

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ERICSSON INC.,
Petitioner

v.

KONINKLIJKE KPN N.V.,
Patent Owner

Patent No. 8,886,772

**DECLARATION OF DR. DANIEL BLUMENTHAL
IN SUPPORT OF ERICSSON'S PETITION FOR
INTER PARTES REVIEW OF U.S. PATENT NO. 8,886,772**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND AND QUALIFICATIONS	1
III.	MATERIALS REVIEWED	8
IV.	INSTRUCTIONS	9
V.	LEVEL OF ORDINARY SKILL	13
VI.	TECHNICAL BACKGROUND	14
A.	Broadband network architecture (LANs, PONs, MANs, WANs)	15
B.	Layered model and Protocol Stacks	22
C.	Packet switches and Routers	25
D.	Packet and Frame Technologies	32
E.	Multiprotocol Label Switching (MPLS)	38
F.	Network Discovery and Internet Border Gateway Protocol BGP/IP and Open Path Shortest First (OSPF)	39
G.	TR-069 CPE WAN Management Protocol (CWMP)	41
VII.	OVERVIEW OF THE '772 PATENT	47
VIII.	CLAIM CONSTRUCTION	60
IX.	DISCUSSION OF GROUNDS	63
A.	Ground 1: <i>Angelot</i> Discloses or Suggests Each and Every Feature of Claims 2-6, 11, 14 and 16 alone or in view of the knowledge of a person having ordinary skill in the art.	63
1.	Claim 1 (cancelled)	74
2.	Claim 2	103

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

3.	Claim 3	107
4.	Claim 4	110
5.	Claim 5	111
6.	Claim 6	113
7.	Claim 10 (cancelled)	115
8.	Claim 11	116
9.	Claim 12 (cancelled)	117
10.	Claim 14	118
11.	Claim 15 (cancelled)	119
12.	Claim 16	120
B.	Ground 2: <i>Angelot</i> as Modified by the Knowledge of a person having ordinary skill in the art Discloses Each and Every Feature of Claims 2-6, 11, 14, 16.....	120
C.	Ground 3: <i>Angelot</i> in view of <i>Zakurdaev</i> and the Knowledge of a person having ordinary skill in the art Discloses Every Feature of Claims 2-6, 11, 14, 16.....	131
X.	CONCLUSION.....	137

LIST OF EXHIBITS

- Ex. 1001 U.S. Patent No. 8,886,772
- Ex. 1004 Prosecution History of U.S. Patent No. 8,886,772
- Ex. 1005 Markman Order from *Koninklijke KPN NV v. Samsung Electronics America, Inc. et al.*, 2-14-cv-01165-JRG (E.D. Tex.)
- Ex. 1006 U.S. Patent Publication No. 2009/0201830 to *Angelot*
- Ex. 1007 U.S. Patent Publication No. 2002/0073182 to *Zakurdaev*
- Ex. 1008 U.S. Patent Publication No. 2003/0061315 to *Jin*
- Ex. 1009 Joint Claim Construction Brief (Dkt. No. 57) filed in *KPN v. Xiaomi*, 21-cv-00041-GBW-CJB (D. Del. June 10, 2022)
- Ex. 1010 TR-069 (“CPE WAN Management Protocol v.1.1”, Broadband Forum, Issue 1 Amendment 2, December 2007)
- Ex. 1011 Excerpts of Microsoft Computer Dictionary, Fifth Edition, dated 2002 (ISBN 0-7356-1495-4)
- Ex. 1012 RFC 2131 (“Dynamic Host Configuration Protocol”, R. Droms, March 1997)
- Ex. 1013 RFC 2132 (“DHCP Options and BOOTP Vendor Extensions”, S. Alexander et al., March 1997)
- Ex. 1014 Joint Request for Stay Pending Settlement (Dkt. No. 105) filed in *KPN v. Xiaomi*, 21-cv-00041-GBW-CJB (D. Del. Nov. 28, 2022).
- Ex. 1015 An Introduction to Packet Switching (Nick McKeown)

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

- Ex. 1016 Next Generation Optical Networks, Peter Tomsu, dated 2002
(ISBN 0-13-028226-X)
- Ex. 1017 Optical Fiber Telecommunications, Ivan Kaminow, dated 2008
(ISBN 978-0-12-374172-1)
- Ex. 1018 A Quick Tutorial on IP Router Design, Nick McKeown, dated
October 10, 2000.
- Ex. 1019 Prosecution History of U.S. Patent No. 9,838,256

I, Dr. Daniel Blumenthal, declare as follows:

I. INTRODUCTION

[001] I have been retained by Ericsson Inc. (“Ericsson” or “Petitioner”) as an independent expert consultant in this proceeding before the United States Patent and Trademark Office (“PTO”) regarding U.S. Patent No. 8,886,772 (the ’772 patent) (Ex. 1001).¹ I have been asked to consider whether certain references disclose or suggest the features recited in claims 2-6, 11, 14 and 16 of the ’772 patent. My opinions are set forth below.

[002] I am being compensated at a rate of \$625/hour for my work in this proceeding. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding.

II. BACKGROUND AND QUALIFICATIONS

[003] My complete qualifications and professional experience are described in my *Curriculum Vitae*, a copy of which can be found in Exhibit 1003

¹ Where appropriate, I refer to exhibits that I understand are to be attached to the petition for *Inter Partes* Review of the ’772 patent.

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

[004] The following is a brief summary of my relevant qualifications and professional experience.

[005] My education and my experience in this and related areas span over 40 years of professional and academic experience.

[006] I am considered a pioneer in communications systems.

[007] I received a B.S. degree in Electrical Engineering from the University of Rochester, Rochester, New York, in 1981, a M.S. degree in Electrical Engineering from Columbia University, New York, in 1988, and a Ph.D. degree in Electrical Engineering from the University of Colorado, Boulder, in 1993. From 1981 until 1984, I worked as an engineer at StorageTek, Louisville, Colorado, on one of the world's first optical data storage products. From 1984 to 1985 I worked as a Senior Engineer at Sievers Research in the area of optical spectroscopy. From 1985 - 1988, I worked at Columbia University Center for Telecommunications Research (CTR) as a research engineer while pursuing my Masters degree in Electrical Engineering. The CTR was one of the National Science Foundation (NSF) centers of excellence that launched the modern telecommunications networks and spawned a wide range of technologies and advances from multi-media communications, including packet communications, voice and video networking, and network layered architectures. From 1988 to 1990 I worked in the Distributed Computing Systems Laboratory at the University of

Pennsylvania, led by Prof. David J. Farber, one of the originators of the internet and pioneer of distributed communications systems (DCS) that is a pre-cursor to today's internet cloud. During that period the Farber research group addressed the early work and standardization in ATM and TCP/IP Ethernet. From 1990 to 1993, I pursued my PhD degree as a graduate researcher in the NSF Optoelectronic Computing Center at the University of Colorado Boulder, where I built one of the world's first self-routing optical packet switches. From 1993 to 1997, I was Assistant Professor in the School of Electrical and Computer Engineering at the Georgia Institute of Technology in Atlanta where I built a research program and lab in communications and packet switching, my area of focus at the time.

[008] I am currently a Distinguished Professor in the Department of Electrical and Computer Engineering at the University of California, Santa Barbara (UCSB) where I have taught and conducted research since 1997. I also serve as the Director of the Terabit Optical Ethernet Center (TOEC). My research areas include, among others, communications and packet switching.

[009] I have authored or co-authored over 512 journal and conference publications, hold 23 issued US patents, and am a co-author of a book, *Tunable Laser Diodes and Related Optical Sources* (New York: IEEE–Wiley, 2005) as well as other book chapters. I have published two invited papers in the prestigious, broadly read, *Proceedings of the IEEE* and one invited paper in the prestigious

broadly read Scientific American magazine. The Proceedings of the IEEE is the leading IEEE journal that provides in-depth review, survey, and tutorial coverage of the technical developments across all engineering areas including electronics, electrical and computer engineering, and computer science and is ranked as one of the top journals by Impact Factor, Article Influence Score and serves as a resource for engineers around the world.

[010] I have served as the principal investigator for multiple large-scale research programs funded by the Defense Advanced Research Projects Agency (DARPA)/Microsystems Technology Office (MTO) including the DARPA LASOR project that conducted research in packet switching and label swapping technologies and architectures.

[011] I was an elected Board Member for the Internet-2 Architecture & Operations Advisory Council from 2008-2012.

[012] In addition to my industry experience at StorageTek and Sievers, I have co-founded two companies, Packet Photonics, Inc. and Calient Technologies, Inc. Packet Photonics, Inc. provided network and data center operators with photonic integrated wavelength tunable transceiver solutions and pluggables to implement, install, operate, and maintain networks. Calient Technologies, Inc. provides software enabled adaptive MEMS mirror based photonic switching

systems that enable dynamic optical layer switching and optimization in broadband and high capacity networks.

[013] While working in industry and at my startup companies, I was involved in the Internet Engineering Task Force (IETF) and the Optical Internetworking Forum (OIF) standards bodies. For example, I contributed to proposals in the IETF that involved sending and updating impairment information related to transmission links, to nodes within a routing network using generalized multiple protocol label switching (G-MPLS) control plane protocols: Internet Draft Document: draft-ietf-ipo-impairments-01.txt, Expiration Date 2002 (<https://www.ietf.org/proceedings/52/I-D/draft-ietf-ipo-impairments-01.txt>).

[014] I was elected as a Fellow of the National Academy of Inventors (NAI) in 2017. From the NAI website: “The program has 1,060 Fellows worldwide representing more than 250 prestigious universities and governmental and non-profit research institutes. Collectively, the Fellows hold more than 38,000 issued U.S. patents, which have generated over 11,000 licensed technologies and companies, and created more than 36 million jobs. In addition, over \$1.6 trillion in revenue has been generated based on NAI Fellow discoveries. With the induction of the 2018 class, there are now more than 125 presidents and senior leaders of research universities and non-profit research institutes, 502 members of the National Academies of Sciences, Engineering, and Medicine; 40 inductees of the

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

National Inventors Hall of Fame, 57 recipients of the U.S. National Medal of Technology and Innovation and U.S. National Medal of Science, 34 Nobel Laureates, 3 Queen Elizabeth Prize for Engineering recipients, 304 AAAS Fellows, 200 IEEE Fellows, and 164 Fellows of the American Academy of Arts & Sciences, among other awards and distinctions.”

[015] In 2020 I was recipient of the prestigious Optical Society of America C.E.K. Mees medal. The medal was established in 1961 in memory of charter member C. E. K. Mees, to recognize achievements that exemplifies the thought that "optics transcends all boundaries". Prior to 2017 the medal was presented every two years since 1962, and it has been presented annually since 2017. Former recipients of the medal include Charles H. Townes, inventor of the laser.

[016] I am a Fellow of the IEEE (only 0.1% of the world-wide membership can be elected as Fellows in a given year: “According to IEEE Bylaw I-305.5, "The total number of Fellow recommendations in any one year must not exceed one-tenth of one percent of the IEEE voting membership on record as of 31 December of the year preceding."). I am also a Fellow of Optica (formerly the Optical Society of America (OSA)). I am a recipient of a 1999 Presidential Early Career Award for Scientists and Engineers (PECASE) from the White House. I also received a National Science Foundation Young Investigator (NYI) Award in 1994, and an Office of Naval Research Young Investigator Program (YIP) Award

in 1997. The Presidential White House PECASE Award citation reads “For outstanding research and creative impact in multi-wavelength optical techniques.”

[017] I have had extensive contributions to the international scientific community in the form of internationally renowned special issue journals and international conferences. I have served as the primary Guest Editor for multiple special issues of the IEEE journals including the 2003 IEEE Journal Of Selected Areas In Communications special issue on “High-Performance Optical/Electronic Switches/Routers for High-Speed Internet.” In terms of regular journal editing, I am currently on the Editorial Board of the prestigious Nature Light Science and Applications journal, and was an Associate Editor for the IEEE Photonics Technology Letters and an Associate Editor for the IEEE Transactions on Communications for many years. I have organized and served on committees for internationally renowned conferences and topical meetings including as General Program Chair for the 2001 OSA Topical Meeting on Photonics in Switching and as Program Chair for the 1999 Meeting on Photonics in Switching. I have also served on numerous other technical program committees including the Conference on Optical Fiber Communications OFC (2018 – Present and 1997 – 2000), the Conference on Lasers and Electrooptics CLEO (1999-2000), the European Conference on Optical Communications ECOC (2004-2005) and SIGCOMM 2006.

[018] I am not an attorney and offer no legal opinions, but in the course of my work, I have had experience studying and analyzing patents and patent claims from the perspective of a person skilled in the art.

III. MATERIALS REVIEWED

[019] The opinions contained in this Declaration are based on the documents I reviewed, my professional judgment, as well as my education, experience, and knowledge regarding optical networking systems.

[020] In forming my opinions expressed in this declaration, I reviewed the exhibits referred to above in the table of exhibits and any other materials that I refer to in this declaration in support of my opinions.

[021] I have been asked to consider the time of the claims to be the mid-to-late 2000s, including July 31, 2008, the priority date of '772 patent. My opinions in this declaration reflect how a person of ordinary skill in the art would have understood the claims and the specification of the '772 patent, the prior art to the patent, and the state of the art at the time of the the application for the 772 patent was filed.

[022] As I discuss in detail below, it is my opinion that certain prior art references disclose or suggest all the features recited in the challenged claims of the '772 patent.

IV. INSTRUCTIONS

[023] I am not an attorney. Counsel provided the following instructions to me: My analysis and opinions are based on my expertise in this technical field, as well as the instructions that I have been given by counsel for the legal standards relating to patentability as outlined in the rest of this section.

[024] The materials I have reviewed in connection with my analysis include the '772 Patent, its file history, and the exhibits identified in the Table of Exhibits above.

[025] I understand that unpatentability in this proceeding must be proven by a preponderance of the evidence, and this is the standard I have used throughout my declaration. Further, I understand that each patent claim is considered separately for purposes of unpatentability.

[026] I understand that a patent claim is unpatentable as “anticipated” if each and every feature of the claim is found in a single prior art reference.

[027] I understand that a patent claim is unpatentable as “obvious” if, in view of a prior art reference or a combination of prior art references, it would have been obvious to a person of ordinary skill in the art (“person having ordinary skill in the art”) at the time of the invention, taking into account:

- (a) the scope and content of the prior art;

- (b) the differences between the prior art and the claim under construction; and
- (c) the level of ordinary skill in the art.

[028] I am informed that legal principles regarding unpatentability of a claim due to obviousness have been addressed by the U.S. Supreme Court. I am informed that, while not absolute, the principles relating to a “motivation,” “suggestion,” or “teaching” in the prior art to combine references are useful in analyzing whether an invention is obvious. I am informed that the suggestion or motivation may be either explicit or implicit and may come from knowledge generally available to a person having ordinary skill in the art, from the nature of the problem to be solved, or from a combination of these factors. The test for an implicit motivation, suggestion, or teaching is what the combined teachings, knowledge of a person having ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art. The problem examined is not the specific problem solved by the invention, but the general problem that confronted the inventor before the invention was made.

[029] I am further informed that the U.S. Supreme Court has clarified that additional principles may also be applied in such an analysis. Some of those principles are set forth below.

[030] As I understand it, it is no longer always required to present evidence of an explicit teaching, suggestion, or motivation to combine prior art references for purposes of determining whether an invention is obvious. Prior art can be combined based on an express teaching, suggestion, or motivation from the prior art itself, or from a reasoned explanation of an expert or other witness.

[031] A patent claim composed of several elements, however, is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. In order to prove obviousness, it must be shown that the improvement is not more than the predictable use of prior-art elements according to their established functions. To determine whether there was an apparent reason to combine the known elements in the way a patent claims, it will often be necessary to look to interrelated teachings of multiple pieces of prior art, to the effects of demands known to the design community or present in the marketplace, and to the background knowledge possessed by a person having ordinary skill in the art. Also, in determining obviousness, one must be aware of the distortion caused by hindsight bias and be cautious of arguments relying upon hindsight reasoning. An obviousness argument cannot be sustained by mere

conclusory statements. Instead, it must be some articulated reasoning with some rational underpinnings to support the legal conclusion of obviousness.

[032] In an obviousness analysis, it is my understanding that there are “secondary considerations” that should be analyzed if they apply. I am told that these considerations include (a) whether the prior art teaches away from the claimed invention, (b) whether there was a long felt but unresolved need for the claimed invention, (c) whether others tried but failed to make the claimed invention, (d) skepticism of experts, (e) whether the claimed invention was commercially successful, (f) whether the claimed invention was praised by others, and (g) whether the claimed invention was copied by others.

[033] I have also been informed that the Board construes claims according to the so-called “Phillips” standard. Under the Phillips standard, terms in a claim are given their ordinary and customary meaning, consistent with the patent’s specification, as understood by a person having ordinary skill in the art. It is my understanding that what is to be considered includes the claims, the patent specifications and drawings, and the prosecution history, including any art listed by the examiner or the Applicant. It is my understanding that information external to the patent, including expert and inventor testimony and unlisted prior art, are to be considered if ambiguities remain. However, expert testimony may be useful in helping to explain the technology.

V. LEVEL OF ORDINARY SKILL

[034] It is my understanding that a person of ordinary skill in the art (“person having ordinary skill in the art”) is a hypothetical person who is presumed to have known the relevant prior art at the time the application that led to the Asserted Patent was filed. I understand the factors that may be considered in determining the level of ordinary skill in the art may include: 1) type of problems encountered in the prior art; 2) prior art solutions to those problems; 3) rapidity with which innovations are made; 4) sophistication of the technology; and 5) educational level of active workers in the field.

[035] I also understand that a person of ordinary skill in the art is also a person of ordinary creativity, not an automaton. They would be able to fit the teachings of multiple patents together like a puzzle and have the capability of understanding the scientific and engineering principles applicable to the pertinent art.

[036] In my opinion, a person having ordinary skill in the art as of the claimed priority date of the '772 patent would have had a B.S. in Electrical Engineering or a related field with at least five years of experience in designing communications systems. More education can supplement practical experience and vice versa.

[037] I understand that a person having ordinary skill in the art is a hypothetical person that is used to analyze the prior art without the benefit of hindsight. A person of ordinary skill in the art is presumed to be one who thinks along the lines of conventional wisdom in the art and is not one who undertakes to innovate, whether by extraordinary insights or by patient and often expensive systematic research. A person of ordinary skill in the art is not the judge, nor a layperson, nor one skilled in remote arts, nor a genius in the art, nor the inventor.

[038] I understand that the hypothetical person of ordinary skill in the art is presumed to have knowledge of all references that are sufficiently related to one another and to the pertinent art and to have knowledge of all arts reasonably pertinent to the particular problem that the claimed invention addresses.

[039] All of my opinions in this declaration are from the perspective of a person having ordinary skill in the art, as I have defined it above and during the relevant time frame, i.e., late 2008. During this time frame, I possessed at least the qualifications of a person of ordinary skill in the art, as defined above.

VI. TECHNICAL BACKGROUND

[040] In this section, I will discuss the concepts and techniques that were known to a person of ordinary skill in the art prior to the '772 patent.

A. Broadband network architecture (LANs, PONs, MANs, WANs)

[041] Since the early 2000s, broadband communications networks have been designed to connect residential, business, and mobile users to services and other users through a hierarchal network architecture. The broadband network architecture provides trade-offs between cost, reach (distance), number of users, and aggregate and per user bandwidth (capacity). Early broadband networks of the 2000s evolved to the cloud infrastructure that we have today. The broadband communication infrastructure connects a hierarchy of networks, including local area networks (LANs), campus networks, enterprise networks, metropolitan area networks (MANs), wide area networks (WANs) and long-haul (LH), ultralong haul (ULH) and backbone networks that formed the early internet. The design, cost, performance, and allocation of network resources were driven by what is connected to each sub-network, what that network connects to, and its aggregate capacity and cost scaling structure. As illustrated in Fig. 1, access networks connect to residential, business and mobile users and minimize the cost of equipment to the premises and monthly cost to the customer. Aggregation networks span metro- and wide-area distances and connect and have the capacity to multiple connected access networks in a region. The service edge connects multiple metro-scale, or regional networks to each other and to the core, and the core connects edge and metro networks to each other and over long distances.

[042] These networks used combinations of packet/frame switching (L2 and L3, described later) technologies and transport (L0 and L1, described later) technologies. Modern data switching technologies have been in development since the 1980s, and include asynchronous transfer mode (ATM), frame relay, and variable length packet IP switching. Modern transport technologies have been in development since the 1990s and early 2000s including ethernet packet transport, MPLS (multi-protocol label switching), and fiber-optic transport including SONET (synchronous optical network), WDM (wavelength division multiplexing) and OTN (optical transport network).

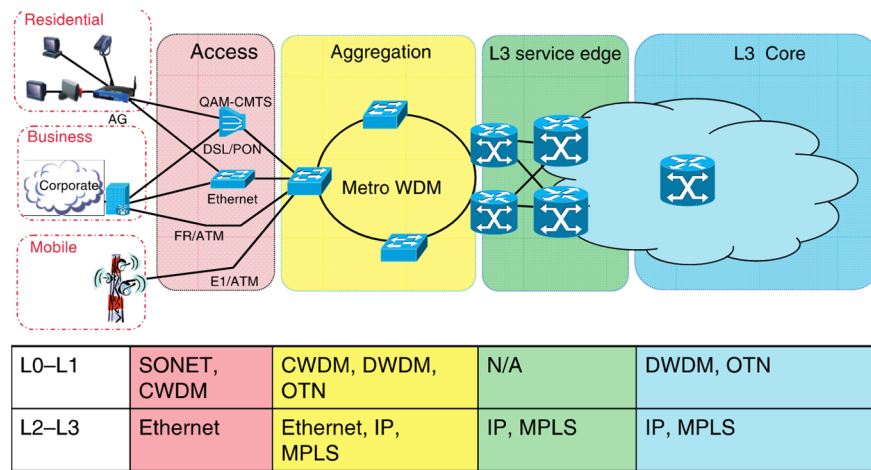


Figure 1. Kaminow, Li, Willner (2008) Ex. 1017.

[043] During the late 1980s and early 1990s, there was a world-wide effort to develop a uniform packet transport and switching technology called asynchronous transfer mode (ATM) that would support broadband networking and transport (e.g., B-ISDN) and switching of video, voice, and data. ATM is a fixed cell size format that required customer and switch interfaces to break up video,

voice, and data streams into the fixed cells (packets that are 53 Bytes long) which contained content identifier information and packet routing headers among other information. Networks, user interfaces, and routers/switches were commercialized that routed ATM packets and broadband traffic over virtual circuit that gave the user the feel of a dedicated circuit but the cost structure of sharing the bandwidth with other users. While the packetization of broadband traffic allowed users to transmit video, voice, and data over the shared internet, the cost of the ATM interfaces was too expensive for LAN users, and the technology lost out to the lower cost Ethernet and IP standards and technology.

[044] Ethernet, a packet technology based on variable length packets, had evolved through the 1980s to become the TCP/IP standard that could support the transmission of video, voice and data using very low cost ethernet interfaces for each user in the LAN. At first, network Ethernet routers were built by adding interfaces to installed ATM routers. Eventually, routers and switches were deployed that were optimized for IP. Due to the low cost of Ethernet interfaces and an industry-wide commitment to reducing board-level electronic chip technologies, there was significant infrastructure investment in the early 2000s to migrate the national and world-wide communications infrastructure to an IP packet centric model all the way from the residential, business and wireless premises to the

network core. An example of a packet transport based broadband architecture broadband to the home is shown in Fig. 2.

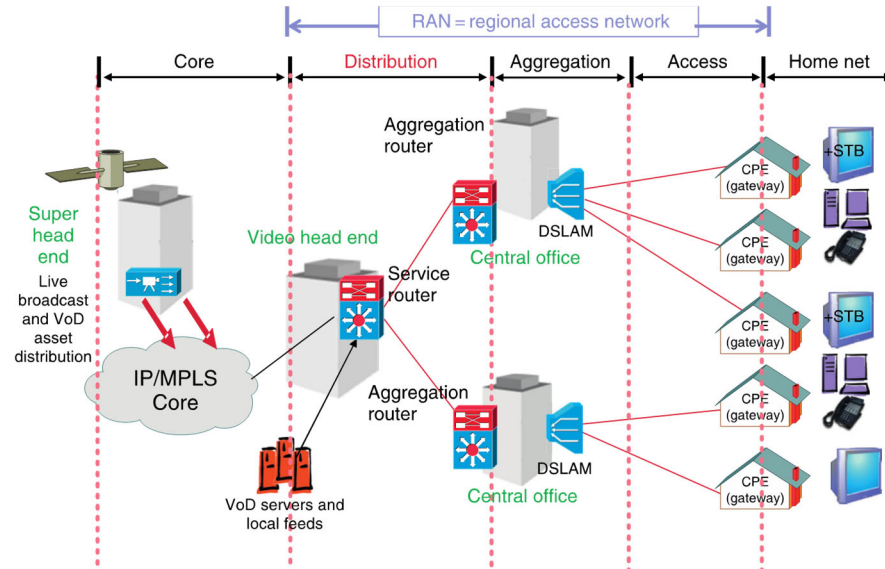


Figure 2. Kaminow, Li, Willner (2008). Ex. 1017.

