability problems

■ Lack of standards regarding public key management

■ Inability of today's Internet to provide end-to-end QoS

Remote Access VPNs

The most interesting and immediate VPN solution for most customers is the replacement of remote access servers. VPN remote access implementations can

save customers from 30% to 70% over traditional dialup remote access server deployment. Remote access servers provide access to remote users, generally via analog plain old telephone service (POTS) lines, or, perhaps, ISDN connections, including dialup protocols and access control for authentication (administered by the servers). However, a remote access server requires that you maintain racks of modems, the appropriate terminal adapters for ISDN services, or DSL-type modems for DSL services. You also need remote access routers, which connect remote sites via a private line or public carriers and provide protocol conversion between the LANs and WANs. To have an internal implementation of remote access, you have to acquire all these devices, as well as the talent to maintain them.

If an enterprise needs remote access connections outside local calling areas, and/or if it needs encrypted communications, it is generally fairly easy to justify a VPN service over an enterprise-based remote access server. The initial cost of hardware for a VPN approach is about 33% less than the cost of hardware for a traditional dialup remote-access server deployment. The customer also saves on charges for local access circuits, and costly toll and international charges are eliminated.

By virtue of supporting a greater range of customers, a service provider that offers VPN-based remote access is more likely to support a wider variety of broadband access options, including xDSL, cable modems, and broadband wireless. VPN-based remote access also reduces the management and maintenance required with modem banks and remote client dial-in problems. For these reasons, remote access represents the primary application for which customers turn to VPNs. Figure 11.8 shows an example of remote access VPN.
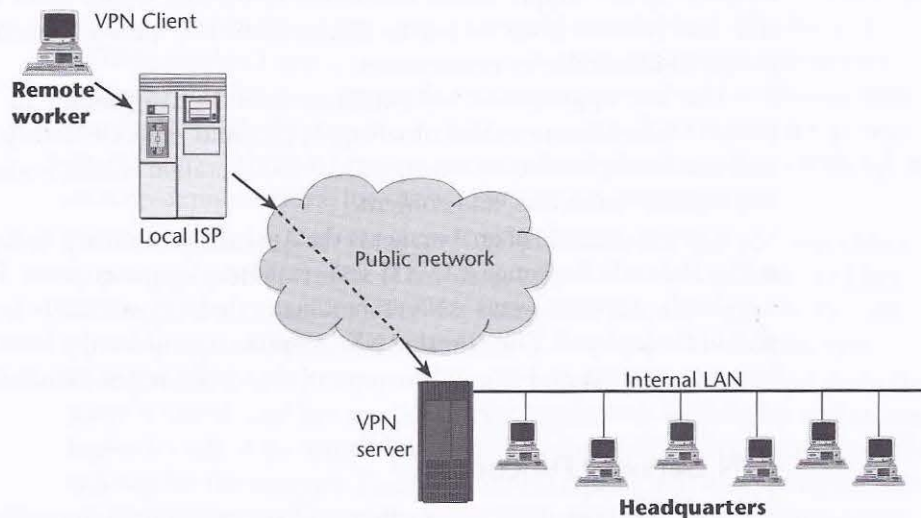

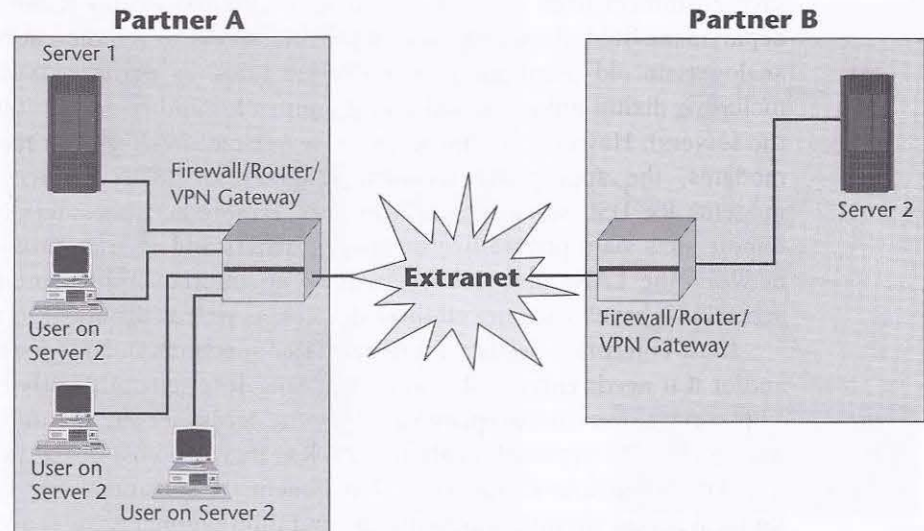**Figure 11.8**   A remote-access VPN

Figure 11.9 An extranet-based VPN

Extranet VPNs

Extranet VPNs allow an external organization to have defined access into an enterprise's internal networks and resources (see Figure 11.9). There are three major categories of extranets: supplier extranets, which focus on speeding communications along the supply chain; distributor extranets, which focus on the demand side and provide great access to information; and peer extranets, which create increased intraindustry competition.