[045] These networks had to satisfy certain scaling rules, including the cost to interface a user at the home or business, the cost of monthly services to the user, and the cost of the aggregation equipment (Capex), operating expenditures (Opex) and maintenance at the various network layers, as well as the capacity and optimization of performance metrics like latency and bandwidth availability and downtime. An example of an early subscriber access network serving residential and business customers using a fiber optic distribution network to connect LANs to a metro network is shown in Fig. 3. The low cost interfaces were deployed at the users via a low cost distribution network, and higher cost aggregation and switching equipment were deployed at the head-end of each distribution network

which serviced many users. Passive splitting technology was also employed, and combinations of fiber, coaxial, and twisted pair copper were utilized to provide the best service at the lowest cost to the user and for the network provider. Examples included hybrid fiber coaxial (HFC), fiber to the curb with DSL to the home (FTTC/xDSL) and fiber to the home (FTTH).

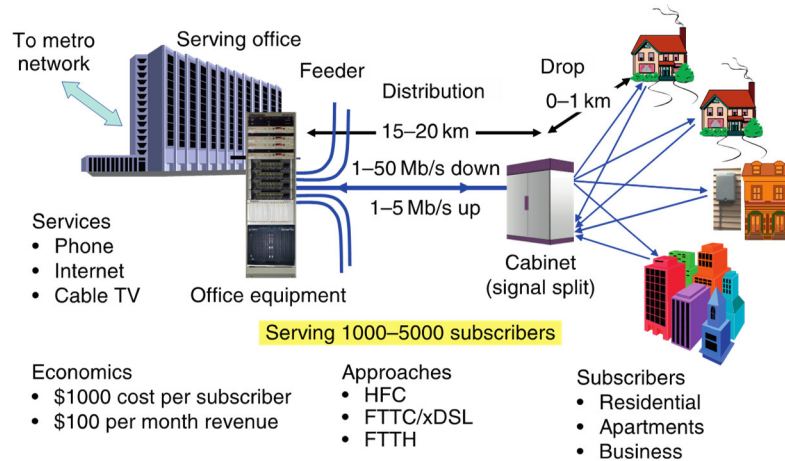


Figure 3. Kaminow, Li, Willner (2008). Ex. 1017.

[046] The PONs were connected to metro-networks, or wide area

networks, that contained higher capacity, more sophisticated transmission and switching equipment that could interconnect many PONs to hub facilities such as video servers and storage networks. These metro networks efficiently aggregated user data, internet data, and video data onto fiber optic pipes and moved the data around using sophisticated data switching equipment. When data and users had to be connected over longer distances over the backbone network, long-haul fiber transmission cables and switches were utilized. The connection of a LAN to the higher layer networks, for example the MAN aggregation layer, was accomplished

through a LAN gateway as shown in Fig. 4. The MAN router network allowed connection of the LAN to any number of multiple resources including configuration servers, video servers, data storage networks (SANs) and more, to other MANs and LANs connected across the core network. The configuration of the access or LAN and the MAN and the servers the users connected to were automatically configured via a control plane that handled node discovery protocols, distributed control, and other switching, routing and network level functions.

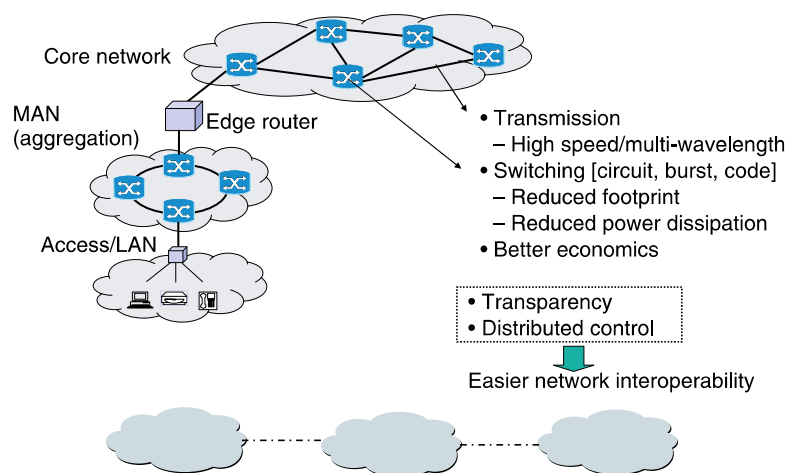


Figure 4. Kaminow, Li, Willner (2008). Ex. 1017.

[047] Configuring the MAN and core to support broadband media and content delivery, the broadband access networks and LANs were connected via gateways to content delivery providers and servers that were configured under the management of an automatic control plane as illustrated in Fig. 5.

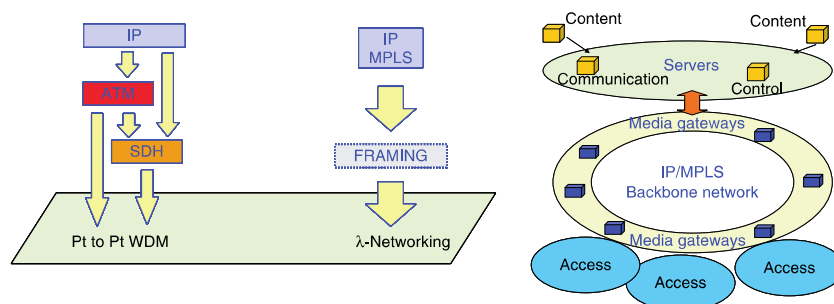


Figure 5. Kaminow, Li, Willner (2008). Ex. 1017.

[048] The control plane supported programmable control and management of the nodes, transport, and network, and is handled using one of two models, the peer network or the UNI illustrated in Fig. 6. The peer network model (less used) allows the LAN or user to directly control core nodes within the network. The more common architecture is for the network provider to utilize a user network interface (UNI) model where the UNI edge node only processes information provided by the user at the entrance (ingress) to the network as well as information in the packet or frame that specifies the final destination. The UNI is then responsible for coordinating all requests from the LAN or access network with communications and routing with other core nodes and other resources (e.g. servers) in the network via a network node interface (NNI). In essence, the UNI acts to discover and communicate with the LAN or access network and hides the details of the network from the LAN or access or user. Such a model is preferred for scaling, security, network stability and other reasons.

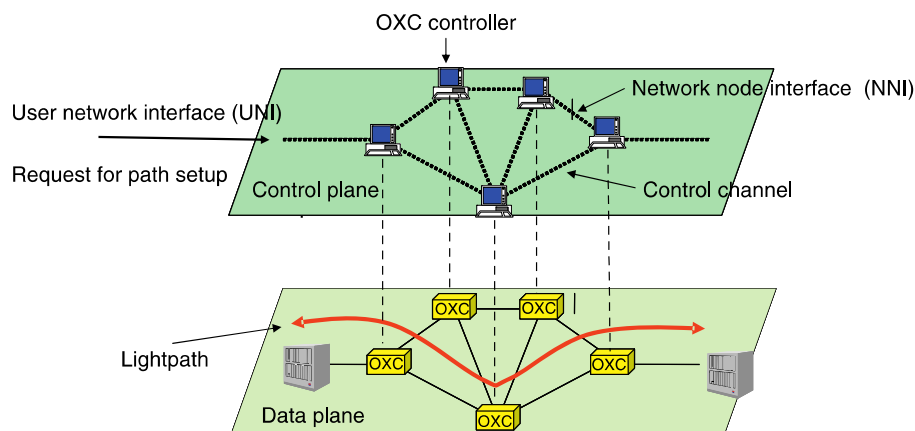


Figure 6. Kaminow, Li, Willner (2008). Ex. 1017.

B. Layered model and Protocol Stacks

[049] Packet data network scaling and automation have been around since the early days of DECNET in 1975, one of the first packet based peer-to-peer network architectures. DECNET was a layered network communication and protocol model with a 3-layer Dec-NET protocol model and evolving to the 7-layer OSI networking protocol layered model used today. The idea of a layered network model is to break down the functions of a network, from the application down to the physical transport (e.g. fiber, wire, wireless), into individual layers that serve functions of an overall network in a way that each layer can be implemented, modified and optimized (e.g. performance and cost), independently of the other layers, as long as the interaction between it and neighboring layers (above and below) do not change. The OSI reference model, shown in the lower left of Fig. 7, involves all the steps required to run an application (the Application Layer at the top) all the way to the underlying Physical Layer that carries data (e.g., wireless,

coaxial, twisted pair, optical fiber). IP/Ethernet primarily sits at the lower two layers, the Data Link and Physical layers. As illustrated in Fig. 5 the data link Ethernet layer performs functions that support the Network Layer above it. These functions include the link logic control (LLC) and media access control (MAC) as well as interfaces between the link layer and the underlying physical layer, which can include Gigabit ethernet (1000 Mbps) and passive optical networks (PON) for example. As shown in Fig.7, the physical layer is designed so that any type of transmission “medium” and data rate can be supported, for example coaxial cable, wireless, fiber optic, 10 Mbps and 10 Gigabit Ethernet, and each physical layer supports the requirements of the data link layer above it.

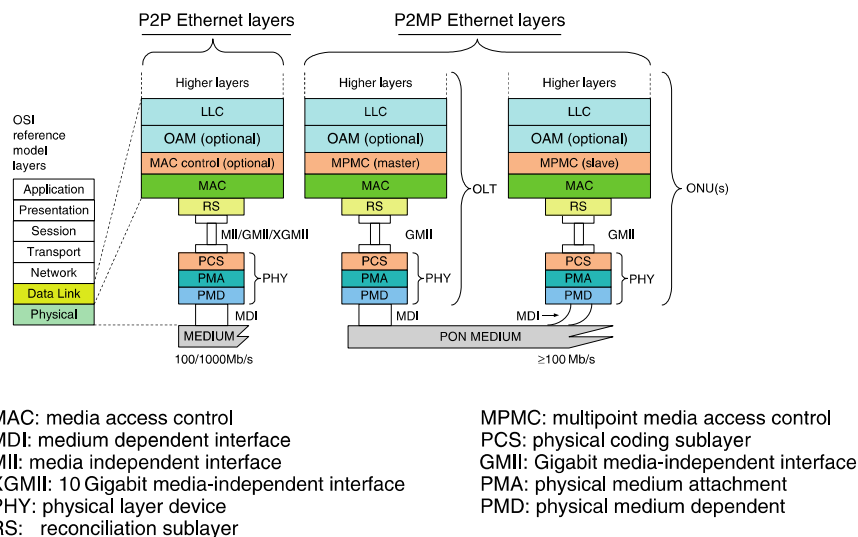


Figure 7. Kaminow, Li, Willner (2008). Ex. 1017.

[050] In the early 2000s, network builders and service providers were building networks from an assortment of technologies that had evolved, including packet technology like IP data and internet services, asynchronous transfer mode

(ATM), fiber optic transport technology like synchronous optical network (SONET), and optical fiber and wavelength division multiplexing (WDM). In order to accommodate the wide variety of technologies that had to be supported on these evolving networks, broadband networks were built on multiple layers as illustrated in Fig. 8.

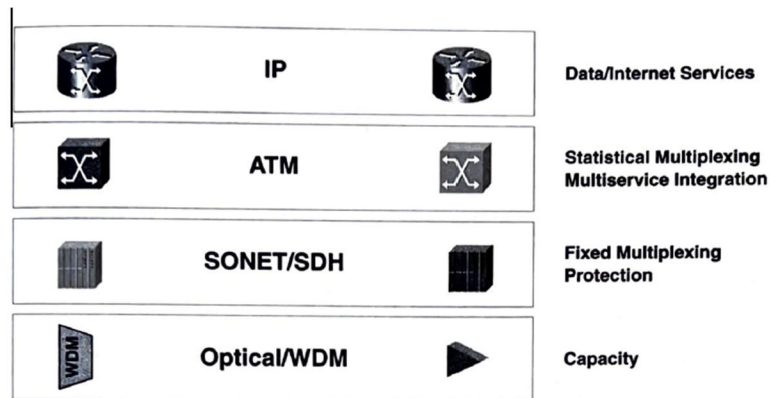


Figure 1-1 The traditional network architecture consists of multiple layers

Figure 8. Tomsu and Schumutzer (2002). Ex. 1016 at 3.

[051] As can be seen in Fig. 9, the telecommunications operators (Telcos) in the early 2000s, deployed a mixture of many different packet and transport technologies, to enable low cost IP interfaces (IP layer) at the customer for voice, video and data, connecting to and integrating through the layered interface model. Examples include DS0/1 (traditional voice multiplexing), PPP (point to point protocols), ATM, xDSL, SONET rings, and xPON based networks using a range of physical layer technologies including optical fiber and copper, all connected to a common local central office that managed users, connections, services, billing, and

all functions needed to deploy, bring online, maintain and upgrade users and network facilities.

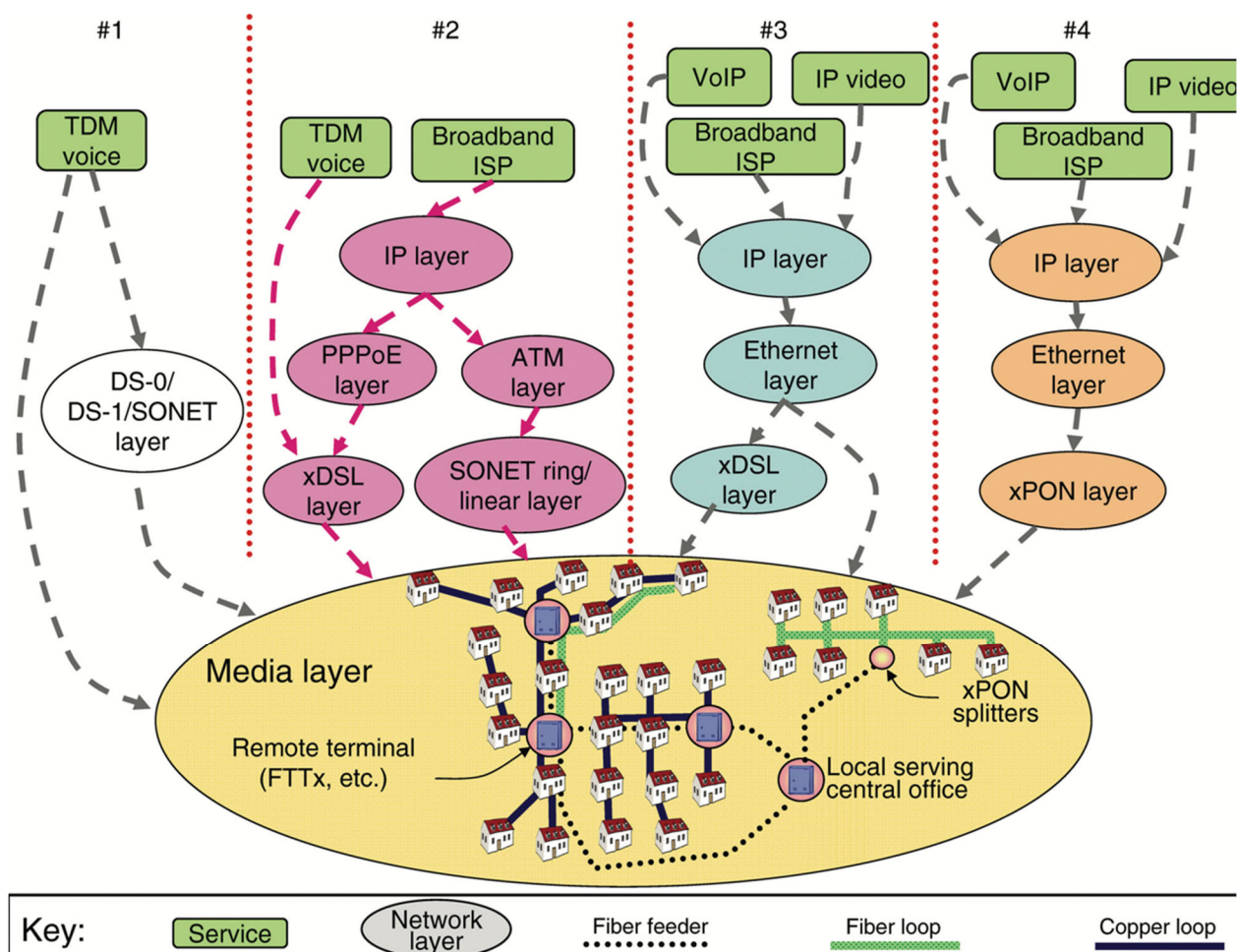


Figure 9. Kaminow, Li, Willner (2008). Ex. 1017.

C. Packet switches and Routers

[052] Packet switches and routers are the workhorse of today's internet protocol (IP) based networks and have been around since the 1980s. In general a packet switch is used to connect devices in a network that communicate with packets and a router is used to connect packet based networks. In terms of the

layered network model, packet switches operate at the OSI layer-2, or the Data Link Layer, and routers operate on data all the way up to the OSI layer-3. Switches are efficient for use within a LAN and routers are used to connect LANs, and in MANs and WANs, although routers may be deployed anywhere in the hierarchy. A packet switch is also essentially used inside a router and a switch.

[053] Switches and routers are organized according to where they sit in the network, the number of connections, the aggregate switch capacity, and functionality. For example, Fig. 8 illustrates a typical network architecture that may have been designed and deployed in 2000. Campus networks and enterprise WANs would have users connected to each other by an ethernet packet switch and a switch would act as a gateway to the internet core. WANs would service many LANs and broadband edge customers that are packetized as shown by example in Fig. 7. The aggregate data that leaves each WAN would be connected to the internet core using an edge router, and data inside the core would be routed using carrier class core routers, ATM switches, and frame relay switches. The edge routers would prepare packetized data for switching inside the core and to follow a pre-planned core routes based on routing tables that are populated using traffic engineering algorithms. The placement of new edge and core routers as the network grows was enabled by auto-discovery algorithms that would automatically detect the neighboring router and switch nodes including their port and associated

MAC addresses, and propagate such information up to a network control plane, and using a network element management system, calculate new route paths and update routing information in tables located in all the routers and switches. The standards for this topology discovery and communications channels to transmit the information as well as the management protocols, were handled by standards organizations such as the IETF, the OIF, and the IEEE.

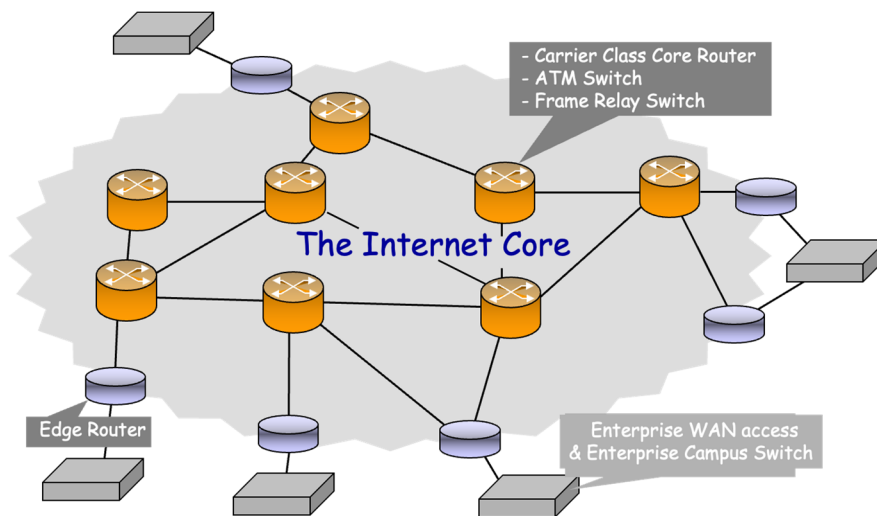
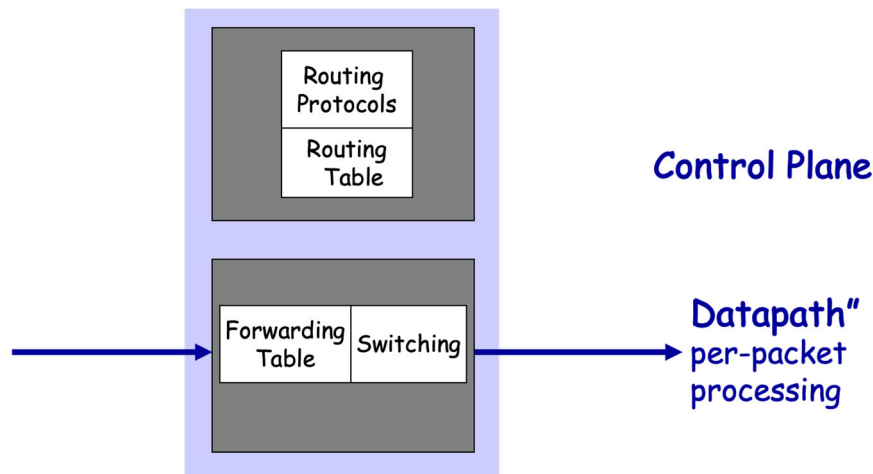


Figure 8. "An Introduction to Packet Switching," N. McKeown (2000).

Ex. 1015 at 7.

[054] The basic components of an IP packet router are shown in Fig. 9. The switch is functionally divided into two planes - the control plane and the datapath plane. The datapath plane is where the actual packets are handled, including the switch input port (e.g., from a fiber or coax) at a switch port, analyzing the information in the packets or packet headers, storing and processing of packets, and physical switching of the packets required output port and if

needed, updating of the header or other packet contents. The control plane is where information about the network is stored, transmitted, and manipulated, including topology of which switches and ports are connected to other switches and ports and where they are physically located, which wires, fibers or wavelengths the ports are connected to, all possible edge router connections that can serve as core network inputs and output for the core and Ethernet connections for the LAN or user, and computation of all routes that a packet can take from its source to its destination. This traffic engineering utilizes information about how routers are connected and where they are located, information gathered during a discovery process, and other information needed to compute paths from any source to any destination. The resulting calculated paths are then distributed to all of the edge and core routers via the control plane and stored in switch routing tables.



[055] Figure 9. “A quick tutorial on IP Router design,” N. McKeown,
Optics and Routing Seminar, 2000.

[056] The packet switch operates on a packet by packet basis, analyzing information stored in each packet related to where it wants to go to, and the path through the switch, from switch input port to switch output port, that the packet needs to take. For ATM cell switching, the packet switch is always reading, switching, and updating cells of the same size, and does so asynchronously where all ATM cells entering ports asynchronously are buffered and aligned to a new internal starting time defined locally within the switch. The switch then forwards all packets through in one cell cycle using the routing table and cell header information to make these decisions. Packets can also be stored in switch output buffers in order to coordinate packets that need to go to the same physical output port at the same time (input buffering can be used also as well as large shared buffers or combinations of all three). The output buffering process is also referred to as scheduling. The control plane is responsible for making reservations and coordinating traffic based on requirements for the broadband service that a packet is carrying information for, through e.g. forwarding tables that the inputs use to make the switching (forwarding) decisions. For example voice cells/packets would be routed high priority since drops in voice will be noticed. Data can be held up in buffers as long as the applications are not negatively impacted and data can be retransmitted if lost or dropped, and video can afford to lose some packets instead of storing since a dropped pixel or other video coding algorithm usually suffices.

In the case of IP packet routing (as opposed to ATM), where the packets are variable length, a switch or router is constructed that can handle variable length packets at its inputs, within the buffers and memory, and withing the switching. Typically the incoming variable length packets are artificially broken up into routing cells, that are optimized in length by the switch designer, and such internal cells are reconstructed at the switch output to transmit the IP packets with modified headers.

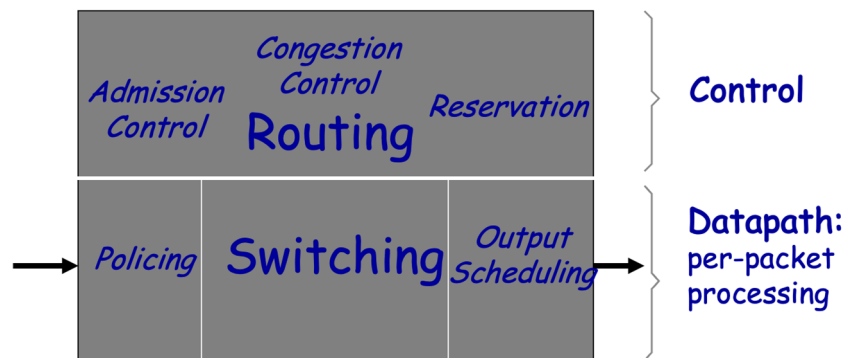


Figure 9. “An Introduction to Packet Switching,” N. McKeown (2000)

[057] The processes involved in packet switching and packet routers are predominantly routing, forwarding, scheduling and buffering, as defined below:

- a. **Routing:** The process of determining a path from source to destination for a packet of data. This is typically implemented by a *route processor*. *Routing tables* contain the information necessary to decode a header and decide based on the address contained within the header to which output port to send a packet.
- b. **Forwarding:** The process of sending a packet from an input to an output within a switch. This is done by performing a lookup in a *forwarding table* to decide how to make the necessary connection between the input and output in order to forward the packet. A *forwarding engine* carries out the process of forwarding packets,

including looking up the forwarding table and setting the switch connections within the switch fabric.

- c. **Scheduling:** A *scheduler* handles the selection of, for each outgoing link of a switch (or router), the packet to be transmitted in the next cycle from contending packets belonging to the flows that share the same output link.
- d. **Buffering:** A means to hold packets that cannot be forwarded via required resources such as

[058] An example router/switch architecture is shown in Fig. 10 with the forwarding, interconnect, and output scheduling stages shown. Multiple input interfaces, connect to e.g., a fiber network (1) handle per packet forwarding based on routing information (e.g., which output port should a packet be switched to). The packets are switched through an interconnect (2) that provides reconfigurable connections between input interfaces and output scheduling (3). The output scheduling with its buffers are able to accept multiple packets at a time from the interconnect, and in the case of output port packet collisions (where multiple packets need to go to the same output port at the same time), the interconnect sends the packets to multiple buffers located at each output port. The output scheduling then moves packets one at a time from the output port buffers to the transmission buffer fort that then transmits the packets.

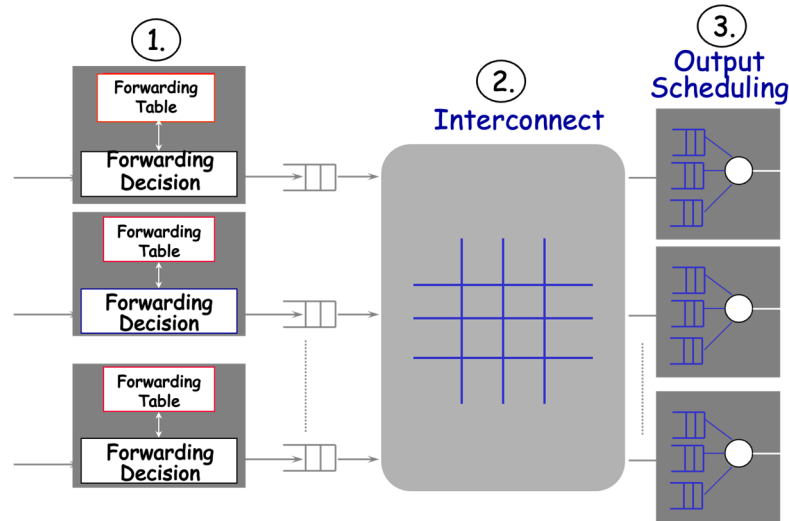


Figure 10. “An Introduction to Packet Switching,” N. McKeown (2000)

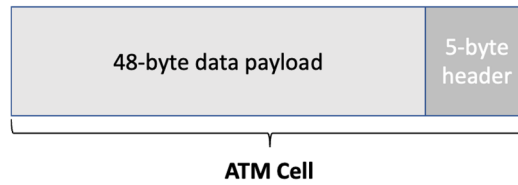
D. Packet and Frame Technologies

[059] Multiple techniques have been introduced into commercial networks since the 1980s to provide a way for many users to efficiently share the communications medium using packet or frame based communications. These techniques were also developed to allow the network to carry different types of traffic (e.g. video, voice, data), and scale the number of users, nodes, bandwidth and capacity, and distance/reach. The OSI layered model provides a way to create virtual circuits or tunnels, out of a packet or frame switched network, that look like dedicated connection to the user. This creation of virtual connections is a layer on top of the sharing of the network using a packet or frame switched technology and is essentially hidden from the user or higher application layer. The integrated services digital network (ISDN) and broadband integrated services digital network

(B-ISDN) standards of the early 1990s were developed to handle the virtual sharing of network bandwidth to home and business users. The installed and legacy telephone circuit switches (that made dedicated connections when a call was made) were modified by installing B-ISDN equipment on the input and output of the circuit switch to artificially setup and takedown the circuits rapidly so that users were sharing the switch resources, but the higher B-ISDN layers made that process hidden. The early B-ISDN technology was expensive to install and operate. Truly packet and frame switched technologies, asynchronous transfer mode (ATM) and Frame Relay, were developed in the 1980s, to provide switching at the hardware layer that could deliver shared network resources with broadband performance. The B-ISDN networks made heavy use of ATM transport and switching technology to provide fast switching and low latency needed for broadband. These technologies were installed in LANs and the core networks, but were also too expensive for the LAN users, since they were required to install an ATM interface at every computer or node as well as an ATM interface at every local gateway switch port. The push to integrate a packet interface for the user, directly in the computer, became more economical for Ethernet, and users eventually migrated to low-cost Ethernet interfaces. At first, in the early to mid- 1990s, the traffic generated by ethernet interfaces communicated over a campus or LAN networks that were built using ATM, frame relay technology, or fiber-based FDDI ring

network technology. LAN could be FDDI, Ethernet switched, Ethernet to ATM or Frame Relay interfaces were required at the network edge and core routers and transport technologies like synchronous optical networking (SONET) were required to have interfaces for all the standards. Eventually the broadband network was migrated to a uniform IP/Ethernet network, and Ethernet became the world-wide packet switching standard. Today, there still exists many legacy networks in the installed infrastructure and interface technologies are still commonly used.

[060] **Asynchronous Transfer Mode (ATM)** is a packet based communications network and set of standards, where all data, voice, and video are coded into fixed-size packets that are 53 Bytes long (shown in the figure below), with 48 Bytes utilized for the data, and a 5-byte header that contains the necessary information to route the packet from a source to destination over a virtual path or circuit that is configured through the network when a connection is setup. The 5-byte header contained information about the mode of transmission (e.g., electrical, fiber, wireless), information needed to establish a virtual path through the network from source to destination, information about what type of data is in the payload (e.g., voice, video, data) and how can the packet be handled based on the application requirements. Other information in the header includes a virtual circuit identifier, priority, and error checking.



[061] There are two types of header formats used in ATM cells. The first is the user network interface (UNI) where headers in cells coming from users or other equipment connected to the edge of an ATM network contain the necessary, source and identification, data type, and other information need to request a connection, but do not have information about the inside of the network in the header, nor information to directly control the ATM switches inside the network. The NNI format is used by core network switches communicating with other cell switches. ATM switches communicate with each other during the routing and transmission process to discover the physical topology, and via a signaling protocol the virtual paths that can be set up with available resources and which resources are to be assigned and used for a virtual path.

[062] **Frame Relay** was first proposed in 1984 and deployed in the early 1990s. It was developed to provide operation between different networking environments. Early frame relay provided efficient data transmission between local area networks (LANs) and between endpoints in wide-area networks (WANs). The frame is the basic unit that could be variable in size and could contain different types of data including packets and were used to create virtual circuits for the

customer at a lower cost than a dedicated circuit. The service provider was responsible for assigning the frame routing. Frame relay utilized a local management interface (LMI) signaling standard between switches and provided auto-configuration information of customer edge (CE) devices.

[063] **Ethernet** was developed at Xerox between 1973 and 1974 and Xerox, Digital Equipment Corporation (DEC), and Intel worked to establish the Ethernet standard published in 1980.

[064] Ethernet is transmitted in the OSI data link layer in units called Ethernet frames over an Ethernet compatible physical layer. Ethernet frames can be variable in length and contain user data that is anywhere from 46 bytes to 1500 bytes long. There are multiple Ethernet standards (the most popular is IEEE 802.3), but they share basic attributes. Ethernet frames are transmitted at the data link layer (Layer 2) over one of any compatible physical layers (Layer 1) that sit under the data link layer. L1 can be any transmission type (e.g., fiber, wire, wifi, etc.). The data from users can be from up to 1500 bytes and other network-based data, such as acknowledgement packets, are 46 bytes.

[065] An Ethernet network adapter at the user or source prepares the data in a frame for L2 packet transmission. The data is assembled into a frame with 6 bytes for the destination MAC address, 6 bytes for the source MAC address, and a two byte frame type. After the user data, the frame contains a 4 byte FRC (for error

checking and reliable data transmission). At the head of the packet 8 bytes are used for a preamble sequence (for clock and data recovery) an SFD which is a unique bit sequence in the packet that marks the start of the frame. There is a built in inter-frame gap at the end of the packet before the next packet transmission. The total frame is between 64 bytes and 1,518 bytes long as shown in Fig. 10.

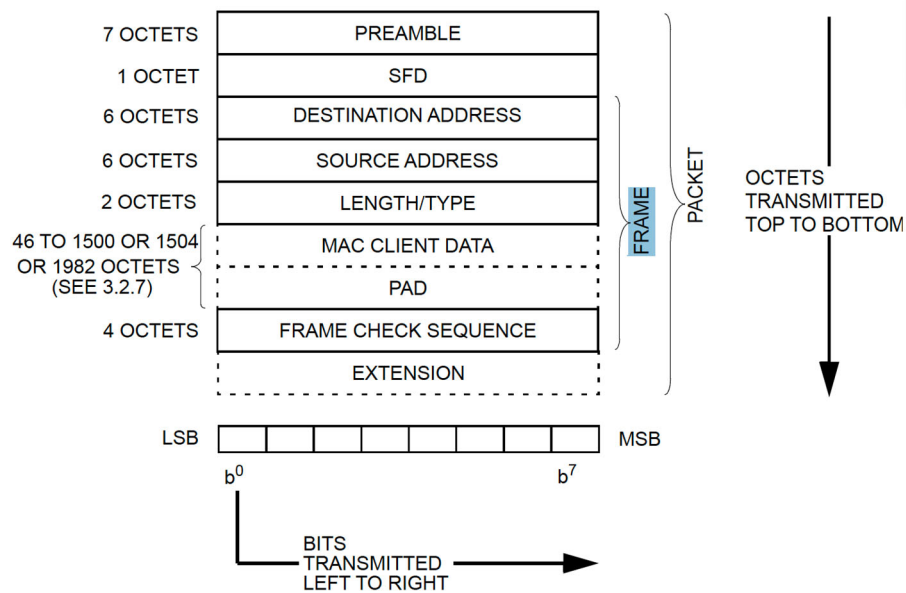


Figure 3-1—Packet format

Figure 10. IEEE Std 802.3TM-2018 (Revision of IEEE Std 802.3-2015)

[066] Network routing of Ethernet Frames (packets) occurs in the OSI Layer 3 (L3), and is called TCP/IP, which is the Internet Protocol in the TCP protocol suite. The IP L3 (Layer-3) is responsible for routing in LANs and WANs, error reporting, and handling datagrams for transmission over networks with different maximum data unit sizes.

E. Multiprotocol Label Switching (MPLS)

[067] Multiprotocol Label Switching (MPLS) was developed to simplify route lookup and separate the routing and forwarding functions in a packet switched network. MPLS can also be used to exchange or encapsulate packet header formats as packets traverse multiple types of networks with different protocols. Packet labels perform similar functions to a packet header and are appended to the head of each packet in addition to its original header (i.e., the original packet payload and header are maintained intact with a label added as a new header). As a labeled packet moves along its path from source to destination from one router to the next, the MPLS label is processed at each router, where locally stored lookup tables are used to choose a new label and next hop (i.e., local output port and link) for the packet. This label decision is made independently from other routers. The label lookup tables and other management and control information have been transported around the network control plane, using an appropriate protocol, to pre-decide all paths packets can take.

[068] Whereas IP and ATM packet networks require complete analysis of each packet header at each router node, MPLS only uses analysis of the header as the packet enters the gateway node to an MPLS network input, at a router called a label edge router (LER). At the LER, a label is added to the packet (in front of its original header without modifying the original header). At subsequent router hops

in the MPLS network only the label is recovered, and in conjunction with the input port number, is used to look up the next label and router output port for that packet in a table. Since the label was added to a packet at a specific LER, MPLS is able to handle packets differently based on where they entered the network, a unique feature of MPLS. At each MPLS core router, the old label is erased and the new label added to the packet (a process also called label swapping), then the newly labeled packet is sent to the specified output port for forwarding to the next hop. Labels are computed and distributed to all node in an MPLS network based on all network inputs and outputs, the router ports, the network physical topology, and other connection related information. In this manner, a packet is routed from an MPLS network ingress node to an MPLS network egress node using the distributed routing tables, label switching, and traffic engineering methods.

F. Network Discovery and Internet Border Gateway Protocol BGP/IP and Open Path Shortest First (OSPF)

[069] The function of network discovery allows nodes (e.g., routers, switches) to figure out which other nodes they are connected to, with which input and output ports, which links, and other attributes of the ports and connections. IP networks and the internet constantly have devices, computers, nodes, and networks added and taken down. Mechanisms must be in place to keep track of all changes in order to enable routing protocols and tables to operate on up to date topology information for packet routing. In this manner the topology of the network can be

discovered, updated as nodes and links are added or removed, and this information is then distributed around to the nodes. This function is automated in part by enabling transmission of information about topology among the nodes using specifically designed protocols.

[070] All computers and devices connected to the internet are connected to an autonomous system, which is a collection of interconnected IP routers that have a unified routing policy. Interconnected autonomous systems make up the internet, and packets will traverse these autonomous systems from the source until they reach the autonomous system that contains the desired final computer or device (destination). Topology discovery in an autonomous system is supported in part by the Border Gateway Protocol (BGP) and Open Path Shortest First (OSPF) routing protocols that are part of the internet protocol (IP) family.

[071] OSPF is a protocol used primarily in a single autonomous system such as a LAN or enterprise network, to enable routers within an autonomous system to create their own routing tables that are used in the packet forwarding process. The routing tables are built with topology and other information like transmission interfaces, the cost of using each interface, and reachable neighbors. This information is exchanged between nearest neighbors (routers) and propagated throughout the network so that every router has complete information of the autonomous system (network). Each router is able to build its own local routing

table from the information distributed by OSPF according to some cost criteria like shortest path. When the network topology changes, e.g. a new device or router is added, the information is propagated and routing tables are updated.

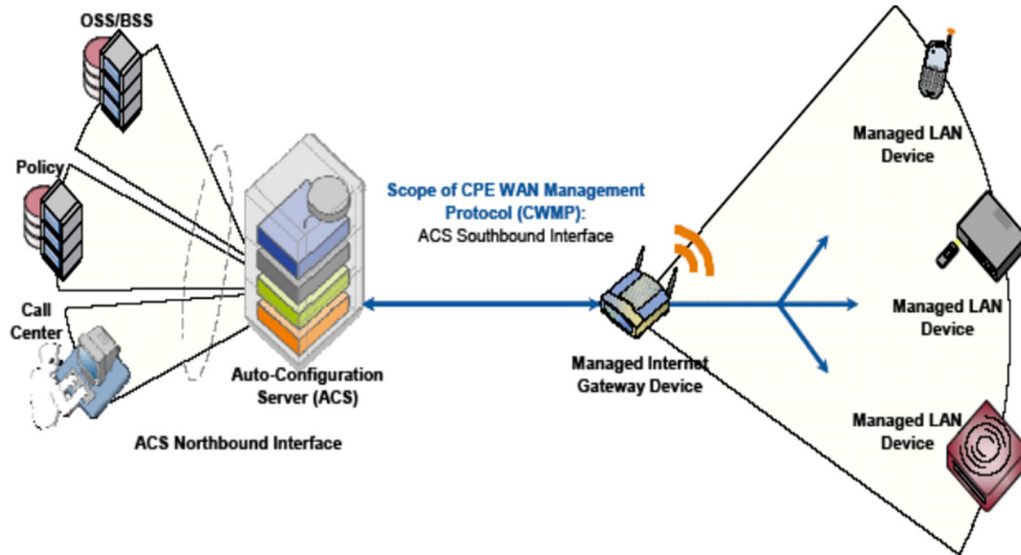
[072] BGP is the scalable protocol used for the larger wide area networks (WANs) and the internet. BGP is a standard of the Internet Engineering Task Force (IETF) (see for example: A Border Gateway Protocol 4 (BGP-4), January 2006, <https://www.rfc-editor.org/rfc/rfc4271>). BGB has two variations, internal BGB (iBGB) which is utilized for routing and topology discovery between routers and switches within an autonomous system, and external BGB (eBGB) which is utilized for routing and topology discovery between autonomous systems.

G. TR-069 CPE WAN Management Protocol (CWMP)

[073] The secure auto-configuration of customer premise equipment (CPE) in LANs and wide area networks (WANs) is critical to the scaling and managing of customer based IP networks. The CPE WAN Management Protocol (“CWMP”) is a protocol that was developed for communication between a CPE and Auto-Configuration Server (ACS). An ACS is used for remote management of CPEs.

[074] CWMP covers secure auto-configuration as well as other CPE management functions and enables remote and safe configuration of network devices that a customer wishes to connect. TR-069 is the document number of a

technical report for the CWMP defined by the Broadband Forum. The TR-069 architecture is reproduced in the figure below:



[075] It was well known before the claimed invention that the consumer home and business markets were projected to support ever increasing number of electronic devices equipped with Internet connect capabilities over time. Such devices are commonly called ‘customer premise equipment’ (CPE) that are linked together to form a home or business local area network (LAN) and each computer or device has its own unique MAC addresses that is assigned at the time of manufacture. The LAN, consisting of a network of CPEs is then connected to a wide area network (WAN) through a LAN gateway, a link to the WAN, and the WAN itself connects to servers such as video servers and auto-configuration servers (ACS).

[076] Provisioning of a CPE with the network is a key part of the installation process required to integrate the CPE with the network and its services. Customer provisioning of a CPE can be a difficult task and pre-provisioning by the network or service operator can require significant resources and limit the ability for the operator to grow the network in terms of number of users and number of devices and computers. Auto-provisioning solutions for CPE and network equipment have been around for a long time.

[077] One approach to auto-provision a CPE is to provide the CPE with the URL of the ACS. Connecting to the URL then allows the configuration file to be provided. For example, as explained in U.S. Application No. 2009/0292794, the CPE sends a request for configuration information to a DHCP server and that request identifies the CPE to the DHCP server. In the first step of this process “the Customer Premises Equipment (CPE), such as the home gateway, [are able] to send a Dynamic Host Configuration Protocol (DHCP) request message that carries the device identifier in a DHCP option to [a] DHCP server of an operator.” In the next step of this process, the DHCP server looks up the ACS, which is going to provide the configuration information, using a look-up table that maps the CPE’s identity to the relevant ACS - “DHCP server finds the URL of the Automatic Configuration Server (ACS) of the CPE according to the device identifier...” Finally, the DHCP server responds to the CPE with the ACS URL. - “The CPE

accesses the ACS according to the URL of the ACS to obtain the corresponding configuration file. Then the CPE is configured automatically according to the configuration file.”

[078] This technique described is also described in Fig. 4 of the '772 patent where the CPE sends a request (M1) for configuration information to a server (25) and that request identifies the CPE to the server (see Ex. 1001 at 7:14-26). Next, the server finds the URL of ACS1 according to CEP's device identifier and replies to the CPE with the ACS's URL (M2) (Ex. 1001 at 7:32-36). Next, the CPE accesses the ACS (M3) according to the URL of the ACS to obtain the corresponding configuration file (M4) (Ex. 1001 at 7:37-47). Then the CPE is configured automatically according to the configuration file (Ex. 1001 at 7:47-50) .

Figure 4

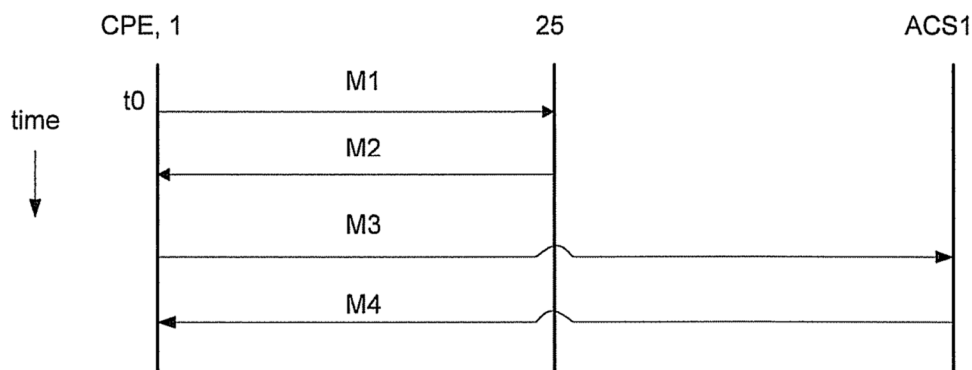


Figure 4 Ex. 1001

[079] Another prior art document (Ex. 1008) discloses that CPE devices are each given the same operation image produced as they are manufactured (see Ex. 1008 at ¶2). This document describes how the CPE devices undergo a configuration procedure before they can be fully used by an end user. According to Ex. 1008 at ¶2, in the early 2000s the configuration methods were “classified as either (a) sending a trained technician to customer sites to do the manual configuration for each customer device” or “(b) shipping a detailed configuration manual with each broadband-based customer device and asking the end user to perform the configuration by reading the User's Manual” (see Ex. 1008 at ¶3).

[080] Early innovations around improving the configuration process involved automatic configuration without any user intervention, e.g., plug and play (see Ex. 1008.) One early 2000's disclosure “completely eliminate[d] the need to do any manual configuration on the client side for broadband customer devices....” (Ex. 1008. ¶10), where the administrator uses an ACS to configure all of the connected consumer devices (ACC) (see Ex. 1008. Fig. 2) also shown as annotated below.

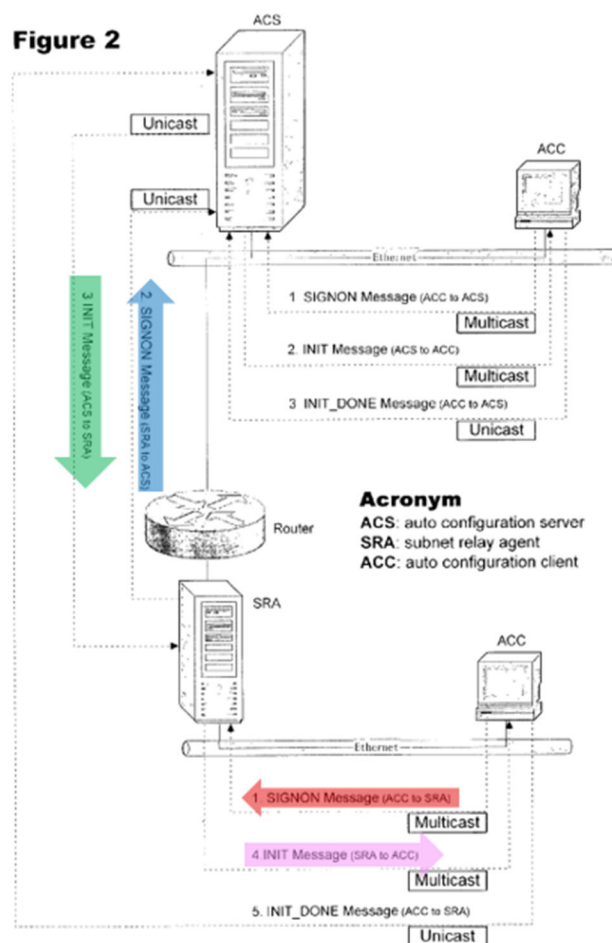


Figure 2 annotated (Ex. 1008

[081] As illustrated in (annotated) Ex. 1008 Fig. 2, when a consumer device (ACC) connects to the network it sends a message (red highlighted arrow) to a Relay Server (SRA) (see Ex. 1008 at ¶47). Next, the Relay Server relays that message (blue highlighted arrow) to an auto-configuration server (ACS) (Ex. 1008 ¶¶48-49). The ACS then replies to the Relay Server with a message (green highlighted arrow) carrying the configuration data from a configuration database (Ex. 1008 ¶¶51-52). Next, the Relay Server relays the message with configuration

data (purple highlighted arrow) to the consumer device (Ex. 1008 ¶53). Finally, the consumer device configures itself according to this information (Ex. 1008 ¶54).

[082] Note that this technique is a slight modification on that specified by other references, such as U.S. Application No. 2009/0292794. In this approach, the SRA (analogous to a DHCP server) receives the CPE's configuration request, identifies the relevant ACS and then *relays* the request to the ACS. The ACS replies to the SRA, which then relays the configuration information to the CPE, which is then configured automatically.

[083] In conclusion, the techniques described in the prior art and background material above can be used to specify the auto configuration of a CPE to an ACS via a LAN gateway. The connection of the LAN to a WAN through a gateway such as an LER, in combination with connection and configuration with other nodes and topology discovery protocols such as BGB, enables the location of multiple ACSs connected in the WAN. The auto provisioning techniques, protocols, network architecture hierarchy, and layered protocol model, can yield the same result as the '722 patent.

VII. OVERVIEW OF THE '772 PATENT

[084] The '772 patent describes a drawback with known configuration technology—it requires each CPE to be pre-configured with the address for the

proper ACS. (Ex. 1001 at 1:46-53.) However, as discussed above that is not true for all known configuration technology.