The key applications for extranets include distribution of marketing and product information, online ordering, billing and account history, training policy and standards, inventory management, collaborative research and development, and e-mail, chat, news, and content.

A prime example of an extranet is the Automotive Industry Action Group's Automatic Network Exchange (ANX). This extranet comprises some 50,000 members worldwide. In many ways ANX is producing de facto standards for how extranets should be deployed. Check with ANX (www.anxo.com) for the latest information on how extranets are evolving and how one of the world's largest extranets is performing.

VPN Gateway Functions

The main purpose of the VPN gateways that are required to enable VPNs is to set up and maintain secure logical connections, called *tunnels*, through the Internet. Key functions of VPN gateways include packet encapsulation, authentication, mes-

sage integrity, encryption, key exchange and key management, as well as firewalling, network address translation, access control, routing, and bandwidth management. The following sections describe these functions in detail.

Tunneling Protocols

Tunneling is a method of encapsulating a data packet within an IP packet so that it can be transmitted securely over the public Internet or a private IP network. The remote ends of the tunnel can be in one of two places: They can both be at the edges of the service provider's network, or one can be at the remote user's PC and the other at the corporate boundary router. Between the two ends of the tunnel, Internet routers route encrypted packets as they do all other IP traffic.

Three key tunneling protocols are needed in VPNs:

- **Point-to-Point Tunneling Protocol (PPTP)**—PPTP was developed by Microsoft, 3Com, and Ascend, and it is included in Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, and Windows XP. PPTP is a Layer 2 protocol that can work in a non-IP enterprise environment, which is one of its strengths for customers that use multiple protocols rather than using only IP. PPTP provides low packet overhead and good compression, but its weaknesses are on the security front: It does not provide encryption or key management in the published specification, and it essentially relies on the user password to generate keys. But all implementations of PPTP include Microsoft Point-to-Point Encryption (MPPE).

- **Layer 2 Tunneling Protocol (L2TP)**—The IETF promotes L2TP, which is a merger between PPTP and Cisco's Layer 2 Forwarding (L2F) protocol. L2TP is another Layer 2 protocol that can work in a non-IP enterprise environment. L2TP is used primarily by service providers to encapsulate and carry VPN traffic through their backbones. Like PPTP, it does not provide encryption or key management in the published specification (although it does recommend IPSec for encryption and key management).

- **IP Security (IPSec)**—IPSec is an IETF protocol suite that addresses basic data integrity and security. It covers encryption, authentication, and key exchange. IPSec involves a 168-bit encryption key, although the key size can vary, depending on the capabilities of each end of the connection. Recent drafts address encapsulating the secured payload, the key management protocol, and key creation. IPSec emphasizes security by authenticating both ends of the tunnel connection, negotiating the encryption protocol and key for the encrypted session, and encrypting and decrypting the session establishment data. However, IPSec is restricted to IP environments, each user is required to have a well-defined public IP address, and IPSec cannot run on networks that use network address translation.

Benefits and Evolution of VPNs

The main benefit of VPNs as compared to leased lines or Frame Relay is cost savings. VPNs also optimize environments with IP; they have less overhead than Frame Relay, and tunneling protocols may eliminate the need for proprietary encapsulation of protocols. Provisioned VPNs also have the additional benefits of Frame Relay and ATM in the administration of virtual circuits and QoS. VPNs also provide the capability to support dialup access, and greater redundancy is achieved in the network by virtue of meshed nets. Also, VPNs do not necessarily demand a digital fiber infrastructure end-to-end.

VPNs are undergoing an evolution, and various parameters still need to be addressed. Among those are the QoS guarantees. Effective traffic prioritization is at the heart of QoS, and current mechanisms that are available include Differentiated Services (DiffServ), Class-Based Queuing, Common Open Policy Service (COPS), and Multiprotocol Label Switching (MPLS). (These mechanisms are covered in Chapter 10, "Next-Generation Networks.") Other areas of evolution in VPNs are tiering of VPN services (that is, bandwidth tiering and different policy management), the capability to support autoprovisioning, and the emphasis on security.

QoS and security are the two most important considerations in administering VPNs, so uptimes, delays, and SLAs need to be structured. For example, QoS guarantees could be structured to promise 100% premises-to-premises network availability and a maximum latency guarantee of 80 milliseconds. Some vendors offer separate SLAs for dedicated and remote access. For dedicated access, the SLA offers an availability guarantee of 99.9% and a maximum latency guarantee of 125 milliseconds. On remote access SLAs, a busy-free dial availability guarantee of 97% is stipulated, and the latency guarantee specifies an initial modem connection speed of 26.4Kbps at 99%.