[085] In contrast, the '772 patent discusses two earlier techniques for providing the CPE with the appropriate ACS contact information. First, the CPE is “pre-programmed” with either a specific IP address or a specific URL for the ACS. (see Ex. 1001 at 1:53-56). Second, the CPE is configured with the ACS’s address or URL during installation (Ex. 1001 at 1:56-60). Ex. 1008 also teaches in paragraph 10 to “eliminate the need to do any manual configuration on the client side for broadband-based customer devices” by using a Relay Server to relay messages and replies between the CPE and the ACS.

[086] The '772 patent provides a management device between the ACS and CPE to facilitate communication between the ACS and CPE. The purpose is to overcome the “pre-configuration” problem where the CPE must know the ACS’s address or URL beforehand. The '772 patent calls this management device the “auto-configuration server managing device” (“ACSMD”), see abstract of Ex. 1001.

[087] The '772 patent claims to improve prior art systems by allowing the configuration of “any type of manageable electronic device ... without pre-configuring a dedicated address for configuration.” (Ex. 1001 at 2:22–25) using the ACSMD.

[088] Referring to Fig. 2 of the '772 patent, an ACSMD (25) is shown between the CPE (1 to 4) and ACS1, ACS2, and ACS3.

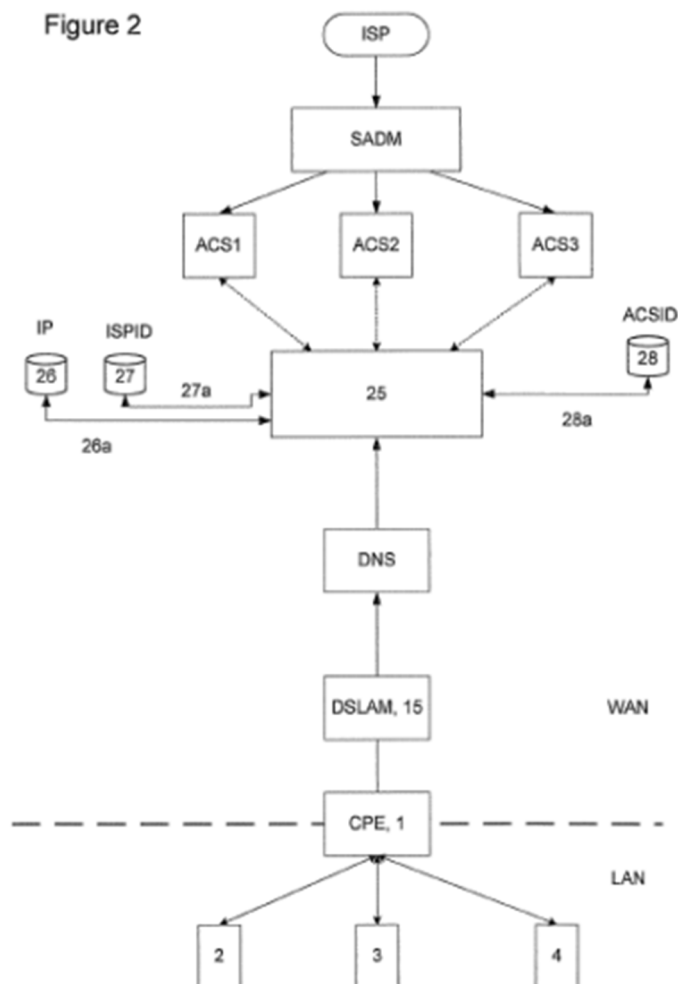


Figure 2 '772 patent.

(Ex. 1001 at Fig. 2). As depicted in Figure 2 '772 patent, CPE 1 is communicatively coupled to the ACSMD 25. ACSMD 25, in turn, is arranged for controlling CPE 1's access to the ACSs, e.g., ACS1, ACS2, and ACS3 (Ex. 1001 at 5:8–10).

[089] As depicted in annotated Fig. 5 (see below), the CPE 1 sends a first message M1 (red) to the default IP address/URL provided in the CPE 1's memory. (Ex. 1001 at 7:53-63). This default IP address/URL points to the ACSMD 25 (Ex. 1001). The first message, M1, "comprises a request for configuration data from the dedicated auto-configuration server." (Ex. 1001 at 7:63-64). "Further the first message M1 comprises at least the IP address (or URL) of the [CPE 1] as identification on the wide area network, an identification of the type or function of the [CPE 1] and optionally additional identification, for example, the identity of the supplier/manufacturer of the device." (Ex. 1001 at 7:65-8:3).

Figure 5

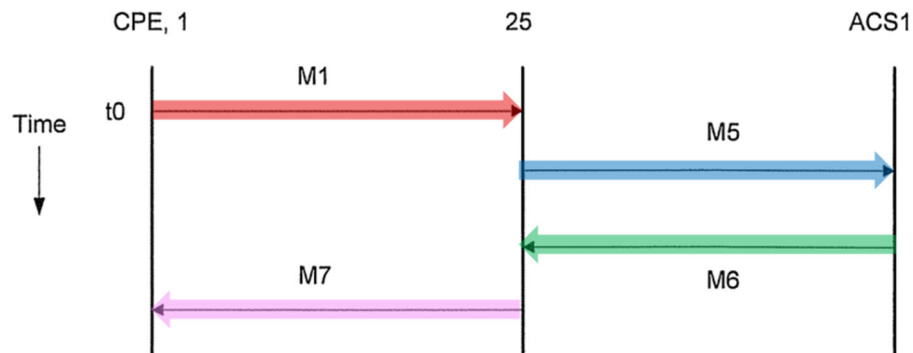


Figure 5 of the '772 patent (annotated).

The "first message M1 [red highlighted arrow] is received by the [ACSMD] 25," which carries out actions "to identify the dedicated auto-configuration server" and subsequently relays "a first relayed message M5 [blue highlighted arrow] to the

dedicated auto-configuration server ... if the first message M1 contains a valid request.” (Ex. 1001 at 8:4-12). “The first relayed message M5 [blue highlighted arrow] comprises at least the request from the requesting manageable electronic device 1.” (Ex. 1001 at 8:12-14). “Next, the dedicated auto-configuration server ACS1 ... receives the first relayed message M5.” (Ex. 1001 at 8:20-21). “In response, the dedicated auto-configuration server ACS1 transmits a reply M6 [green highlighted arrow] to the first relayed message to the auto-configuration server manager 25.” (Ex. 1001 at 8:21-24.) “The reply M6 [green highlighted arrow] to the first relayed message M5 comprises the configuration data requested by the manageable electronic device,” and the ACSMD 25 “receives the reply” and “relays that reply M6 to [CPE] 1 as a second relayed message M7 [pink highlighted arrow].” (Ex. 1001 at 8:25-31). “The second relayed message M7 [pink highlighted arrow] comprises the configuration data requested by the manageable electronic device.” (Ex. 1001 at 8:32-33).

[090] The '772 patent describes the communication flow in Fig. 5 as advantageously allowing any CPE to be configured “without pre-configuring a dedicated address for configuration” because the “addresses of the auto-configuration servers only need to be maintained in a central database.” (Ex. 1001 at 2:22-32).

[091] I have been made aware that during prosecution, Patent Owner overcame prior art by arguing that “relaying” a message is different from “forwarding” a message. (Ex. 1004 at 21-62, 85-87). But, in the following claim construction briefing against Xaiomi, Patent Owner has clarified that “relay” means “send.”

¹⁰ To the extent it construes the term, the Court should at most construe “relay” to mean “send.”

52

(see Ex. 1009 at 52 fn. 10).

[092] I have also been made aware that Patent Owner has stated that the issue is “no more complicated than ... the message is passed from one device to another....” (Ex. 1009 at 55 (emphasis added).) In my opinion, as detailed below and in my technical background section, the sending/passing/relaying of a message or reply is not innovative.

[093] I have also been made aware that the Patent Owner previously canceled independent claims 1, 10, 12, and 15 and that the Patent Owner also canceled dependent claims 7-9, and 13. Claim 2 is exemplary of claims 11, 14 and 16, and recites:

Claim Elements	Mapping to the specification ²
1. A system for remote device management comprising:	Fig. 2.
a plurality of auto-configuration servers (ACSs);	Green boxes.

² I am informed that written description, indefiniteness, and enablement defenses are not available during IPR. Therefore, I have formed no opinions about these issues. The mapping provided in this table is not a concession that the claims have written description support, are enabled, or definite. Instead, the mapping is to help provide the reader with an understanding of where the closest possible disclosures are in the specification for the claimed elements.

a manageable electronic device;	One of the red boxes
an auto configuration server managing device (ACSMD) for controlling access to the ACSs communicatively coupled intermediately between the plurality of ACSs and the managed electronic device; and	Purple box.
at least one database communicatively coupled to	Orange box

the ACSM and storing information for the identification of electronic devices,	Figure 2
wherein the manageable electronic device is configured to send a request for configuration data to the ACSMD,³	Red arrow in Fig. 2 and Fig. 5.
wherein configuration data comprise data for configuring the manageable electronic device, and	Ex. 1001 at 4:30-35 (“Configuration data for the auto-configuration server ACS1 or ACS2 is delivered from some provisioning systems (P1, P2, P3: P4, P5, P6), which may relate to equipment

³ This request is “M1” in Fig. 5.

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

	specific, service level specific and/or customer specific configuration data.”)
wherein the ACSMD is configured, responsive to receiving the request, to: identify the manageable electronic device by comparing at least a portion of the request with the information for the identification of electronic devices of the at least one database, and identify an ACS from the plurality of ACSs in accordance with the identification of the manageable electronic device to provide configuration data to the manageable electronic device, and	Ex. 1001 at 6:10-15 (“In a second action 102, the auto-configuration server manager 25 compares the received IP address of the manageable electronic device with a first database 26 (or IP address database) that comprises IP address information on IP addresses that are valid for allowing access to (the service of) the auto configuration server manager 25.”) Ex. 1001 at 29-43 (“In action 104, the auto-configuration server manager 25 resolves (by information signal 27A) an identity of the service provider ISPID from the IP address by means of a second database 27 which comprises information that associates the identity of the service provider ISPID with the IP address of the manageable electronic device. In a next action 105, the auto-configuration server manager 25 resolves (by information signal 28A) an IP address ACSID of the dedicated auto-configuration server from at least one of the identity of the service provider ISPID and the received IP address of the manageable electronic device 1 by means of a third database 28 which comprises information that associates the IP address of the dedicated auto-configuration server with at least one of the identity of the service provider

	ISPID and the IP address of the manageable electronic device.”)
wherein the ACSMD is further configured to relay the request to the identified ACS. ⁴	Blue arrow in Fig. 2 and Fig. 5. Ex. 1001 at 6:65-7:3 (“the auto-configuration server manager 25 functions as an intermediate and relays the request from the requesting manageable electronic device 1 to the dedicated auto-configuration server as identified by ACSID, receives the reply from the dedicated auto-configuration server and transmits that reply to the manageable electronic device 1.”) Ex. 1001 at 8:5-14 (“The auto-configuration server manager 25 carries out the actions 101-105 of the method as described above to identify the dedicated auto-configuration server and subsequently the alternative action 106a, in which the auto configuration server manager 25 functions as an intermediate and relays a first relayed message M5 to the dedicated auto configuration server as identified by ACSID if the first message M1 contains a valid request. The first relayed message M5 comprises at least the request from the requesting manageable electronic device 1.”)

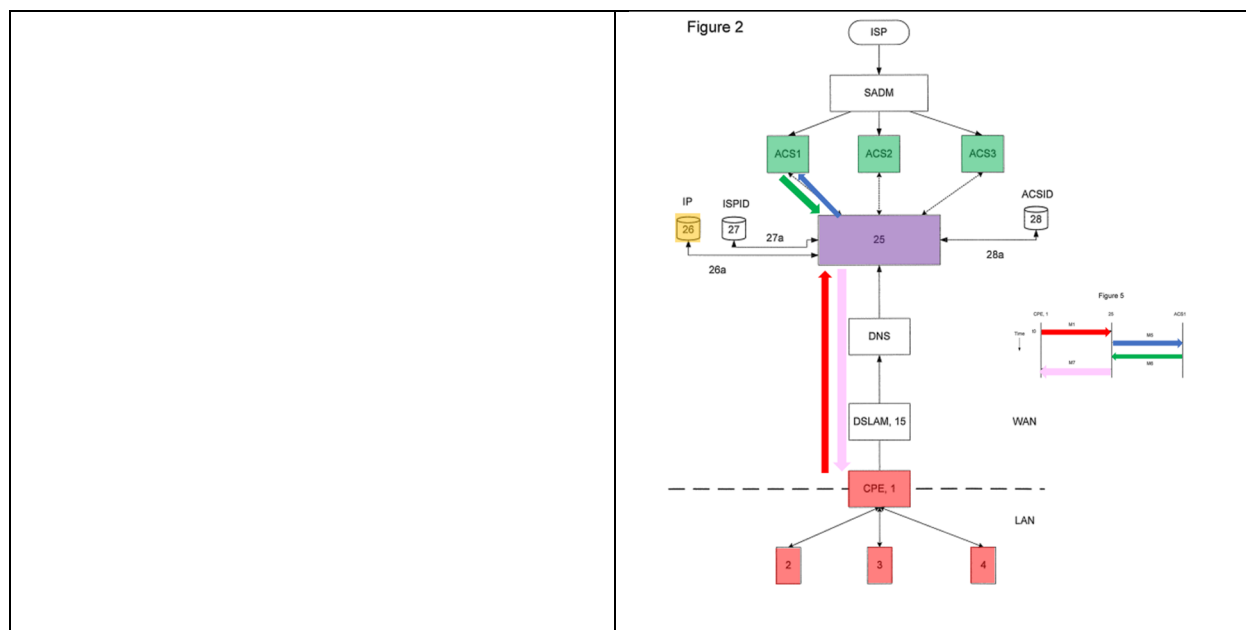
⁴ The relayed request is “M5” in Fig. 5.

	Figure 2
2. The system according to claim 1, wherein the ACSMD is further configured to receive a reply from the identified ACS,⁵ and	Green arrow in Fig. 2 and Fig. 5. Ex. 1001 at 8:20-31 (“Next, the dedicated auto-configuration server ACS1 identified by ACSID receives the first relayed message M5. In response, the dedicated auto-configuration server ACS1 transmits a reply M6 to the first relayed message to the auto configuration server manager 25. The reply M6 to the first relayed message M5 comprises the configuration data requested by the manageable electronic device. The auto-configuration server manager 25 receives the reply from the dedicated auto-configuration server ACS1 and relays that reply M6 to the manageable electronic device 1 as a second relayed message M7.”)

⁵ This reply is “M6” in Fig. 5.

	Figure 2
relay the reply to the manageable electronic device.⁶	Pink arrow in Fig. 2 and Fig. 5. Ex. 1001 at 8:28-37 (“The auto-configuration server manager 25 receives the reply from the dedicated auto-configuration server ACS1 and relays that reply M6 to the manageable electronic device 1 as a second relayed message M7. The second relayed message M7 comprises the configuration data requested by the manageable electronic device. The manageable electronic device receives the second relayed message and uses the configuration data within the second relayed message for any configuration purposes as described above.”)

⁶ This reply is “M7” in Fig. 5.



VIII. CLAIM CONSTRUCTION

[094] I understand that claim terms are typically given their ordinary and customary meaning, as would have been understood by a person of ordinary skill in the art, at the time of the alleged invention, which I was asked to assume to be the late 2008 time frame.

[095] I have reviewed the language of the claims in light of the specification and prosecution history of the '772 patent and have applied the ordinary and customary meaning of the terms in my analysis.

[096] I also understand that the claims of the '772 patent were previously construed by a judge in the Eastern District of Texas and that Patent Owner recently advocated for additional constructions in front of another judge in the District of Delaware, as summarized in **Table 1** below.

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

Term	Construction
Preamble	limiting (Ex. 1005 at 38)
“manageable electronic device”	“electronic device that can be configured over a network” (Ex. 1005, 42.)
“plurality of auto-configuration servers (ACSs)”	“two or more systems of hardware and/or software, each of which is capable of automatically configuring a manageable electronic device” (Ex. 1005 at 46.)
“auto-configuration server managing device (ACSMD)”	“hardware and/or software that relays configuration requests to the auto-configuration servers” (Ex. 1005, 48.)
“computer” and “processing unit”	“plain meaning” (Ex. 1005, 51.)
“controlling access”	“remaining in contact with the manageable electronic device and the ACS, and controlling whether the

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

	manageable electronic device gains access” (Ex. 1005, 54.)
“configuration data” and “configuration data comprises data for configuring the manageable electronic device”	“plain meaning” (Ex. 1005, 57.)
“request for configuration data” and “request from a manageable electronic device for configuration data”	“plain meaning” (Ex. 1005, 59.)
“relay” ⁷	“change, process, or otherwise manage a request based at least in part on its payload.” (Ex. 1005 at 61.) Patent Owner now contends that “relay” means “send” or “pass.” (Ex. 1009 at 52 fn 10, 55; <i>see also</i> Ex. 1009 at 13 (“the

⁷ KPN contends that “relay” means “send” or “pass.” (Ex. 1009, 52 fn 10, 55; *see also id.*, 13 (“the ACSMD enables information ... to pass between the ACSs and the manageable electronic device”).)

	ACSMD enables information ... to pass between the ACSs and the manageable electronic device”).)
--	---

Table 1

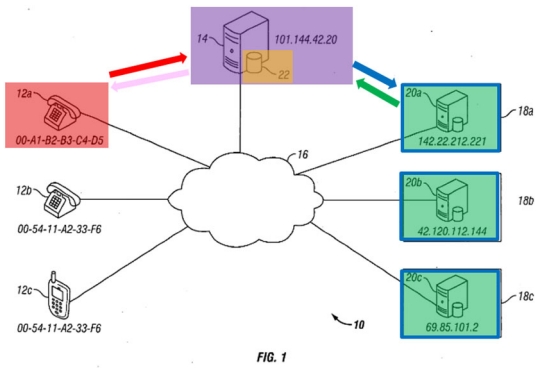
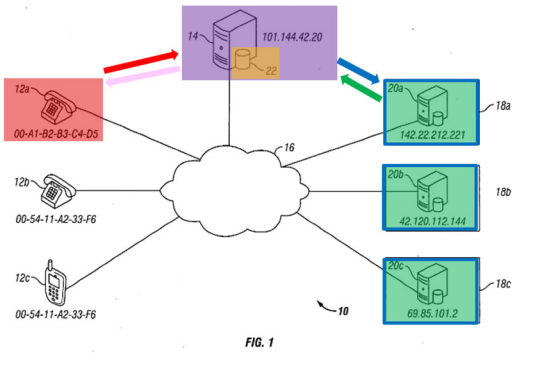
[097] Any reasonable construction is disclosed in the prior art.

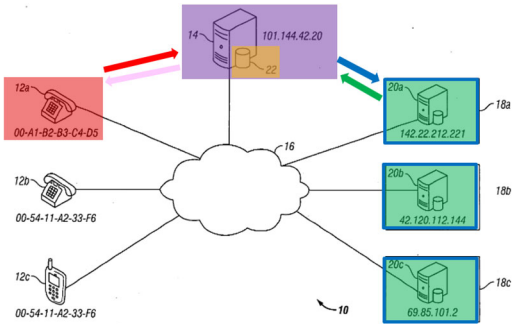
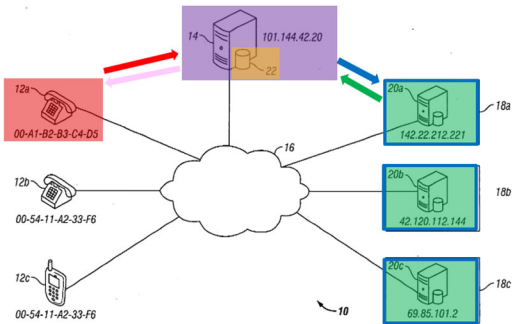
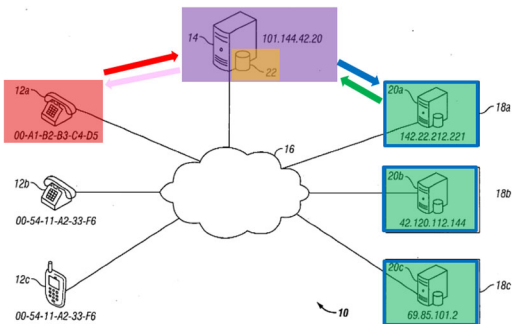
Nonetheless, out of an abundance of caution, Petitioner has asked me to analyze the claims under the plain meaning of the terms listed in the above table, under the district court constructions discussed in this Section, and under Patent Owner’s current understanding that “relay” means “send” or “pass.”

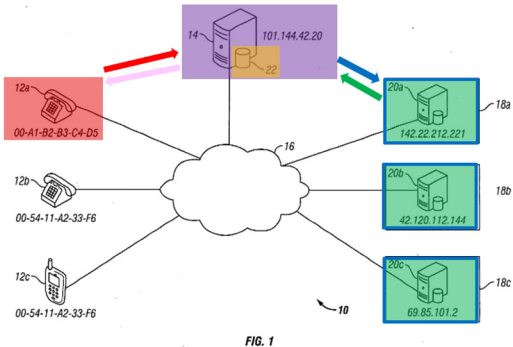
IX. DISCUSSION OF GROUNDS

A. Ground 1: *Angelot* Discloses or Suggests Each and Every Feature of Claims 2-6, 11, 14 and 16 alone or in view of the knowledge of a person having ordinary skill in the art.

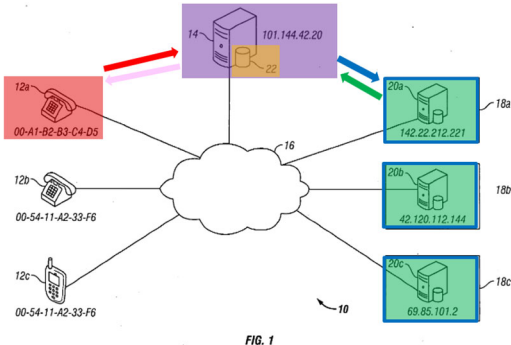
[098] As discussed below, it is my opinion that *Angelot* discloses or suggests all of the features of claims 2-6, 11, 14, and 16. For orientation purposes, I am providing a high-level mapping to exemplary claim 2. My analysis for each challenged claim follows.

Claim Elements	Mapping to the <i>Angelot</i>
1. A system for remote device management comprising:	Fig. 1.  FIG. 1
a plurality of auto-configuration servers (ACSs);	Green boxes.  FIG. 1

a manageable electronic device;	Red box  FIG. 1
an auto configuration server managing device (ACSM) for controlling access to the ACSs communicatively coupled intermediately between the plurality of ACSs and the managed electronic device; and	Purple box.  FIG. 1
at least one database communicatively coupled to the ACSM and storing information for the identification of electronic devices,	Orange box  FIG. 1

wherein the manageable electronic device is configured to send a request for configuration data to the ACSMD,⁸	Red arrow  FIG. 1
wherein configuration data comprise data for configuring the manageable electronic device, and	<i>Angelot</i> discloses a system 10 for “automatically configuring at least one network entity,” e.g., phone 12a (red), where the phone 12a is “associated with at least one service provider” 18a to 18c (blue outline box in annotated figure) having a “configuration server” 20a to 20c (green in annotated) that stores “configuration settings for the” phone 12a. (1006 at ¶¶11-15.)
wherein the ACSMD is configured, responsive to receiving the request, to: identify the manageable electronic device by comparing at least a portion of the request with the information for the identification of electronic devices of the at least one database, and	The central server 14 (purple) controls access to the various service providers 18 [blue] and their corresponding configuration server’s 20 [green]. (Ex. 1006 at ¶50.). “As part of the provisioning process the MAC address of the IP phone 12a,” i.e., the phone’s identity, “is associated with at least one of the service providers 18a, 18b, or 18c [blue], at the central server 14” in its

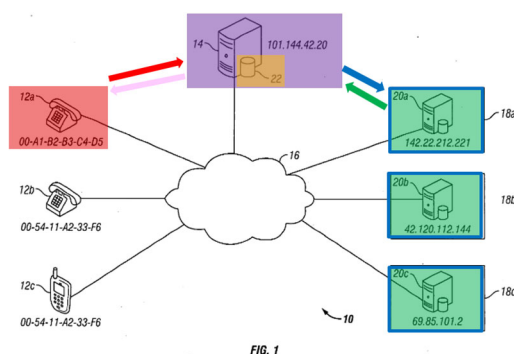
⁸ This request is “M1” in Fig. 5.

identify an ACS from the plurality of ACSs in accordance with the identification of the manageable electronic device to provide configuration data to the manageable electronic device, and	“database 22” (orange), which is “for storing the records of the MAC addresses and the associated service provider 18a, 18b, or 18c, such as a first mapping table which is maintained in a memory [orange] associated with the central server 14.” (Ex. 1006, ¶51.) “[A] configuration server 20a, 20b or 20c [green], <i>associated with the appropriate service provider</i> ... selects the configuration settings for the IP phone 12a [red] with that specific MAC address....” (Ex. 1006 at ¶54.)
wherein the ACSMD is further configured to relay the request to the identified ACS.⁹	Blue arrow  As <i>Angelot</i> explains, the “server [ACSMD] redirect[s] the request to an appropriate configuration server [green] having the configuration settings data specific to the identifier.” (Ex. 1006 at ¶19.) “[T]he request [is] redirected to an appropriate configuration server based on the identifier, the configuration server having configuration settings data associated with the identifier and specific to the network entity.” (Ex. 1006, ¶25.)

⁹ The relayed request is “M5” in Fig. 5.

2. The system according to claim 1, wherein the ACSMD is further configured to receive a reply from the identified ACS,¹⁰ and

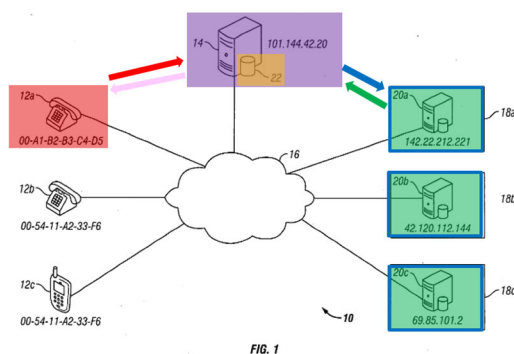
Green arrow.



The server 14 (purple) serves as an “intermediary” and *communicates “with one of the configuration servers 20a... to directly request* and acquire the configuration settings data, and then forwarding the configuration setting data to the network entity 12a.” (Ex. 1006 at ¶62.)

relay the reply to the manageable electronic device.¹¹

Pink arrow.



The server 14 (purple) serves as an “intermediary” and communicates “with one of the configuration servers 20a... to directly request and *acquire the configuration*

¹⁰ This reply is “M6” in Fig. 5.

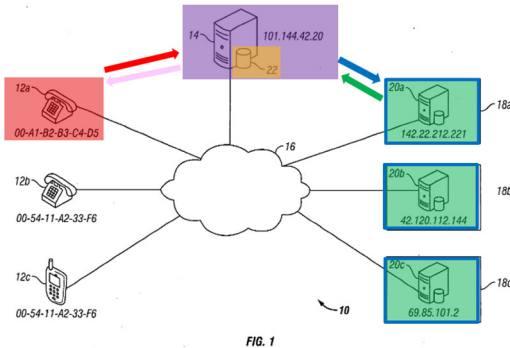
¹¹ This reply is “M7” in Fig. 5.

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

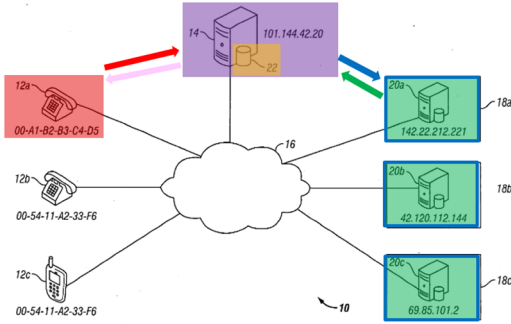
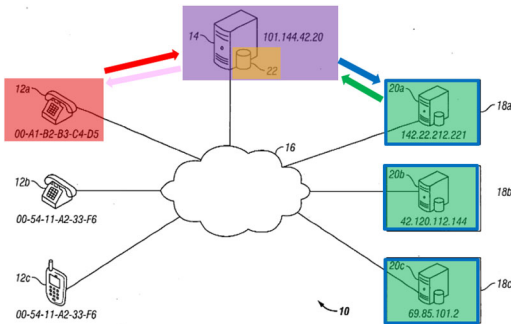
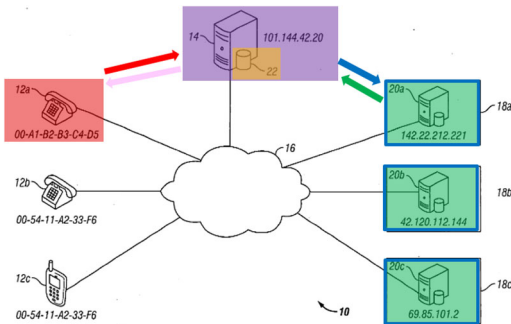
	<i>settings data, and then forwarding the configuration setting data to the network entity 12a.”</i> (Ex. 1006 at ¶62.)
--	---

[099] I also point out that during prosecution of a follow-on application, the USPTO’s Office of Patent Quality Assurance found *Angelot*, which by that time had issued as a patent (U.S. Patent No. 8,089,953). Ex. 1019 at 67.

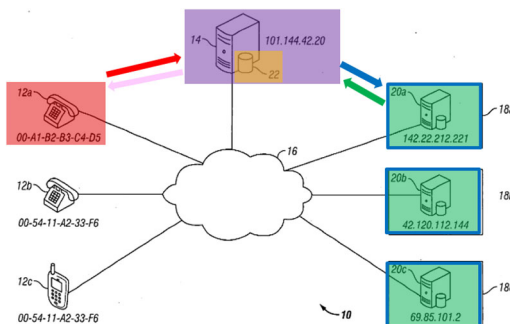
[0100] Below is a summary of the examiner’s opinions regarding *Angelot*, which aligns well with my opinions set for the below.

772 patent Claim Elements	Examiner’s Mapping to <i>Angelot</i>
1. A system for remote device management comprising:	• <i>A system for remote device management in a network comprising:</i> ◦ <i>an auto-configuration server managing device,</i> (Angelot, Fig. 1, Central server 14); Ex. 1019 at 41. 
a plurality of auto-configuration servers (ACSs);	◦ <i>a plurality of auto-configuration servers,</i> (Angelot, Fig. 1 service provide 18a, 18b, 18c, which includes configuration server 20a, 20b, 20c respectively); Ex. 1019 at 41.

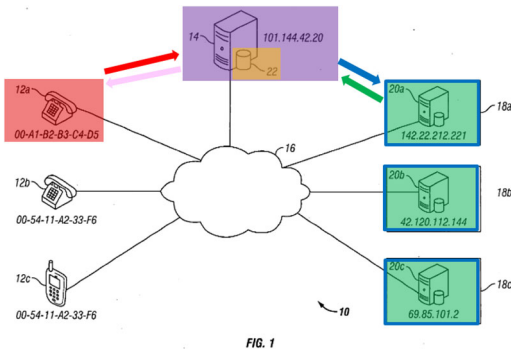
Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

	 FIG. 1
a manageable electronic device;	Not claimed but shown as element 12a in Fig. 1. Ex. 1019 at 41-42.  FIG. 1
an auto configuration server managing device (ACSMD) for controlling access to the ACSs communicatively coupled intermediately between the plurality of ACSs and the managed	• A system for remote device management in a network comprising: ○ an auto-configuration server managing device, (Angelot, Fig. 1, Central server 14); Ex. 1019 at 41.  FIG. 1

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

electronic device; and																					
at least one database communicatively coupled to the ACSM and storing information for the identification of electronic devices,	○ <i>at least one database arranged for holding information for identification of electronic devices</i>, (Angelot, Fig. 1 – database 22 for storing the records, Fig. 3a col. 7 lines 51-54); Ex. 1019 at 41. ○ <i>wherein the auto-configuration server managing device and the at least one database are coupled in a communicative connection</i>, (Angelot, Fig. 1); Ex. 1019 at 41.  FIG. 1 <table><tr><td>IP Device MAC address</td><td>00-A1-B2-B3-C4-D5</td><td>00-54-11-A2-33-F6</td><td>00-54-11-A2-33-F6</td><td>.....</td><td>xx-xx-xx-xx-xx</td></tr><tr><td>SERVICE PROVIDER ID</td><td>SP 18a</td><td>SP 18b</td><td>SP 18c</td><td>.....</td><td>SP 18x</td></tr><tr><td>Configuration server(s) (IP address)</td><td>142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66</td><td>42.120.112.144 144.110.212.20</td><td>69.85.101.2</td><td>.....</td><td>yy-yy-yy-yy</td></tr></table> FIG. 3a <tr><td>wherein the manageable electronic device is configured to send a request for configuration data to the ACSMD,</td><td> ○ <i>wherein the auto-configuration server managing device is arranged for communication with a manageable electronic device over the network, the manageable electronic device configured for sending a request for configuration data</i>, (Angelot, Fig. 1 component 12a, 12 b, 12c – network entity] over the network [Fig. 1], the manageable electronic device configured for sending a request for configuration data [Fig. 1 component 12a, 12b, 12c, col. 2 </td></tr>	IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		xx-xx-xx-xx-xx	SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x	Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		yy-yy-yy-yy	wherein the manageable electronic device is configured to send a request for configuration data to the ACSMD,	○ <i>wherein the auto-configuration server managing device is arranged for communication with a manageable electronic device over the network, the manageable electronic device configured for sending a request for configuration data</i>, (Angelot, Fig. 1 component 12a, 12 b, 12c – network entity] over the network [Fig. 1], the manageable electronic device configured for sending a request for configuration data [Fig. 1 component 12a, 12b, 12c, col. 2
IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		xx-xx-xx-xx-xx																
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x																
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		yy-yy-yy-yy																
wherein the manageable electronic device is configured to send a request for configuration data to the ACSMD,	○ <i>wherein the auto-configuration server managing device is arranged for communication with a manageable electronic device over the network, the manageable electronic device configured for sending a request for configuration data</i>, (Angelot, Fig. 1 component 12a, 12 b, 12c – network entity] over the network [Fig. 1], the manageable electronic device configured for sending a request for configuration data [Fig. 1 component 12a, 12b, 12c, col. 2																				

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

wherein configuration data comprise data for configuring the manageable electronic device, and	lines 40-42 “...the at least one network entity to automatically request configuration settings data...”); ○ <i>and the auto-configuration server manager further being arranged for: receiving the request from the manageable electronic device for configuration data</i>, (Angelot, col. 2 line 44 “receiving the request at the central server...”); Ex. 1019 at 41, 42.  FIG. 1
wherein the ACSMD is configured, responsive to receiving the request, to: identify the manageable electronic device by comparing at least a portion of the request with the information for the identification of electronic devices of the at	○ <i>determining an identification of the manageable electronic device by comparing the request with the information for identification of electronic devices of the at least one database</i>, (Angelot, col. 7 lines 51-55, Fig. 3a, col. 5 lines 62-67, col. 7 lines 34-40, 64-67, col. 8 lines 1-2, i.e. obtain MAC address of the network entity in order to determine the identification of a service provider/configuration server); ○ <i>determining an identification of an auto-configuration server from the plurality of auto-configuration servers in accordance with the identification of the manageable electronic device</i>, (Angelot, col. 8 lines 58-59, Fig. 2 step 112 “determine the service provider/configuration server matching the identifier”, Fig. 3a – table/database) Ex. 1019 at 42.

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

least one database, and identify an ACS from the plurality of ACSs in accordance with the identification of the manageable electronic device to provide configuration data to the manageable electronic device, and	<table><tr><td>IP Device MAC address</td><td>00-A1-B2-B3-C4-D5</td><td>00-54-11-A2-33-F6</td><td>00-54-11-A2-33-F6</td><td>.....</td><td>xx-xx-xx-xx-xx</td></tr><tr><td>SERVICE PROVIDER ID</td><td>SP 18a</td><td>SP 18b</td><td>SP 18c</td><td>.....</td><td>SP 18x</td></tr><tr><td>Configuration server(s) (IP address)</td><td>142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66</td><td>42.120.112.144 144.110.212.20</td><td>69.85.101.2</td><td>.....</td><td>yyyyyyyy</td></tr></table> FIG. 3a	IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		xx-xx-xx-xx-xx	SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x	Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		yyyyyyyy
IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		xx-xx-xx-xx-xx														
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x														
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		yyyyyyyy														
wherein the ACSMD is further configured to relay the request to the identified ACS.	The examiner stated that Angelot does not “specifically” disclose relaying the requests to the auto-configuration server, I disagree for the reasons stated below, e.g., “relaying” has been construed in a manner that is covered by Angelot and patent owner argued that “relay” means send, and Angelot plainly discloses sending the request to the identified ACS. Ex. 1019 at 42.																		

In response, the patent owner did not dispute the examiner’s findings and argued against modifying Angelot because the secondary reference disclosed relaying data for video conferences. Ex. 1019 at 28-30.

1. Claim 1 (cancelled)

a) [1pre]. A system for remote device management comprising:

[0101] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 41. An example of a “system for remote device management” is *Angelot* system for “configuring network entities with the requisite settings in order to participate within a network.” (see Ex. 1006 at ¶3). *Angelot* also clearly addresses the need to automate earlier systems that required the user to manually configure device, server, and network settings so that the user is no longer tasked with manual configurations. Specifically, *Angelot* discloses that the remote configuration is automatic and different from earlier systems where “the user is often tasked to manually enter the configuration settings for the device, such as the service provider’s configuration server address or other network settings.” (Ex. 1006 at ¶7).

[0102] *Angelot* is different from the earlier manual configuration systems because *Angelot*’s system will automatically configure a network entity, like a phone 12a¹² (red in annotated Fig. 1 below), where the phone 12a is “associated

¹² See Ex. 1006, ¶43 (The network entity 12a to 12c may be “any IP device or endpoint (end node) for participating in a packet switched network, such as, but not limited to, IP phones, H.323 phones, DECT phones, SIP-DECT phones, ATAs, mobile phones, IPTVs, projectors, PDAs, digital cameras, PC, MP3 players, set-

with at least one service provider” 18a to 18c (blue in annotated figure) having a
“configuration server” 20a to 20c (green in annotated) that stores “configuration
settings for the” CPE. (Ex. 1006 at ¶¶11-15).

top boxes, game consoles, gateways, soft phones, firewalls, access-points,
modems, network appliances, or any combination(s) thereof”).

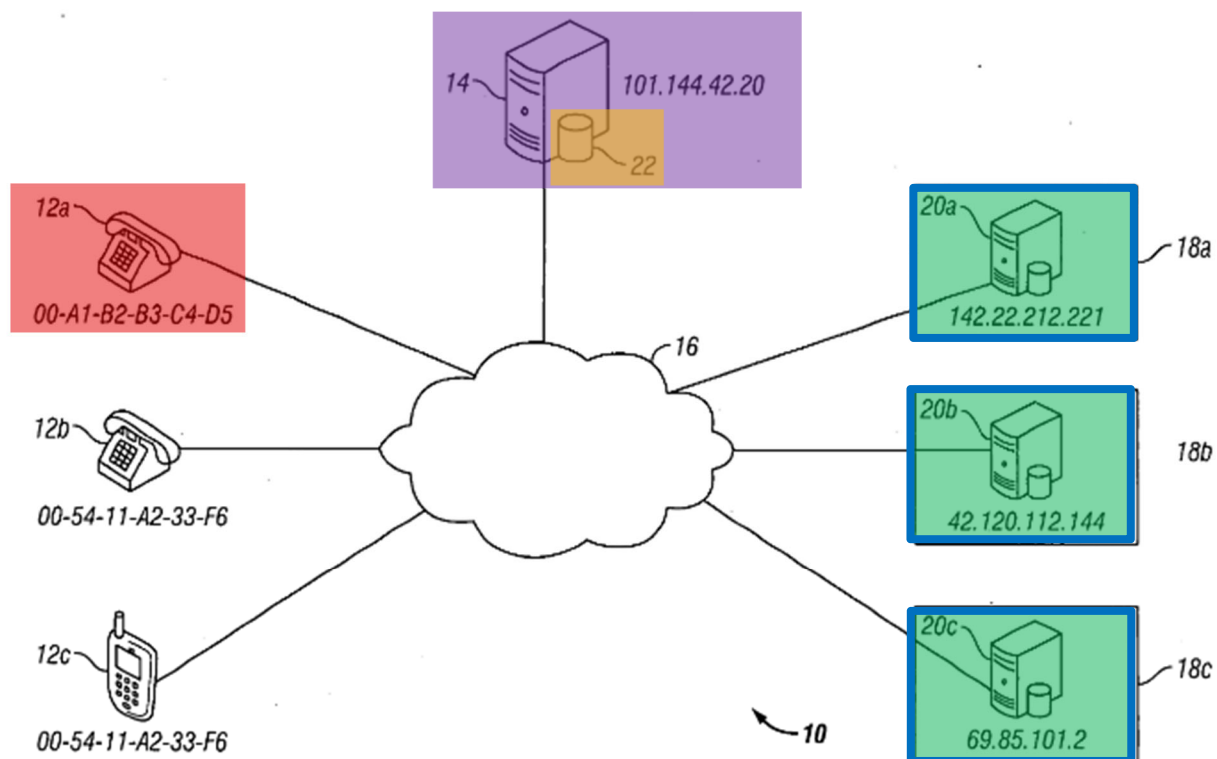


FIG. 1

Figure 1 (annotated) Ex. 1006.

[0103] The network entity, red phone 12a, is “included with factory-set default configuration data, such as, DHCP settings (enabled)” so it can be automatically configured using an included “URI to a central server 14 [purple] having information related to the IP phone 12a’s configuration settings.” (Ex. 1006 at ¶50). The red phone 12a “automatically initiates a discovery process, in which it sends messages over any suitable transport protocol, such as UDP, TCP, TLS, HTTP(S), FTP, or TFTP, in order to retrieve its settings from a remote central server 14 [purple].” Also, the central server 14 (purple) controls access to the

various service providers 18 (blue) and their corresponding configuration servers 20 (green).

[0104] The red phone's identity is its MAC address. The central server 14 (purple) includes database 22 (orange). "As part of the provisioning process, the MAC address" (identity) is "associated with at least one of the service providers 18a, 18b, or 18c [blue]" in the orange database 22. (Ex. 1006 at ¶51). The database is "for storing the records of the MAC addresses and the associated service provider 18a, 18b, or 18c, such as a first mapping table" that is stored in the database's memory that is "associated with the central server 14." (Ex. 1006 at ¶51). It is, therefore, my opinion that *Angelot* discloses the features claimed here.

[0105] *Angelot* allows any type of network device to be configured without pre-configuring a dedicated address for configuration because the addresses of the configuration servers is maintained in the central server's database. (See Ex. 1006 at ¶55: "This arrangement thus allows for all *IP phones 12a from manufacturer A ... to receive the same configuration settings, while all IP phones 12b from manufacturer B ... receive the same configuration settings.*") This is like the '772 patent's auto-configuration disclosure, in my opinion.

[0106] I have annotated Figure 1 below to show that *Angelot*'s red phone 12 sends a message (red arrow) to the purple central server 14. The purple central server 14 then relays (blue arrow) that message to the relevant configuration server

20. The relevant configuration server replies (green arrow) with configuration information, and the central server 14 relays the configuration information (pink arrow) to the IP phone 12.

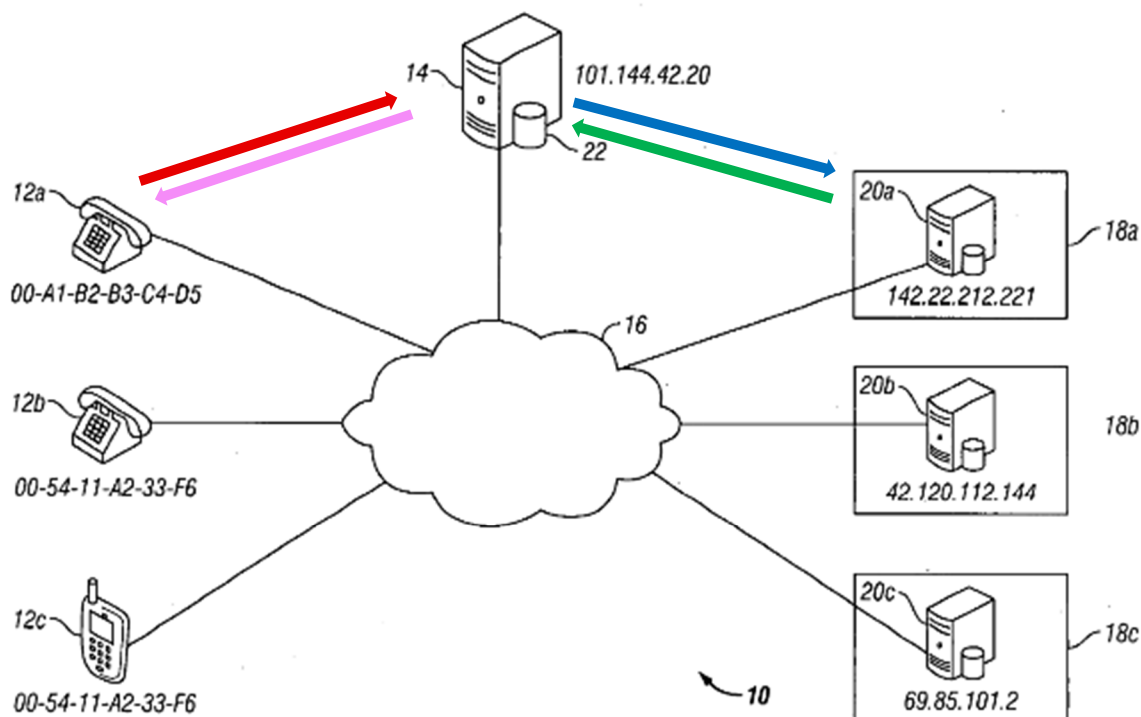


Figure 1 (annotated) Ex. 1006.

Therefore the features of this claim are disclosed by Angelot.

b) [1a]. a plurality of auto-configuration servers (ACSs);

[0107] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 41.

a plurality of auto-configuration servers, (Angelot, Fig. 1 service provide 18a, 18b, 18c, which includes configuration server 20a, 20b, 20c respectively);

I have annotated an excerpt from Figure 1, below, to show a plurality of service providers 18a to 18 c (blue), which each have a configuration server 20a to 20c (green).

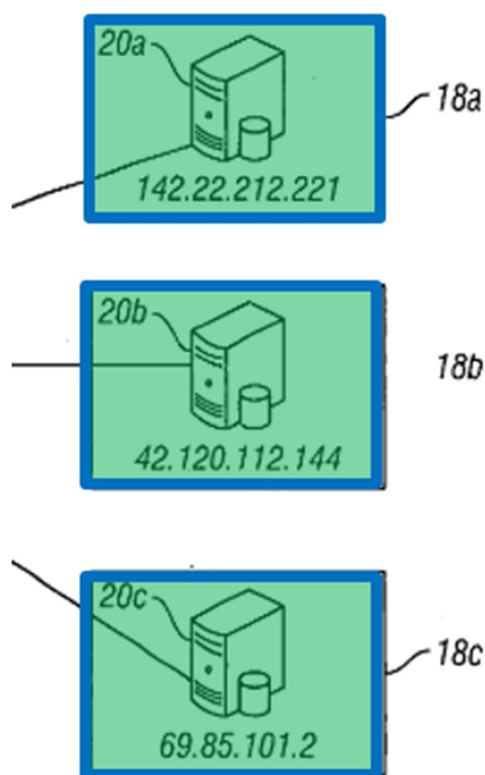


Figure 1 (excerpted and annotated) Ex. 1006.

In my opinion, each configuration server 20a to 20c (green) corresponds to an auto-configuration server (ACS). See Ex. 1006 at ¶52: “The configuration server 20a, 20b or 20c includes configuration settings specific to the IP phone 12 a with specific MAC addresses.”

[0108] Notably, the configuration settings for network entities 12 (like the red phone) are stored on the configuration servers 20. As *Angelot* explains “each IP

phone 12a is typically identified by its MAC address,” so “*the configuration files on the configuration server 20a may be named using this information, for example, a configuration file named iphone12a-mac-00-a1-b2-b3-c4-d5.cfg would correspond to the IP phone 12a having 00-a1-b2-b3-c4-d5 as its MAC address.*”

Ex. 1006 at 52 (with my emphasis added). “The configuration settings may include phone-specific configuration information, and platform-specific configuration information, such as, but not limited to, the type of phone, carrier, service, or enterprise system information, central server(s) URIs, configuration server(s) URI, port assignments, registration information, dial plan, NTP time settings, soft-keys, XML services and applications, SIP registration information, usernames and passwords, phone book directory, speaker volume settings and so forth.”

[0109] The district court’s construed as “plurality of auto-configuration servers (ACSs)” as “two or more systems of hardware and/or software, each of which is capable of automatically configuring a manageable electronic device.” (see Ex. 1005 at 46). In my opinion, the configuration servers 20a to 20c are a plurality of ACSs because they meet the district court’s construction.