▪ Security

Security is very important to the proper operation of VPNs. This section describes the available security mechanisms and the anticipated developments in the realm of standards for encryption and key management.

Firewalls

A *firewall* is typically defined as a system or a group of systems that enforces and acts as a control policy between two networks. It can also be defined as a mechanism used to protect a trusted network from an untrusted network—usually while still allowing traffic between the two. All traffic from inside to outside and vice versa must pass through the firewall. Only authorized traffic, as defined by the

Viruses

Virus is a term that's used broadly to refer to a program that is designed to interfere with computers' normal operations. The tab for all computer viruses in 1999 was, shockingly, greater than US$12 billion.

The term *virus* can be used more narrowly to refer to programs that move from one file to another and can be transmitted to other PCs via an infected file. They generally don't seek out the Internet or e-mail to spread.

Another type of virus is the *worm*, such as the Love Bug. Worms make use of a LAN or the Internet (especially via e-mail) to replicate and forward themselves to new users.

Finally, a *Trojan horse* hides within another program or file and then becomes active when someone opens the unwitting host.

A big part of administrating security involves managing viruses. The fact that we can deploy such functionality on a proxy server is very attractive.

local security policy, is allowed to pass through it. The system itself is highly resistant to penetration. A firewall selectively permits or denies network traffic.

There are several variations of firewalls, including these:

- A firewall can use different protocols to separate Internet servers from internal servers.
- Routers can be programmed to define what protocols at the application, network, or transport layer can come in and out of the router—so the router is basically acting as a packet filter.
- Proxy servers can be used to separate the internal network users and services from the public Internet. Additional functions can be included with proxy servers, including address translation, caching, encryption, and virus filtering.

Authentication

Another aspect of security is the authentication of users and access control, which is commonly handled by RADIUS. RADIUS servers are designed to block unauthorized access by remote users. RADIUS provides authentication, authorization, and accounting, and it relies on Challenge Handshake Authentication Protocol (CHAP) to authenticate remote users, which means that there's a back-and-forth dialogue to verify a user's identity. In fact, RADIUS makes use of CHAP, which uses a three-way handshake to periodically verify the identity of the peer throughout the connection. The server sends a random token to the remote workstation. The token is then encrypted, by using the user's password, and sent back to the server. The

server performs a lookup to see whether it recognizes the password. If the values match, the authentication is acknowledged; if the values do not match, the connection is terminated. Because a different token is provided each time a remote user dials in, CHAP provides robust authentication.

Encryption

The best way to protect electronic data is to use encryption—that is, to encode data so as to render a document unreadable by all except those who are authorized to have access to it. The content of an original document is referred to as *plain text*. When encryption is applied to the document, the plain text is scrambled, through the use of an algorithm and a variable or a key; the result is called *ciphertext*. The key is a randomly selected string of numbers. Generally, the longer the string, the stronger the security.

There are two major categories of encryption algorithms: symmetric and asymmetric (also called *public key encryption*).

Symmetric Encryption

In symmetric encryption, the sender and the receiver use the same key or machine setup. There are two approaches to encoding data using symmetric encryption: block cipher and streaming cipher. With the block cipher approach, the algorithm encodes text in fixed-bit blocks, using a key whose length is also fixed in length. With the streaming cipher approach, the algorithm encodes the stream of data sequentially, without segmenting it into blocks. Both of these techniques require a secure method of reexchanging keys between the participants.

Symmetric encryption algorithms include the following:

- **Data Encryption Standard (DES)**—DES was developed in the 1970s and is very popular in the banking industry. It is a block cipher that encodes text into fixed-bit blocks, using a 56-bit key. DES is being replaced by the Advanced Encryption Standard (AES).

- **Triple DES (3DES)**—3DES is 168-bit encryption that uses three 56-bit keys. 3DES applies the DES algorithm to a plain text block three times.

- **Rivest Cipher 4 (RC4)**—RC4 is a streaming cipher technique; a stream cipher adds the output of a pseudorandom number generator bit by bit to the sequential bits of the digitized plain text.

- **Blowfish**—Blowfish is a 64-bit block code that has key lengths of 32 bits to 448 bits. Blowfish is used in more than 100 products, and it is viewed as one of the best available algorithms.

- International Data Encryption Algorithm (IDEA)—IDEA, developed by ETH Zurich, is free of charge for noncommercial use. It is viewed as a good algorithm and is used in Pretty Good Privacy (PGP) and in Speak Freely, a program that allows encrypted digitized voice to be sent over the Internet.