[0110] The configuration servers 20a to 20c store “the configuration settings.” The configuration settings are also “are provided to the network entity 12 a, 12 b, or 12 c” so the each entity, e.g., the red phone 12 a, “is automatically configured without requiring any manual input of settings by the user.” Ex. 1006 at

¶47. Therefore, in my opinion, *Angelot* discloses a plurality of ACSs as required by this claim.

c) **[1b] a manageable electronic device;**

[0111] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 41.

communication with a manageable electronic device over the network, the manageable electronic device configured for sending a request for configuration data, (Angelot, Fig. 1 component 12a, 12 b, 12c – network entity] over the network [Fig. 1], the manageable electronic device configured for sending a request for configuration data [Fig. 1 component 12a, 12b, 12c, col. 2

Angelot discloses numerous manageable electronic devices like mobile phones, set-top boxes, gateways, etc. Ex. 1006 at ¶43. These devices are generically called a network entity 12. In my analysis, network entity 12a, such as the red IP phone, corresponds to the claimed “manageable electronic device.”

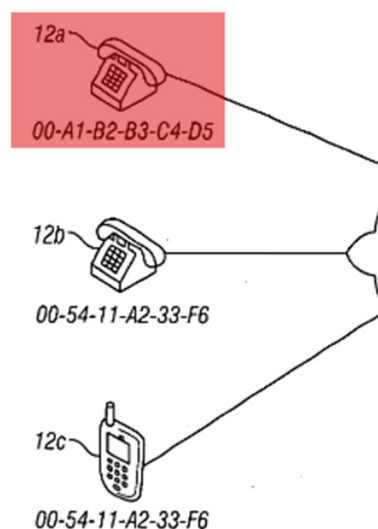


Figure 1 Ex. 1006 (excerpted and annotated).

In my opinion, this device is a manageable device because it requests “configuration settings from the central server 14” and “the configuration settings are provided to the network entity 12a” to automatically configure it “without requiring any manual input of settings by the user.” (Ex. 1006 at ¶¶46-47). Also, the red phone 12a is an “electronic device that can be configured over a network” as required by the district court claim construction (see Ex. 1005 at 42). It is, therefore, my opinion that *Angelot* discloses the features of this claim.

- d) **[1c]. an auto-configuration server managing device (ACSMD) for controlling access to the ACSs communicatively coupled intermediately between the plurality of ACSs and the managed electronic device; and**

[0112] In my opinion, *Angelot* discloses this feature. The USPTO found substantially the same. Ex. 1019 at 41.

- *an auto-configuration server managing device, (Angelot, Fig. 1, Central server 14);*
- *wherein the auto-configuration server managing device and the at least one database are coupled in a communicative connection, (Angelot, Fig. 1);*

I have annotated figure 1 to show that *Angelot* discloses re-direct server 14 (purple), which identifies the querying phone 12a (red) and relays the query to the appropriate configuration server 20a (green) based on the identity of the IP phone 12a (red).

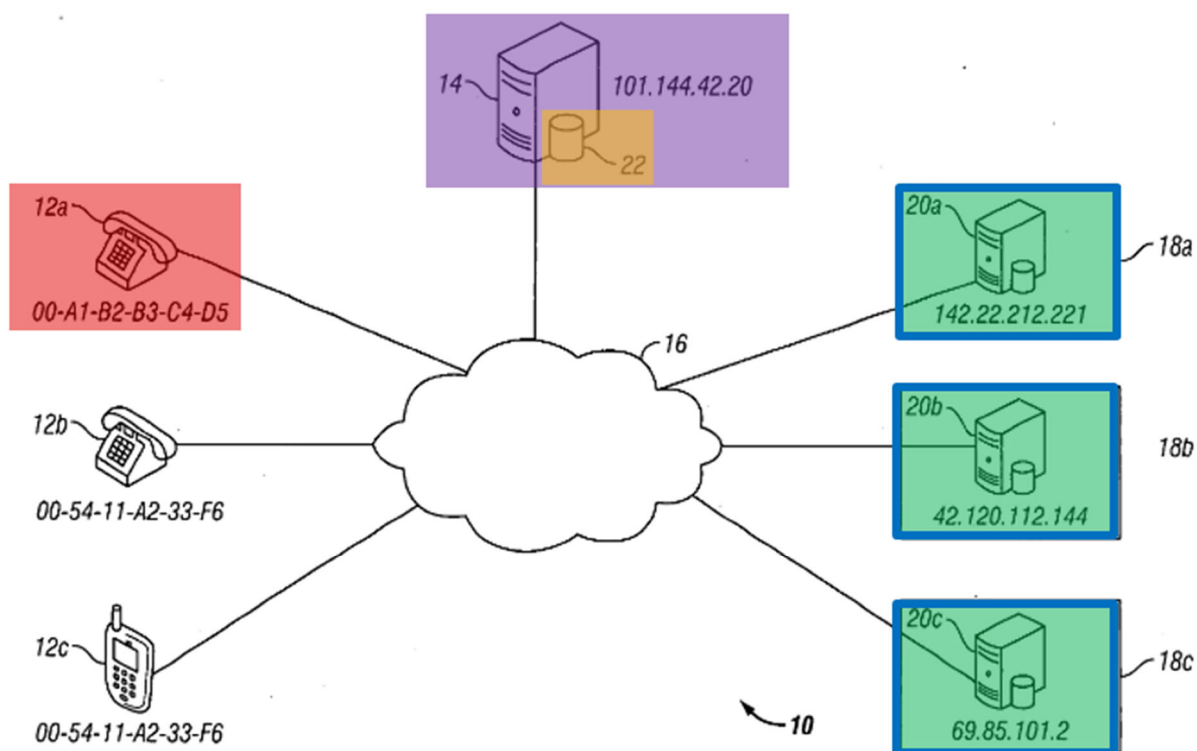


FIG. 1

Figure 1 (annotated) Ex. 1006.

The “server 14 [purple] redirects any configuration related queries from the [red phone] 12a ... to the configuration server 20a, 20b, 20c [green].” (Ex. 1006, ¶47.)

The redirecting by the purple server 14 “based on the identity of the [red phone] 12a....” (Ex. 1006, ¶47.)

[0113] “Upon receipt of the request, the central server 14 [purple] processes the request to ... determine[] which of the plurality of service providers 18a, 18b, 18c [blue] the MAC address belongs to. Once such a determination has been established, the central server 14 [purple] then *redirects the request to an appropriate service provider* 18a, 18b or 18c [blue],” next “a configuration server 20a, 20b or 20c [green], *associated with the appropriate service provider* ... selects the configuration settings for the IP phone 12a [red] with that specific MAC address....” (see Ex. 1006 at ¶54). Therefore, in my opinion, the server 14 (purple) meets the district court’s requirement for the ACSMD because it is “hardware and/or software that relays configuration requests to the auto-configuration servers.” (Ex. 1005 at 48).

[0114] The server 14 (purple) also *processes* the requests based on the red phone’s MAC address and directs the requests to the relevant service provider/configuration server (blue/green). Therefore, in my opinion, server 14 (purple) controls whether the red phone 12a gains access to the configuration servers 20 (green) (Ex. 1006 at ¶54). The server 14 (purple) also remains in contact

with the IP phone 12a (red) and the configuration servers (green) via the network

16. In my opinion this meets the district court’s construction of “controlling access” because the server 14 (purple) controls access to the configuration servers (green) in the manner required by the district court’s construction (Ex. 1005 at 54).

It is therefore my opinion that *Angelot* discloses the features of this claim.

- e) **[1d]. at least one database communicatively coupled to the ACSM[D] and storing information for the identification of electronic devices,**

[0115] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 41.

- *at least one database arranged for holding information for identification of electronic devices*, (*Angelot*, Fig. 1 – database 22 for storing the records, Fig. 3a col. 7 lines 51-54);

Below I have annotated a portion of Figure 1 to show that *Angelot* discloses database 22 (orange) communicatively coupled to the central server 14 (purple).

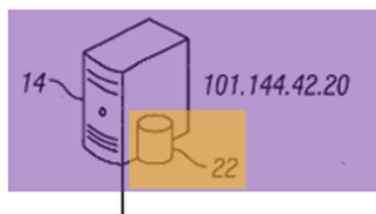


Figure 1 (excerpted and annotated) Ex. 1006.

In my opinion, database 22 corresponds to the claimed “at least one database.” As I explained above, the purple server 14 includes the orange database 22. The orange

database 22 is “for storing the records of the MAC addresses and the associated service provider 18 a, 18 b, or 18 c, such as a first mapping table ..., as shown in FIG. 3a.” (Ex. 1006 at ¶51). Therefore, a person having ordinary skill in the art would have immediately understood that *Angelot* discloses “at least one database” 22 “communicatively coupled to the ACSM[D],” i.e., the database 22 (orange) is communicatively coupled to the server 14 (purple). A person with ordinary skill in the art that read *Angelot* also would have readily appreciated that orange database 22 is used by the purple server 14 to know which configuration server to direct the request for configuration settings.

IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		xx-xx-xx-xx-xx
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		yy.yyy.y.yyy

FIG. 3a

(Ex. 1006 at Fig. 3a). Fig. 3a shows that database 22 stores IP Device MAC addresses. The MAC addresses are examples of “information for the identification of electronic devices.” The database 22 also stores configuration server IP addresses that correspond to the MAC addresses. Therefore, in my opinion, *Angelot* discloses the features of this claim.

- f) **[1e]. wherein the manageable electronic device is configured to send a request for configuration data to the ACSMD,**

[0116] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 41-42.

communication with a manageable electronic device over the network, the manageable electronic device configured for sending a request for configuration data, (Angelot, Fig. 1 component 12a, 12 b, 12c – network entity) over the network [Fig. 1], the manageable electronic device configured for sending a request for configuration data [Fig. 1 component 12a, 12b, 12c, col. 2

lines 40-42 “...the at least one network entity to automatically request configuration settings data...”);

The red phone 12a in *Angelot* “transmit[s] a first signal to request configuration settings associated with the IP phone 12a []from the central server 14.” (Ex. 1006 at ¶54). The central server 14 (purple) “receives a request for configuration settings from the [red phone] 12a” including the phone’s “identity data” such as its “unique MAC address.” (Ex. 1006 at ¶54). The red phone 12a, which again is an example of the manageable electronic device, sends a request for configuration settings, which again is an example of the claimed request for configuration data, to the

server 14 (ACSMD) (Ex. 1006). Thus, Angelot discloses a manageable electronic device that sends a request for configuration data to an ACSMD.

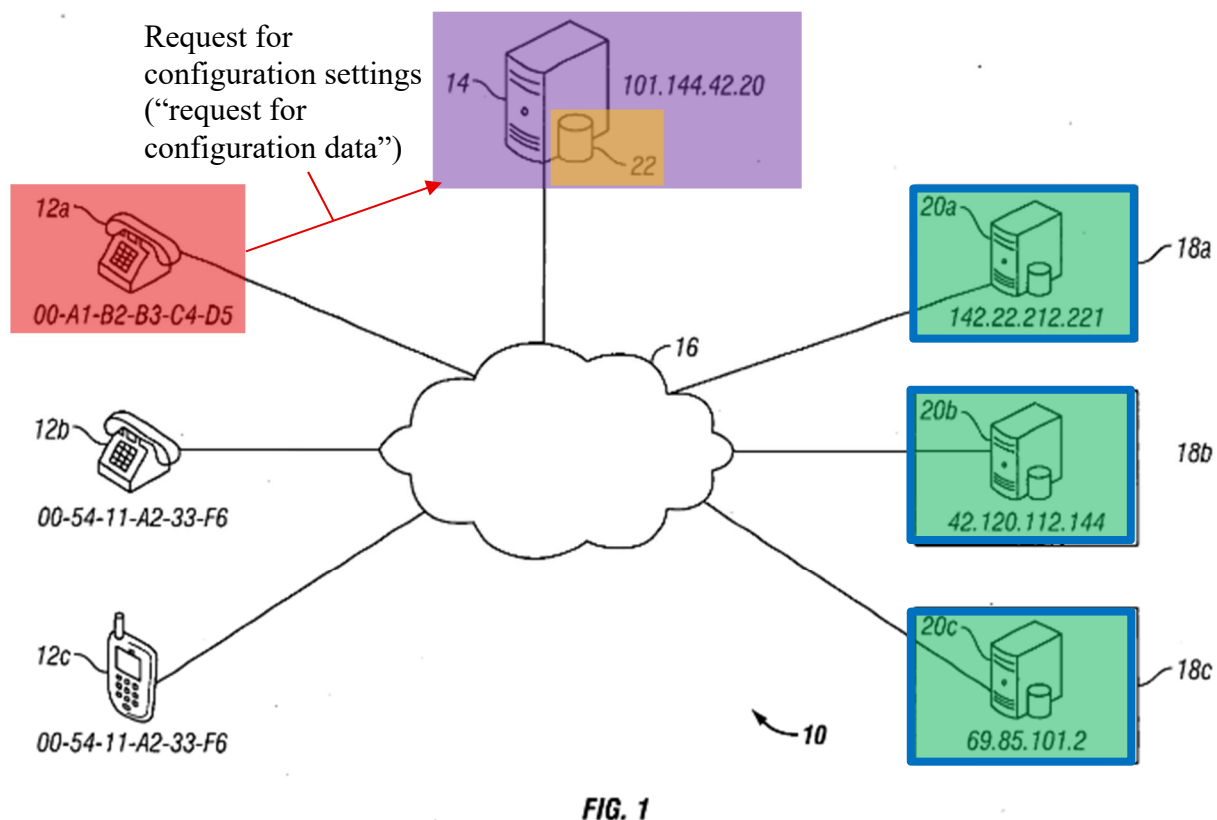


Figure 1 (annotated) Ex. 1006.

Figure 2 (reproduced below) also shows that the red phone 12a will “automatically request configuration settings from the central server 14 via the URI” in step 110 and the URI is included in the phone 12a’s software (102).

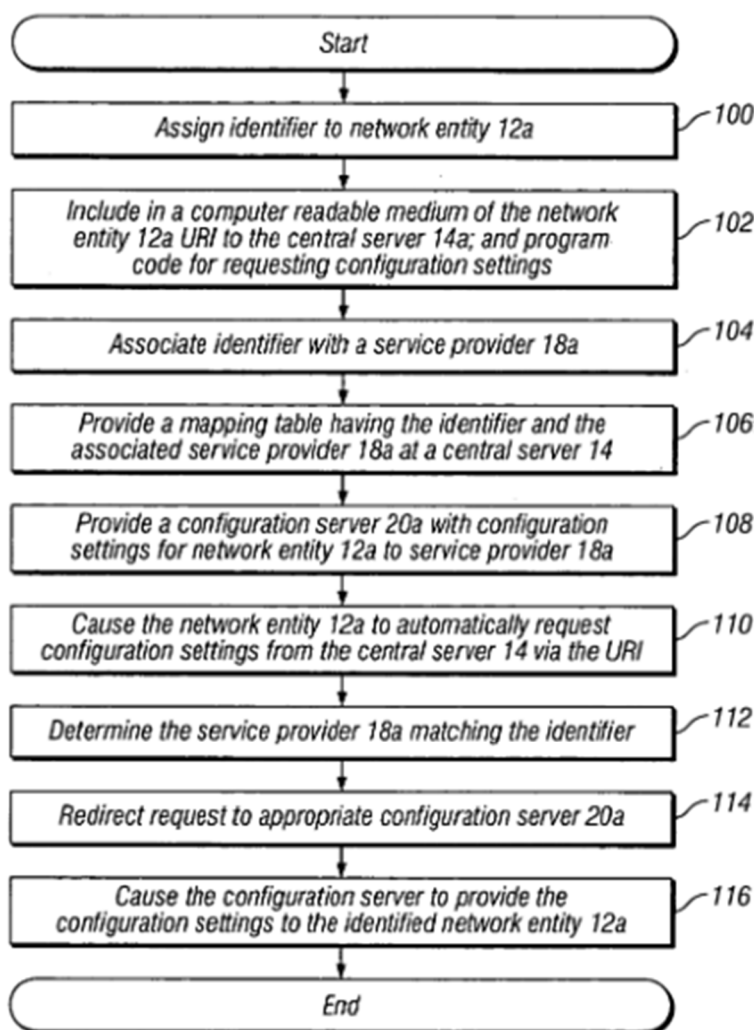


FIG. 2

Therefore, in my opinion, *Angelot* discloses the features of this claim.

- g) [1f]. wherein configuration data comprise data for configuring the manageable electronic device, and

[0117] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 41-42.

communication with a manageable electronic device over the network, the manageable electronic device configured for sending a request for configuration data, (Angelot, Fig. 1 component 12a, 12 b, 12c – network entity] over the network [Fig. 1], the manageable electronic device configured for sending a request for configuration data [Fig. 1 component 12a, 12b, 12c, col. 2

lines 40-42 “...the at least one network entity to automatically request configuration settings data...”);

Angelot discloses that the phone 12a “is auto-configured in the background and without user input.” (Ex. 1006).

[0118] In my opinion, a person having ordinary skill in the art would have understood that this auto-configuration is a result of the configuration data from the configuration server 20 of a service provider 18. The “configuration server 20a, 20b or 20c includes configuration settings specific to the IP phone 12a with specific MAC addresses,” and each provider 18 has a server 20 having “a second mapping table with MAC addresses and *associated configuration settings data* in a database associated with each of the configuration servers 20a, 20b or 20c.” (Ex. 1006 at ¶52).

[0119] Since the configuration settings are associated with a specific device’s MAC address, e.g., the red phone’s MAC address, the configuration

settings are for configuring that device. *See, e.g.*, Ex. 1006 at ¶54: “service provider 20a, 20b or 20c, selects ***the configuration settings for the IP phone 12a*** with that specific MAC address....” (emphasis added). Also paragraph 55 in Angelot discloses that: “The request is subsequently forwarded to the appropriate service provider 18b with configuration server 20b which ***selects the appropriate configuration settings for the IP phone 12b*** using the second mapping table....” (emphasis added). And paragraph 62 discloses that: “[T]he redirect server 14 serves as ... [an] intermediary,¹³ by communicating with one of the configuration servers 20a, 20b or 20c to directly request and acquire the configuration settings data, and then forwarding the configuration setting data to the network entity 12 a.”

[0120] Therefore, in my opinion, the configuration settings data corresponds to the claimed “configuration data” that includes “data for configuring the manageable electronic device.” Angelot’s “configuration files on the configuration server 20a may be named using this information, for example, a configuration file named iphone12a-mac-00-a1-b2-b3-c4-d5.cfg would correspond to the IP phone 12a having 00-a1-b2-b3-c4-d5 as its MAC address.” (Ex. 1006 at ¶52). “The configuration settings may include phone specific configuration information, and

¹³ This is the same as the claimed “ACSMD,” which the ’772 patent explains “functions as an intermediate and relays” a message for configuration data “to the dedicated auto-configuration server...” (Ex. 1001 at 6:63-7:3; 8:4-14.)

platform specific configuration information, such as, but not limited to, the type of phone, carrier, service, or enterprise system information, central server(s) URIs, configuration server(s) URI, port assignments, registration information, dial plan, NTP time settings, soft-keys, XML services and applications, SIP registration information, usernames and passwords, phone book directory, speaker volume settings and so forth.” (Ex. 1006). Therefore, in my opinion, *Angelot* discloses the features of this claim.

- h) **[1g]. wherein the ACSMD is configured, responsive to receiving the request, to:**
- identify the manageable electronic device by comparing at least a portion of the request with the information for the identification of electronic devices of the at least one database, and**
- identify an ACS from the plurality of ACSs in accordance with the identification of the manageable electronic device to provide configuration data to the manageable electronic device, and**

[0121] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 41.

- *and the auto-configuration server manager further being arranged for: receiving the request from the manageable electronic device for configuration data*, (Angelot, col. 2 line 44 “receiving the request at the central server...”);
- *determining an identification of the manageable electronic device by comparing the request with the information for identification of electronic devices of the at least one database*, (Angelot, col. 7 lines 51-55, Fig. 3a, col. 5 lines 62-67, col. 7 lines 34-40, 64-67, col. 8 lines 1-2, i.e. obtain MAC address of the network entity in order to determine the identification of a service provider/configuration server);

The purple server 14, which corresponds to the claimed ACSMD, receives a request for configuration data, as I explained above when discussing claim elements 1e and 1f. Below, I have reproduced Figure 2, which shows that red phone 12a (the claimed “manageable electronic device”) will “automatically request configuration settings from the central server 14,” (the claimed ACSMD) “via the URI.” The purple server 14 then processes the red phone 12a’s request to determine the corresponding service provider 18a and “redirect[s the] request to [the] appropriate configuration server 20a,” which is example of the claimed ACS from among multiple ACSs (20a, 20b, 20c). See Figure 2 steps 110 to 114 in Ex. 1006 ¶54.

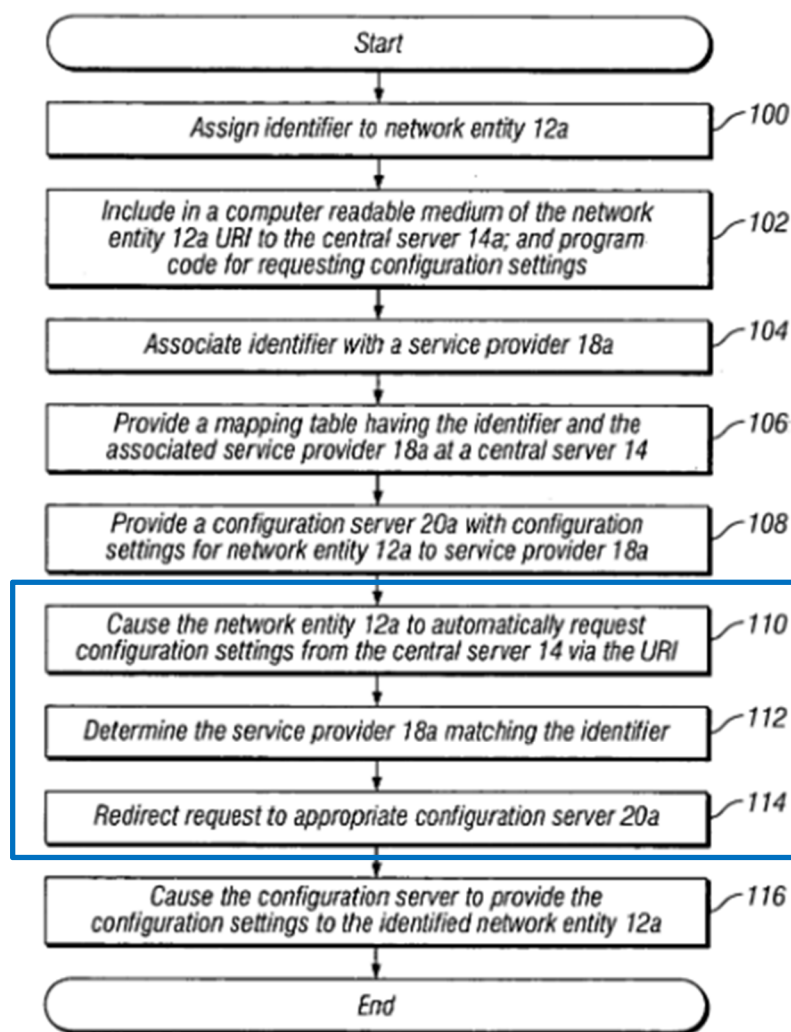


FIG. 2

Figure 2 Ex. 1006 (see steps 110 to 114)

[0122] The purple server 14 “receives a request for configuration settings from the [red] IP phone 12a.” (Ex. 1006 at ¶54.) The “request includes the identity data of the [red] IP phone 12a, such as the unique MAC address.” (Ex. 1006 at ¶54.) After receiving that request, the purple server 14 (claimed ACSMD) identifies the red phone 12a (claimed manageable electronic device) by comparing

at least a portion of the request (identity data/MAC address) with the information for the identification of electronic devices of the at least one database (IP Device MAC address in Table 1).

[0123] Below I reproduced Angelot's Figure 3a to show that the server's 14 database 22 includes the device's unique MAC address. Ex. 1006 , ¶51: "database 22 [is] for storing the records of the MAC addresses and the associated service provider 18a, 18b, or 18c, such as a first mapping table which is maintained in a memory associated with the central server 14 [], as shown in FIG. 3 a."

IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		XX-XX-XX-XX-XX
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		YY.YYY.Y.YYY

FIG. 3a

Figure 3a (annotated) Ex. 1006.

The server 14 (ACSMD), after receiving the configuration data request from the phone 12a (manageable electronic device), identifies the phone 12a by comparing at least a portion of the request (identity data including the MAC address) with the IP Device MAC address stored in database 22 (the information for the identification of electronic devices of the at least one database).

[0124] Additionally, in response to receiving that request, the server 14 (ACSM) also identifies the IP address of a configuration server (identifies an ACS) from the plurality of configuration servers (ACs) in accordance with the identification of the manageable electronic device (IP Device MAC address) to provide configuration data to the IP phone 12a (manageable electronic device).

[0125] I have annotated Figure 3a below to show that “the first mapping table [is] used to redirect the request to a[n] appropriate configuration server [green] associated with each of the service providers [blue]....” Ex. 1006 , ¶23; ¶54: “a configuration server 20 a, 20 b or 20 c, associated with the appropriate service provider [], selects the configuration settings for the IP phone 12 a with that specific MAC address...”. “The configuration servers 20 a, 20 b, 20 c are coupled to the central server 14 a, such that queries for configuration settings may be redirected thereto based on the first mapping table.” (Ex. 1006 at ¶52).

IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		XX-XX-XX-XX-XX
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		YY.YYY.Y.YYY

FIG. 3a

Figure 3a (annotated) Ex. 1006.

Therefore, a person having ordinary skill in the art reading *Angelot* would understand that the server 14 (ACSMD) receives the request for configuration settings from the red phone 12a (manageable network device) and, in response, the server 14 is configured to identify the phone 12a by comparing identity data/MAC address of the phone 12 (at least a portion of the request) with the information in Table 1 shown in Fig. 3a Ex. 1006 (information for the identification of electronic devices) which is stored in database 22 (the at least one database).

[0126] The server 14 “also determines which of the plurality of service providers 18a, 18b, 18c the MAC address belongs to” and once “such a determination has been established, the central server 14 then redirects the request to an appropriate service provider 18 a, 18 b or 18 c, as per first mapping table (step 114).” (Ex. 1006 , ¶54). Therefore, a person having ordinary skill in the art would have understood that the server 14 (ACSMD) receives the request for configuration settings from the red phone 12a (manageable network device) and, in response, the server 14 is configured to identify an configuration server 20a (identity an ACS from the plurality of ACSs) in accordance with the identification of the phone 12a (manageable electronic device) to provide configuration settings (configuration data) to the phone 12a (manageable electronic device). In my opinion, *Angelot* discloses the features of claim element 1g.

- i) **[1h]. wherein the ACSMD is further configured to relay the request to the identified ACS.**

[0127] In my opinion, *Angelot* does disclose this feature, especially in view of the construction of “relay” and patent owner’s litigation interpretation of “relay.” As I previously explained, the server 14 (ACSMD) is coupled to the configuration servers 20 (ACSs) such that requests for configuration settings are redirected to the relevant configuration server based on the first mapping table shown in Fig. 3a. Below I annotated Figure 2 to highlight step 114 where the server 14 (ACSMD) relays the request for configuration settings (the request) to the configuration server 20a corresponding to the requesting phone 12a (the request is relayed to the identified ACS).

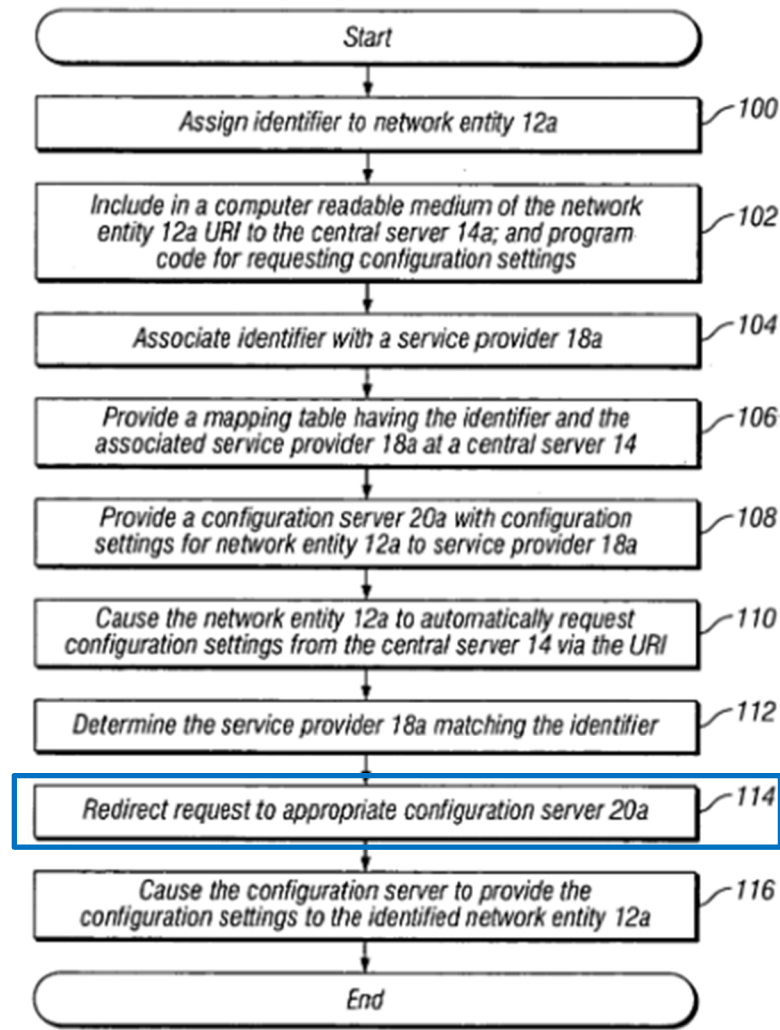


FIG. 2

Figure 2 (annotated) Ex. 1006.

[0128] *Angelot* explains that the “server [ACSM] redirect[s] the request to an appropriate configuration server having the configuration settings data specific to the identifier.” (Ex. 1006 at ¶19): “[T]he request [is] redirected to an appropriate configuration server based on the identifier, the configuration server having configuration settings data associated with the identifier and specific to the

network entity.” (Ex. 1006 at ¶25). Also, the “server 14 redirects any configuration related queries from the network entity 12a, 12b, or 12c to the configuration server 20a, 20b, 20c.” (Ex. 1006 at ¶47). And, “[t]he configuration servers 20a, 20b, 20c are coupled to the central server 14a, such that queries for configuration settings may be redirected thereto ***based on the first mapping table.***” (Ex. 1006 at ¶52 (emphasis added)). “[T]he redirect server 14 serves as a proxy or intermediary, by communicating with one of the configuration servers 20a, 20b or 20c to directly request and acquire the configuration settings data...” (Ex. 1006 at ¶62).

[0129] Therefore, a person having ordinary skill in the art would have read Angelot and understood that the server 14 “relays” the phone 12a’s request to the configuration server (identified ACS) identified in the first mapping table.

[0130] In my opinion, the sending of the request from the server 14 to the configuration server 20a meets the district court’s construction of “relay” because the server 14 ***processes or otherwise manages the request based on the requesting device’s identity/MAC address***, i.e., “based at least in part on” the request’s “payload.” (see Ex. 1005 at 61). As *Angelot* explains, “[u]pon receipt of the request, *the central server 14 processes the request to determine whether the first mapping table comprises the unique MAC address associated with the request*, and also determines which of the plurality of service providers 18 a, 18 b, 18 c the MAC address belongs to... [then] a configuration server 20 a, 20 b or 20 c,

associated with the appropriate service provider 20 a, 20 b or 20 c, selects the configuration settings for the IP phone 12a with that specific MAC address as per the second mapping table...” (see Ex. 1006 at ¶54).

[0131] In my opinion, Angelot’s disclosure of sending of the request from the purple server 14 to the configuration server 20a meets the Patent Owner’s understanding in litigation of “relay” because the server sends/passes the request to the configuration server 20a. Ex. 1006 at ¶62: “[T]he redirect server 14 serves as a proxy or intermediary, by *communicating with one of the configuration servers 20 a, 20 b or 20 c to directly request* and acquire the configuration settings data, and then forwarding the configuration setting data to the network entity 12 a”. Also, in Ex. 1006 ¶46, the IP phone 12a is communicatively coupled to the network 16 and “[t]he term ‘communicatively coupled’ is used in its broadest sense to mean coupling in any fashion *that allows information to be passed between network entities 12 a, 12 b, 12 c, and other network devices within the network 16, such as the central server 14, configuration servers 20 a, 20 b or 20 c, or other servers, gateways, routers, switches, and so forth*”.

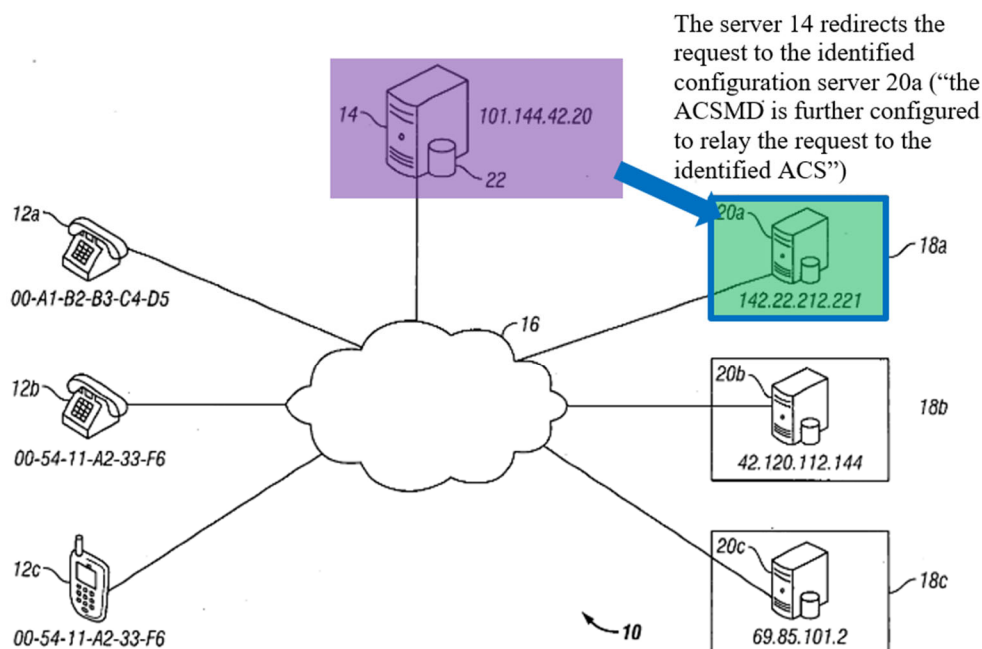


FIG. 1

Figure 1 (annotated) Ex. 1006.

[0132] As an example, “when an end user powers on a phone 12b and connects it to the network 16, the phone 12b immediately connects to *the central server 14... refers to the master table* to determine whether the MAC address falls within the range of MAC addresses for any of the service providers 18a, 18b, or 18c. The request is subsequently forwarded to ... configuration server 20b which selects the appropriate configuration settings for the IP phone 12b using the second mapping table...” (see Ex. 1006 at ¶55 (emphasis added)). The same is true for IP phone 12a’s request being relayed to configuration server 20a by the central server 14. Therefore, in my opinion, *Angelot* discloses the features of this claim.

2. Claim 2

- a) **The system according to claim 1, wherein the ACSMD is further configured to receive a reply from the identified ACS, and relay the reply to the manageable electronic device.**

[0133] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 43.

As per claims 3, 12, 14 and 16, claims 2, 11, 13 and 15 are incorporated and Angelot further discloses:

- *wherein the auto-configuration server managing device is further arranged for receiving a reply from the identified auto-configuration server and relaying the reply to the manageable electronic device, (Angelot, Col. 10:30-37).*

The purple server 14 (ACSMD) is an “intermediary” that communicates “with one of the configuration servers 20a... to directly request and *acquire the configuration settings data, and then forwarding the configuration setting data to the network entity 12a.*” (Ex. 1006 at ¶62, my emphasis added). This is an example of the purple server 14 *sending/passing* the configuration setting data (“the reply”) to the red phone 12a (“the manageable electronic device”), and this communication between the red phone 12a and server 14 aligns with Patent Owner’s definition of “reply,” in my opinion.

[0134] As I have previously explained, *Angelot* processes the IP phone 12a’s request to determine the proper configuration server 20a by using the first

look-up table (Fig. 3a Ex. 1006), and then relays the request to the relevant server, e.g., sever 20a. In Ex. 1006 at ¶47, the server 14 identifies the network entity 12a and sends the query to the appropriate configuration server 20a based on the identity of the network entity 12a. In paragraphs 51 and 52, the purple server 14 knows which configuration server 20 to send the query to by using a “first mapping table” stored in the orange database 22, which correlates the red phone 12a’s MAC address with the IP address of the configuration server 20a. “The configuration settings may include phone specific configuration information, and ... *central server(s) URIs...*” (Ex. 1006 at ¶ 52 (emphasis added)). Therefore, a person having ordinary skill in the art would have understood that *Angelot* is teaching that the configuration server 20a knows where (purple central server 14) to send the configuration settings data. A person having ordinary skill in the art would have understood that when the purple server 14 acquires the configuration setting data from the identified configuration server (receives a reply from the identified ACS), it then “pass[es] said configuration setting data to said [red phone] having said identifier.” (see Ex. 1006 at cl. 13 as originally filed.)

[0135] Another way to state this is that as the purple server 14 receives a reply from the identified configuration server 20a with the configuration setting data, and relays the configuration setting data to the phone 12a. The configuration setting data (reply) from the identified configuration server 20a is (1) acquired by

the purple server 14 from the configuration server 20a and then (2) “***provided to the IP phone 12a based on the MAC address.***” (Ex. 1006 at ¶¶52, 62. (emphasis added)). Therefore, a person having ordinary skill in the art reading Angelot would have understood that the purple server 14 relays/sends/passes the configuration setting data to the phone 12a based on its MAC address and the server 14 is processing or otherwise managing the reply based on its payload, as required in the Texas court’s construction.

[0136] Below is an annotation of Figure 1 that I made to help illustrate the reply back to the phone 12.

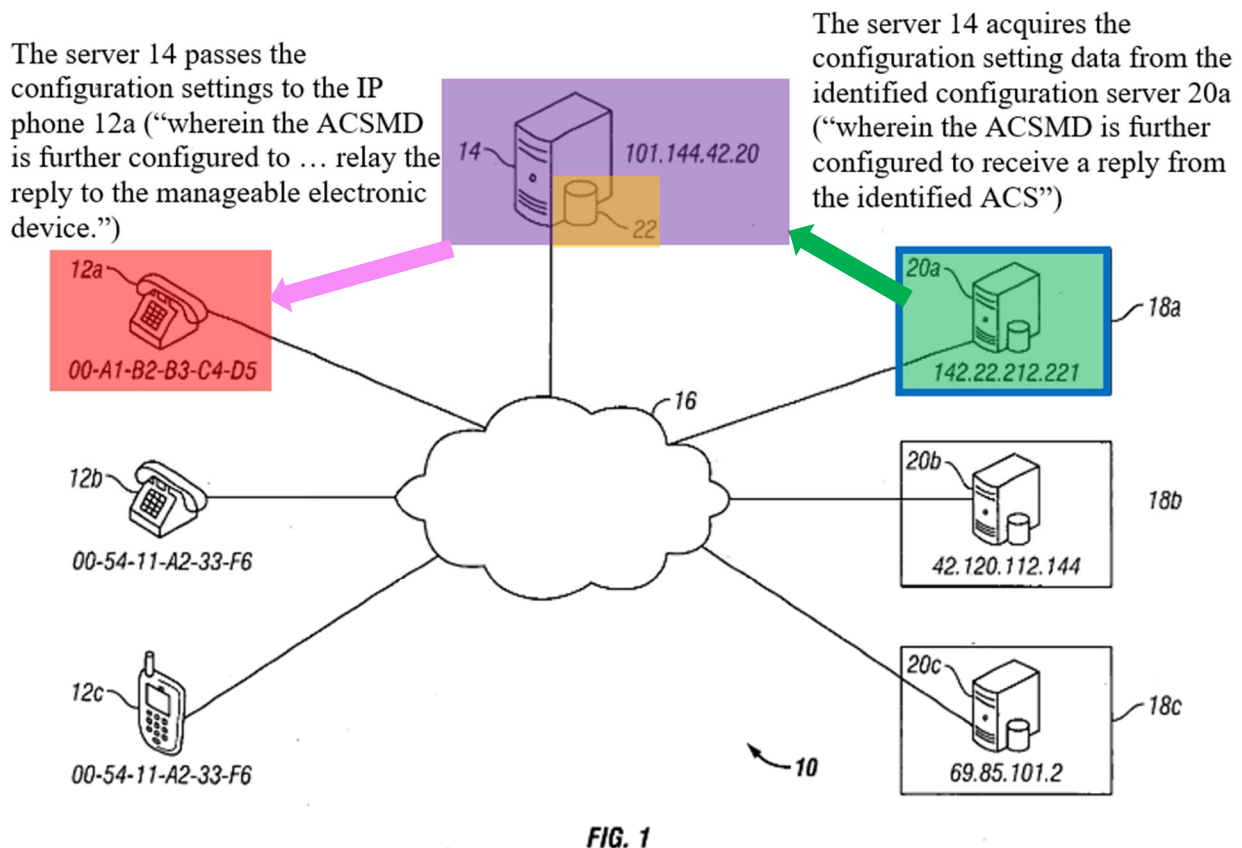


Figure 1 Ex. 1006 (cropped and annotated)

To begin, the red phone “12a is typically identified by its MAC address” and “the configuration files on the configuration server 20a may be named using this information, for example, a configuration file named *iphone12a-mac-00-a1-b2-b3-c4-d5.cfg* would correspond to the IP phone 12 a having *00-a1-b2-b3-c4-d5* as its MAC address.” (Ex. 1006 at ¶52 (emphasis added)). In response to receiving a configuration file named *iphone12a-mac-00-a1-b2-b3-c4-d5.cfg*, the server 14 looks to database 22 to determine the MAC address of the phone where the configuration file will be provided/relayed.

Configuration server 20a sends server 14 a configuration file named “iphone12a-mac-00-a1-b2-b3-c4-d5.cfg”

IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		XX-XX-XX-XX-XX
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		yy.yyy.y.yyy

FIG. 3a

Figure 3a (annotated) Ex. 1006.

Therefore, in my opinion, *Angelot* discloses the features of claim 2.

3. Claim 3

- a) **The system according to claim 1, wherein the ACSMD is further configured to identify the type of the manageable electronic device by comparing a network address of the manageable electronic device in the request with a predetermined plurality of network addresses in the at least one database.**

[0137] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 43.

As per claim 4, claim 2 is incorporated and Angelot further discloses:

- *wherein the auto-configuration server managing device is further arranged for identifying the type of manageable electronic device by comparing a network address of the manageable electronic device in the request with a predetermined plurality of network addresses in the at least one database, (Angelot, Fig. 2:112 and Col. 2:63-67 and Col. 3:1-6).*

Angelot discloses that IP phone 12a's MAC address, which corresponds to "a network address of the manageable electronic device in the request," "includes an encoding comprising six groups of two hexadecimal digits, for example 00-a1-b2-b3-c4-d5" where the "first three octets (in transmission order) 00-a1-b2 identify the manufacturer (or organization) that issued the identifier (and hence the network interface adapter) and are known as the Organizationally Unique Identifier (OUI)." (Ex. 1006 at ¶49).

[0138] An example is shown in the following table:

Aastra (12a)	MATRA (12b)	DeTeWe-Deutsche Telephonwerke (12c)
OUI 00-10-BC	OUI 08-00-71	OUI 00-30-42
Service Provider 18b	Service Provider 18b	Service Provider 18b
First configuration settings	Second configuration settings	Second configuration settings

“As an example, all IP phones 12a from manufacturer A, e.g. Aastra Telecom, Canada, comprise the OUI 00-10-BC, and phone 12b from manufacturer B, e.g. MATRA, France comprise the OUI 08-00-71, and IP phones 12c from manufacturer C, e.g. DeTeWe-Deutsche Telephonwerke, Germany, comprise the OUI 00-30-42.” (Ex. 1006, ¶55.) “The central server 14 thus includes a centralized repository [database 22] having a master table associating all MAC address starting with 00-10-BC, 08-00-71 and 00-30-42, and/or including a range of remaining octets assigned by the manufacturer, to service provider 18b.” (Ex. 1006).

[0139] “Therefore, a single set of resources or configuration settings may be applied to particular OUIs and/or a range of trailing octets, or for a range of MAC addresses, or for a certain class of devices 12a, 12b, and 12c.” (Ex. 1006 at ¶55).

“This arrangement thus allows for all IP phones 12a from manufacturer A with OUI 00-10-BC to receive the same configuration settings, while all IP phones 12b from manufacturer B with OUI 08-00-71 to receive the same configuration settings.” (Ex. 1006). “Thus, when an end user powers on a phone 12b and

connects it to the network 16, the phone 12b immediately connects to the central server 14, which captures the OUI part of the MAC address (08-00-71) and the trailing octets, and refers to the master table to determine whether the MAC address falls within the range of MAC addresses for any of the service providers 18a, 18b, or 18c. The request is subsequently forwarded to the appropriate service provider 18b with configuration server 20b which selects the appropriate configuration settings for the IP phone 12b using the second mapping table, and the configuration settings data is subsequently sent to the IP phone 12b via a suitable protocol.” (Ex. 1006 at ¶55).

[0140] Given these disclosures a person having ordinary skill in the art would have understood that the server 14, which corresponds to the ACSMD, identifies the class of device 12 (whether the manageable electronic device is from manufacturer A or C and what service provider 18 the device should receive configuration data from) by comparing MAC address of the device, e.g., phone 12a’s network address in the request, with the MAC addresses in the database 22. The MAC addresses in the database correspond to the claimed a predetermined plurality of network addresses in the at least one database. Therefore, in my opinion, *Angelot* discloses the features of claim 3.

4. Claim 4

- a) **The system according to claim 3, identifying the type of the manageable electronic device further comprises identifying a service provider based on the network address from a predetermined plurality of service provider identifications associated with the predetermined plurality of network addresses in the at least one database.**

[0141] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 43.

As per claim 4, claim 2 is incorporated and Angelot further discloses:

- *wherein the auto-configuration server managing device is further arranged for identifying the type of manageable electronic device by comparing a network address of the manageable electronic device in the request with a predetermined plurality of network addresses in the at least one database, (Angelot, Fig. 2:112 and Col. 2:63-67 and Col. 3:1-6).*

As I explained for claim 3, the service provider 18a to 18c is identified during the identification of the network device manufacturer A to C. This service provider identification is also based on the network device's MAC address (network address) as I explained previously for claim 3 and claim elements related to Fig. 3a Ex. 1006. I have annotated Figure 3a to show that *Angelot* discloses identifying a service provider based on the network address (IP Device mac address) from a predetermined plurality of service provider identifications (SP 18a to 18x and/or the corresponding configuration server IP addresses) associated with the

predetermined plurality of network addresses (IP Device MAC addresses in the table) in the at least one database

IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		XX-XX-XX-XX-XX
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		yy.yyy.y.yyy

FIG. 3a

Therefore, in my opinion, *Angelot* discloses the features of claim 4.

5. Claim 5

- a) **The system according to claim 4, wherein identifying the ACS from the plurality of ACSs in accordance with the identification of the manageable electronic device further comprises determining a network address of the identified ACS from a predetermined plurality of ACS network addresses in the at least one database.**

[0142] In my opinion, *Angelot* discloses this feature. The USPTO appears to agree. Ex. 1019 at 44.

As per claim 6, claim 5 is incorporated and Angelot further discloses:

- *wherein determining an identification of an auto-configuration server from the plurality of auto-configuration servers in accordance with the identification of the manageable electronic device further comprises determining a network address of the identified auto-configuration server from a predetermined plurality of auto-configuration server network addresses in the at least one database, (Angelot, Col. 2:44-46).*

As I previously explained, the server 14 identifies the appropriate configuration server (ACS) using the Fig. 3a table that associates the network device's identification (IP device MAC address) with the configuration server's IP address (a network address of the identified ACS from a predetermined plurality of ACS network addresses in the at least one database).

IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		XX-XX-XX-XX-XX
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		yy.yyy.y.yyy

FIG. 3a

Therefore, in my opinion, *Angelot* discloses the features of claim 5.

6. Claim 6

- a) **The system according to claim 3, wherein identifying the ACS from the plurality of ACSs in accordance with the identification of the manageable electronic device further comprises determining a network address of the identified ACS from a predetermined plurality of ACS network addresses in the at least one database.**

[0143] In my opinion, *Angelot* discloses this feature for the reasons I explained for claim 5. The USPTO appears to agree. Ex. 1019 at 44-45.

As per claim 7, claim 4 is incorporated and Angelot further discloses:

- *wherein determining an identification of an auto-configuration server from the plurality of auto-configuration servers in accordance with the identification of the manageable electronic device further comprises determining a network address of the identified auto-configuration server from a predetermined*

plurality of auto- configuration server network addresses in the at least one database, (Angelot, Col. 7:51-55).

Specifically, the network address of the identified configuration server (ACS) is shown in Fig. 3a table that associates the network device's identification (IP device MAC address) with the configuration server's IP address (a network address of the identified ACS from a predetermined plurality of ACS network addresses in the at least one database).

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		XX-XX-XX-XX-XX
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		yy.yyy.y.yyy

FIG. 3a

Therefore, in my opinion, *Angelot* discloses the features of claim 6.

7. Claim 10 (cancelled)

a) **[10pre] A computer configured for remote device management,**

[10a] the computer comprising a processing unit and memory, the memory being connected to the processing unit,

[10b] the computer being communicatively coupled to at least one database, a plurality of auto-configuration servers (ACSs), and a manageable electronic device,

[10c] the computer being disposed as an intermediary between the manageable electronic device and the plurality of ACSs for controlling access to the ACSs, the at least one database storing information for the identification of electronic devices;”

[10d] wherein the computer is configured, responsive to receiving a request from a manageable electronic device for configuration data, to:

[10e] identify the manageable electronic device by comparing at least a portion of the request with the information for the identification of electronic devices of the at least one database, and

[10f] identify an ACS from the plurality of ACSs in accordance with the identification of the manageable electronic device to provide configuration data to the manageable electronic device,

[10g] wherein configuration data comprise data for configuring the manageable electronic device, and

[10h] wherein the computer is further configured to relay the request to the identified ACS.