- Twofish—Twofish, developed by Bruce Schneier of Counterpane Internet Security, is very strong, and it was one of the five initial candidates for the AES.

According to the National Institute of Standards and Technology (NIST), it would take 149 trillion years to crack the U.S. government's AES, which uses the Rijndael algorithm and specifies three key lengths—128 bit, 192 bits, and 256 bits. In comparison, DES, which uses a 56-bit key, would take only a matter of hours using a powerful computer, but, of course, this is totally dependent on the speed of the hardware used for cracking the code; a typical desktop PC would require much more than a few hours to crack a 56-bit DES key.

Asymmetric Encryption

Key encryption requires a secure method for exchanging keys between participants. The solution to key distribution came, in 1975, with Diffie and Hellman's public key cryptography scheme. This permits the use of two keys, one of which can be openly published and still permit secure encrypted communications. This scheme later became known as *asymmetric key cryptography.*

Asymmetric cryptography can be used for authentication. After encrypting a signature by using a private key, anyone with access to the public key can verify that the signature belongs to the owner of the private key. As shown in Figure 11.10, the following are the steps in public key encryption:

1. User A hashes the plain text.
2. User A encrypts that hash value with a private key.
3. User A encrypts the plain text with user B's public key.
4. User B decodes the cipher text with the private key.
5. User B decodes the hash value, using User A's public key, thereby confirming the sender's authenticity.
6. User B compares the decrypted hash value with a hash value calculated locally on the just-encrypted plain text, thereby confirming the message's integrity.

Public key management involves the exchange of secrets that both ends use to produce random short-term session keys for authenticating each other. It is a method of encrypting data by using two separate keys or codes. The sender uses a public key that is generally provided as part of a certificate issued by a CA to
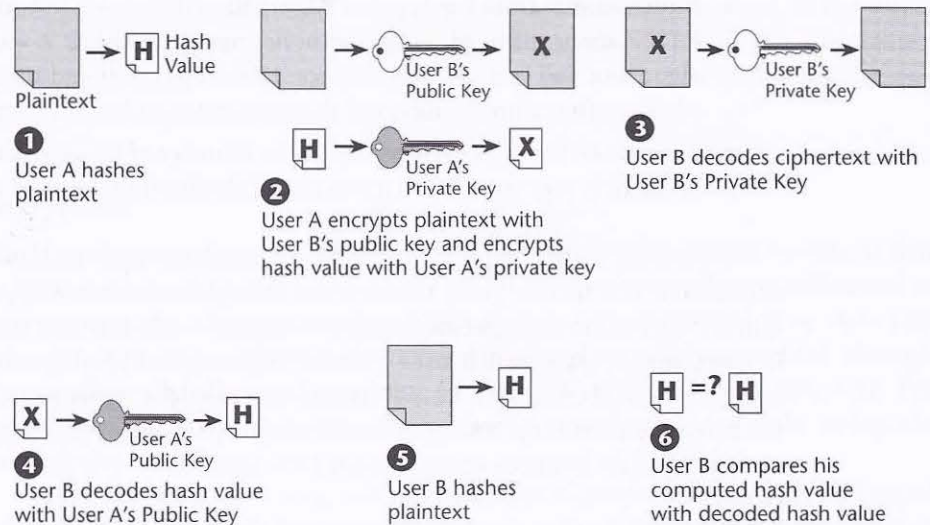
Figure 11.10 Encryption and authentication

scramble data for transmission. The receiver then uses a unique private key to decrypt the data upon receipt. The CA is an entity that, like a bank, is government regulated. It issues certificates that contain data about individuals or enterprises that has been verified to be authentic. In essence, the CA vouches for the authenticity of other parties so that their communications are secured.

Message authentication verifies the integrity of an electronic message and also verifies that an electronic message was sent by a particular entity. Before an outgoing message is encrypted, a cryptographic hash function—which is like an elaborate version of a checksum—is performed on it. The hash function compresses the bits of the plain-text message into a fixed-size digest, or hash value, of 128 or more bits. It is then extremely difficult to alter the plain-text message without altering the hash value.

Message authentication mechanisms include Message Digest-5 (MD5) and Secure Hash Algorithm-1 (SHA-1). MD5 hashes a file of arbitrary lengths into 128-bit value. SHA-1 hashes a file of arbitrary length into 160-bit value; it is more processor intensive but it renders higher security.

Public key management provides a secure method for obtaining a person's or an organization's public key, with sufficient assurance that the key is correct. There are three main public key algorithms: RSA (named for its creators, Rivest, Shamir, and Adelman), Diffie-Hellman, and PGP. RSA is 22 years old, and its security derives from the difficulty of factoring large prime integers. Diffie-Hellman is used mostly for exchanging keys; its security rests on the difficulty of computing discrete algorithms in a finite field, generated by a large prime number. PGP, which is