[0144] In my opinion, *Angelot* discloses the features of claim elements

10preample to 10h for the same reasons I discussed above for claim elements 1pre

to 1h. Additionally, *Angelot*'s server 14 corresponds to the claimed "computer" and it has a processor unit, memory, and computer code to perform the features discussed above in claim 1 and required by claim 10. For example, the server 14 includes "data processing means comprising a processor (which may be referred to as a central processor unit or CPU, logic means, or controller) that is in communication with a computer-readable medium having data and/or program code, input/output (I/O) devices, a network interface, and other interfaces." (Ex. 1006 at ¶45). Thus, in my opinion, *Angelot* anticipates claim 10.

8. Claim 11

- a) **The computer according to claim 10, wherein the computer is further configured to relay the request to the identified ACS, receive a reply from the identified ACS, and relay the reply to the manageable electronic device.**

[0145] In my opinion, *Angelot* discloses the features of claim 11 for the same reasons discussed above for claim 2.

9. Claim 12 (cancelled)

- a) **[12pre] A computer program product comprised of instructions stored on a non-transitory computer-readable medium to be read and executed by a computer,**

[12a] the computer comprising a processing unit and memory, the processing unit being connected to the memory and being arranged in a network,

[12b] the computer being communicatively coupled via the network to at least one database, a plurality of auto-configuration servers (ACSs), and a manageable electronic device,

[12c] the computer being disposed as an intermediary between the manageable electronic device and the plurality of ACSs for controlling access to the ACSs;

[12d] wherein the at least one database is configured to store information for identification of electronic devices;

[12e] wherein the computer program product is configured to cause the processing unit to, responsive to receiving a request for configuration data from the manageable electronic device, carry out:

[12f] identifying the manageable electronic device by comparing at least a portion of the request with the information for the identification of electronic devices of the at least one database, and

[12g] identifying an ACS from the plurality of ACSs in accordance with the identification of the manageable electronic device to provide configuration data to the manageable electronic device,

[12h] wherein configuration data comprise data for configuring the manageable electronic device, and

[12i] wherein the computer program product is further configured to cause the processing unit to relay the request to the identified ACS.

[0146] In my opinion, *Angelot* discloses the features of claim elements 12pre to 12i for the same reasons I discussed above for claim elements 1pre to 1h, and claim 10.

10. Claim 14

- a) **The computer program product according to claim 12, wherein the computer program product is further configured to receive a reply from the identified ACS, and relay the reply to the manageable electronic device.**

[0147] In my opinion, *Angelot* discloses the features of claim 14 for the same reasons I discussed above for claim 2.

11. Claim 15 (cancelled)

- a) **[15pre] A method for remote device management of a manageable electronic device in a network,**
- [15a] the network comprising an auto-configuration server managing device (ACSMD),**
- [15b] at least one database storing information for the identification of electronic devices, and**
- [15c] a plurality of auto-configuration servers (ACSs),**
- [15d] the ACSMD being coupled intermediately between the ACSs and the managed electronic device for controlling access to the ACSs, the method comprising the steps of:**
- [15e] the manageable electronic device sending a request for configuration data to the ACSMD via the network, wherein configuration data comprise data for configuring the manageable electronic device, and**
- [15f] responsive to receiving the request, the ACSMD:**
- [15g] identifying the manageable electronic device using a comparison of at least a portion of the request with the information for the identification of electronic devices of the at least one database, and**
- [15h] identifying an ACS from the plurality of ACSs in accordance with the identification of the manageable electronic device to provide configuration data to the manageable electronic device, and**
- [15i] relaying the request to the identified ACS.**

[0148] In my opinion, *Angelot* discloses the features of claim elements

12pre to 15i for the same reasons I discussed above for claim elements 1pre to 1h.

12. Claim 16

- a) **The method of claim 15, further comprising the steps of: the ACSMD receiving a reply from the identified ACS, and relaying the reply to the manageable electronic device.**

[0149] In my opinion, *Angelot* discloses the features of claim 16 for the same reasons I discussed above for claim 2.

B. Ground 2: *Angelot* as Modified by the Knowledge of a person having ordinary skill in the art Discloses Each and Every Feature of Claims 2-6, 11, 14, 16.

[0150] I am informed that Patent Owner may incorrectly contend that the communications between the server 14 and configuration servers 20 are not a disclosure of the ACSMD *relaying* the request to the identified ACS (claim element 1h, 10h, 12i, 15i) or that the server's passing of the configuration file to the network device is not a disclosure of *relaying* the reply from the ACS to the manageable electronic device (claims 2, 11, 14, 16). If the Patent Owner makes that allegation, I disagree. Nevertheless, assuming such an accusation is made and found to have merit, a person having ordinary skill in the art would have found it routine and conventional to modify *Angelot* to relay the request and reply.

[0151] A person having ordinary skill in the art would have understood that relaying messages between a consumer device 12 and a configuration server 20 using a server 14 coupled to the consumer device 12 and configuration server 20 was straightforward, routine, conventional and the predominant manner of sending

information between devices and servers. ***Nothing about “relaying” information from one server to another or from a server to a device is innovative. The ’772 patent admits as much, when it teaches that “relaying” information was known in the prior art.***

The requesting manageable electronic device 1 sends its request to the wide area network WAN. In case the request comprises the IP address of the auto-configuration server manager, the DSLAM transmits the request to the network switch (not shown) that will ***relay the request to the auto configuration server manager (as known in the art).***

(Ex. 1001 at 5:56-61 (emphasis added).)

[0152] Also, as I previously mentioned, Patent Owner asserts that relaying is simply sending or passing. (Ex. 1009 at 54 fn. 10.) In my opinion, a person having ordinary skill in the art would have recognized limited options for supplying the consumer device 12a with configuration data: (1) coding the configuration server’s URI into the device, (2) coding the central server’s URI into the device so that the device can request configuration information from the central server, which will relay the request to the relevant configuration server with sufficient information for the configuration server to reply directly to the device, (3) coding the central server’s URI into the device so that the device can request configuration information from the central server, which will relay the request to the relevant configuration server with sufficient information for the configuration

server to reply to the configuration server, which will then relay the configuration information to the device.

[0153] There is no dispute that the claimed “relay” was known in the art. Moreover, the claimed relaying of “the request to the identified ACS” and relaying of “the reply to the manageable electronic device” is, at most, a predictable variation of *Angelot*’s system. Therefore, in my opinion, a person having ordinary skill in the art would have found it straightforward, routine, conventional, and predictable to modify *Angelot*’s system to relay requests and replies, as claimed.

[0154] Also, as discussed above, device 12a *does not know* the configuration server’s 20a address, but it does know the unique resource identifier (URI) of the central server 14. Therefore, in my opinion, a person having ordinary skill in the art would have recognized that there is a good reason for the central server 14 to “relay” messages between the consumer device 12a and the configuration server 20a—without relaying the requests/replies, the device 12a and configuration server 20a would not be able to communicate. A person having ordinary skill in the art would have readily understood that in response to receiving the request, server 14 must ascertain where to send the request by looking at table 3a stored in database 22. (Ex. 1006 at ¶¶47 (“the central server 14 redirects any configuration related queries from the network entity 12a, 12b, or 12c to the configuration server 20a, 20b, 20c....”))

[0155] A person having ordinary skill in the art would have found it conventional to design *Angelot's* server 14 to match the MAC address of the network device 12a with the corresponding IP address of the configuration server 22a and then relay the network device 12a's request to the configuration server 22a based on the matching/processing performed by the server 14 (see Ex. 1006 at ¶¶51, 54, Fig. 2: steps 104, 106, 110, 112, 114). Such a relaying is an example of server 14 changing, processing, or otherwise managing the request based at least in part on its payload. Of course, the relaying is also an example of simply sending or passing the request from one device 12a to another 20a.

IP Device MAC address	00-A1-B2-B3-C4-D5	00-54-11-A2-33-F6	00-54-11-A2-33-F6		XX-XX-XX-XX-XX
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		YY.YYY.Y.YYY

FIG. 3a

Figure 3a (annotated) Ex. 1006.

Given these disclosures and the knowledge of a person having ordinary skill in the art, modifying *Angelot's* server 14 to relay the network device 12's request for configuration settings after changing/processing that request would have been routine and conventional because it would have ensured that the request is sent/passed to the appropriate configuration server 20a. Also, in my opinion, a

person having ordinary skill in the art would have found it desirable to acquire the correct configuration file from the configuration server identified in table 3a—otherwise, the system would not operate properly. As Ex. 1006 explains at ¶52: “the configuration servers [] are coupled to the central server 14a, such that queries for configuration settings may be redirected [to the configuration servers] based on the first mapping table”. Ex. 1006 goes on to explain in ¶54 that “Upon receipt of the request, the central server 14 *processes* the request to determine whether the first mapping table comprises the unique MAC address associated with the request, and also determines which of the plurality of service providers 18 a, 18 b, 18 c the MAC address belongs to... the central server 14 then redirects the request to an appropriate service provider 18 a, 18 b or 18 c, as per first mapping table (step 114)” such that the configuration server 20 “associated with the appropriate service provider [], selects the configuration settings for the IP phone 12a with that specific MAC address as per second mapping table.”

[0156] In my opinion, a person having ordinary skill in the art would have understood that processing (i.e., modifying) the request before sending it to the proper configuration server would have beneficially provided a mechanism for straightforward and accurate automatic configuration of the network entity 12a “without user intervention except to power-on and connect the at least one network entity to the network in order to contact the central server.” (Ex. 1006 at ¶21). Such

a modification would have been desirable to prevent misconfigurations with improper parameters.

[0157] Additionally, a person having ordinary skill in the art would have been motivated to ensure that the request is relayed to the proper configuration server because *Angelot*'s goal is to ensure that the appropriate configuration settings are provided to the network entity 12a so each of the network entity 12a "is automatically configured without requiring any manual input of settings by the use." (Ex. 1006 at ¶47 and Ex. 1006 at ¶54, cl. 1). In my opinion, such a modification would have been well within the knowledge and skill of a person having ordinary skill in the art. This would have been on more than applying a known technique, i.e., modifying a request before relaying it to its destination, to a known device, i.e., *Angelot*'s server 14, to yield predictable results, i.e., ensuring that the proper configuration server receives the request for configuration settings from the network device 12a. A skilled person would have found, using such techniques as discussed above, a predictable implementation at the time of the invention of the '772 patent. This especially the case in view of *Angelot*'s disclosures and the knowledge of a person having ordinary skill in the art.

[0158] Additionally, modifying server 14 to relay the reply from the configuration server 20a (e.g., "the configuration file named iphone12a-mac-00-a1-b2-b3-c4-d5.cfg") to the network device (manageable electronic device) also

would have been routine and conventional to a person having ordinary skill in the art. I understand that the Patent Owner might argue that *Angelot* does not expressly disclose that server 14 provides the configuration server 20a with the IP address of the requesting device 12a. However, when the configuration server 20a responds to the relevant configuration data, i.e., “a configuration file named *iphone12a-mac-00-a1-b2-b3-c4-d5.cfg*,” it would have been straightforward to modify the server 14 to compare the configuration file name to the IP Device MAC addresses in the database’s table (see Fig. 3a Ex. 1006), determine that the configuration file is intended for the network device 12a based on the table, modify the message from the configuration server 20a to include the network device’s IP/MAC address, and relay the configuration file to the network device based on the IP address obtained from the table (Ex. 1006 at 52 (emphasis added)).

Configuration server 20a sends server 14 a configuration file named “iphone12a- <u>mac-00-a1-b2-b3-c4-d5.cfg</u> ”					
IP Device MAC address	<u>00-A1-B2-B3-C4-D5</u>	00-54-11-A2-33-F6	00-54-11-A2-33-F6		XX-XX-XX-XX-XX
SERVICE PROVIDER ID	SP 18a	SP 18b	SP 18c		SP 18x
Configuration server(s) (IP address)	142.22.212.221 100.232.2.214 72.12.15.32 120.200.45.255 222.48.25.66	42.120.112.144 144.110.212.20	69.85.101.2		yy.yyy.y.yyy

FIG. 3a

Figure 3a (annotated) Ex. 1006.

[0159] A person having ordinary skill in the art would have understood the conventional nature of configuring server 14 to identify the IP address of the intended requesting device based on the configuration file's name and relay the configuration file to the identified IP address. Specifically, a person having ordinary skill in the art reading *Angelot* and using their knowledge, would have found it conventional and straightforward to modify *Angelot*'s server 14 to transmit the configuration file from the configuration server 20a to the network device 12 after modifying the configuration server's message to ensure it is sent to the appropriate network device 12a because it would have been desirable to provide the correct configuration file to the correct network device 12a using the IP MAC address identified in the table 3a.

[0160] Modifying the reply from the configuration server before relaying it to the network device 12a would have beneficially provided a mechanism for straightforward and accurate automatic configuration of the network entity 12a "without user intervention except to power-on and connect the at least one network entity to the network in order to contact the central server." (Ex. 1006 at ¶21). A person having ordinary skill in the art would also have been motivated to ensure that the configuration file is relayed/sent/passed to the proper network entity because *Angelot*'s goal is to ensure that the appropriate configuration settings are provided to the network entity 12a so each of the network entity 12a "is

automatically configured without requiring any manual input of settings by the use.” (Ex. 1006 at ¶47 and Ex. 1006 at ¶54, cl. 1). Such a modification would have been straightforward because it would have amounted to no more than applying a known technique, specifically relaying a reply from one server to a device, to a known device which is *Angelot*’s server 14, to yield predictable results i.e., ensuring that the proper network device 12a receives configuration file it requested.

[0161] Given the disclosures of *Angelot* and the knowledge of a person having ordinary skill in the art, such a skilled person would have found using such techniques as discussed above a predictable implementation at the time of the the application that led to the ’772 patent was filed. For the above-described reasons, in my opinion, the Challenged Claims were known and predictable, given *Angelot*’s disclosures in view of the knowledge of a person having ordinary skill in the art.

[0162] Moreover, *Angelot* discloses that server 14 functions as a “proxy” or an “intermediary.” (Ex. 1006 at ¶62). It would have been straightforward and conventional for a person having ordinary skill in the art to deploy the server 14 as a “proxy” such that it relays a request for information from the red phone 12a to the configuration server and a reply from the configuration server to the red phone 12a.

[0163] I have been made aware that applicant argued during prosecution that a “proxy server” is a server that evaluates (1) requests from clients and (2) responses from the internet to help prevent attackers from invading a private network (see Ex. 1004 at Response dated July 30, 2014, 11-12). In my opinion, a person having ordinary skill in the art would have understood that a “proxy” is “[a] computer (or the software that runs on it) that acts as a barrier between a network and the Internet by presenting only a single network address to external sites. By acting as a go-between representing all internal computers, the proxy protects network identities while still providing access to the Internet.” (Ex. 1011 at, 428). A proxy server is “[a] firewall component that manages Internet traffic to and from a local area network (LAN) and can provide other features, such as document caching and *access control*. A proxy server ... *can filter and discard requests that the owner does not consider appropriate*, such as requests for unauthorized access to proprietary files.” (Ex. 1006 (emphasis added)). Therefore, in my opinion, a person having ordinary skill in the art would have found it routine and conventional to deploy *Angelot*’s server 14 as a proxy server such that only known devices, e.g., devices whose IP Device MAC addresses are in the Fig. 3a table (Ex. 1006), have their requests for configuration data serviced and sent/passed to a configuration server 20. And such that only appropriate configuration files from known configuration servers are sent/passed to the red phone 12a.

[0164] A person having ordinary skill in the art would have been motivated to modify *Angelot's* server in this manner because (1) doing would have prevented unauthorized devices from being configured and would have prevented devices from being configured with malicious configuration data and (2) setting up such a proxy server was well-known at the time of the application that led to the 772 patent was filed and would have provided an extra layer of protection for network providers and their end users. A POSTIA would have been motivated to ensure that *Angelot's* server 14 evaluates (1) requests from the red phone 12a to ensure that unknown devices are not supplied with configuration data and (2) responses from the configuration servers to ensure that attackers do not gain access to the red phone 12a and networks on which it reside. Setting *Angelot's* server as a proxy server would have beneficially provided a firewall that prevented unauthorized devices from obtaining configuration data and nefarious configuration data from being supplied to the red phone 12a, and similar devices.

[0165] In the modified system of *Angelot*, server 14 would process or otherwise manage request for configuration data based on the network device's IP MAC address and its presence in the database 22 (Table in Fig. 3a Ex. 1006). The modified server 14 would also process or otherwise manage replies with configuration data based on the file provided by the configuration server as matched with the network device's IP MAC address in the database 22 (Table in

Fig. 3a; Ex. 1006). Such a modification would have been evident to a POSITA because it would have amounted to no more than applying a known technique (i.e., checking incoming and outgoing messages determining whether or not to relay them) to a known device (i.e., *Angelot*'s server 14) to yield predictable results (i.e., ensuring that only known devices are supplied with configuration data, ensuring that only known devices are having their requests serviced, and ensuring that only known configuration servers are supplying red phone 12a, and similar devices, with configuration files). Given the disclosures of *Angelot* and the knowledge of a person having ordinary skill in the art, such a skilled person would have found using such techniques as discussed above a predictable implementation at the time claimed invention of the '772 patent was conceived.

C. Ground 3: *Angelot* in view of *Zakurdaev* and the Knowledge of a person having ordinary skill in the art Discloses Every Feature of Claims 2-6, 11, 14, 16.

[0166] I am informed that Patent owner may further argue that *Angelot* does not disclose or suggest the claimed relaying, and that a person having ordinary skill in the art would not have been motivated to make such a modification like that discussed in the previous section of my Declaration. I am further informed that the Board might not agree with Patent Owner's position that "relay" means "send" or "pass." Should either event occur, it is my opinion that modifying *Angelot* to include the aforementioned relaying features would have been well-understood,

routine and conventional given the knowledge of a person having ordinary skill in the art, *Angelot* and the disclosures of *Zakurdaev*.

[0167] Like *Angelot*, *Zakurdaev* is directed to facilitating the provisioning configuration data into a consumer device (Ex. 1007 at ¶¶2-11). Given this similarity, a person having ordinary skill in the art would have had reason to consider the teachings of *Zakurdaev* when implementing *Angelot*'s system.

[0168] *Angelot*'s IP phone (12a) has "factory-set default configuration data, such as, DHCP settings (enabled)." (Ex. 1006 at ¶50). And *Zakurdaev* discloses a "Smart DHCP Relay proxy server placed between the user terminal," like *Angelot*'s IP phone 12a, "and the ISP," like *Angelot*'s service provider 18 (Ex. 1007 at ¶12) The DHCP Relay server receives "all IP address requests," determines "the ISP to which the request should be forwarded" and, "based on the user preferences and supplied credentials," sends "the request to the ISP." (Ex. 1007 at ¶12). "[T]he ISP equipment responds" by "generat[ing] an IP address for delivery to the user terminal that generated the request." (Ex. 1007 at ¶12).

[0169] Like the first table (Fig. 3a Ex. 1006) stored in *Angelot*'s proxy server 14, the "Smart DHCP Relay includes a database that maps user equipment (terminal) identity or user account information with a select Internet Service Provider." (Ex. 1007 at ¶14). "[T]he first time the subscriber equipment," e.g., like *Angelot*'s IP phone 12a, "is initialized and connected to the network, the Smart

DHCP Relay receives an IP address request ... generated by the subscriber equipment.” (Ex. 1007) “The IP address request includes an identifier that uniquely identifies the subscriber and/or the subscriber equipment,” thus “the Smart DHCP Relay identifies the select ISP and forwards the address request to it” and the ISP “responds by generating and transmitting an IP address” which is sent to the DHCP Relay that relays the IP address “to the subscriber equipment.” (Ex. 1007 and also Ex. 1007 at ¶¶27, 37, 41, 42, Fig. 2).

[0170] As shown in *Zakurdaev*’s Fig. 2 (which I have annotated below), a user terminal 204 transmits an IP address request (DHCPDISCOVER (red)) to a gateway device 208 (e.g., a router on the network) (see Ex. 1007 at ¶24). The request (red) is provided to a DHCP Relay (Ex. 1007 at ¶25). Like *Angelot*’s server 14, *Zakurdaev*’s DHCP Relay analyzes the request for settings to discover “a terminal MAC address to determine the IP address of the DHCP Server of the corresponding ISP.” (Ex. 1007 at ¶26). The DHCP Relay then relays the DHCPDISCOVER (blue) to the DHCP server at the ISP (Ex. 1007 at ¶27). The ISP 216 then “generates a DHCPOFFER signal [green] that is transmitted back to the Smart DHCP Relay 212.” (see Ex. 1007). Also, “The Smart DHCP Relay 212, upon receiving the DHCPOFFER signal, stores (maps) an IP address for the ISP server 216 to a subscriber MAC address.” (Ex. 1007). After this processing, the

DHCP Relay relays the DHCPOFFER signal (pink) to the terminal 204. (Ex. 1007).

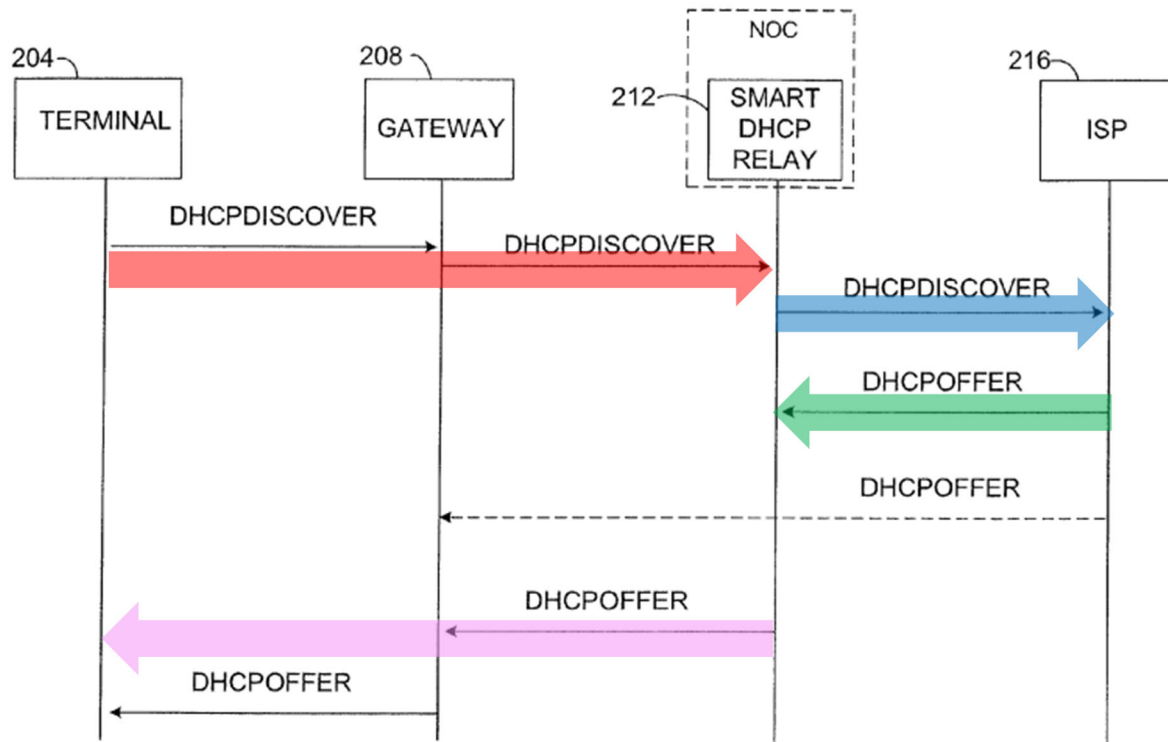


FIG. 2

Figure 2 (annotated) Ex. 1007

[0171] A person having ordinary skill in the art would have been motivated to take these teachings from *Zakurdaev* and apply them to *Angelot* such that *Angelot*'s server 14 can “provide a capability for automatically loading IP addresses into a user’s terminal.” (Ex. 1007 at ¶47). A person having ordinary skill in the art would have understood that such a modification would have facilitated the reduction in “the number of problems that may be encountered and the amount

of time required to” establish “a new account with a new ISP.” (Ex. 1007 at ¶47).

A person having ordinary skill in the art also would have been motivated to make such a modification because it would have freed “technical support resources” for “use in tackling other and perhaps more significant problems.” (see Ex. 1007 at ¶47).

[0172] While *Angelot* discloses the use of DHCP settings for providing initial setup, it does not provide details on how to utilize DHCP communications. Nevertheless, a person having ordinary skill in the art would have understood that DHCP communications was a well-known communication technique in the art. DHCP communications techniques were used in systems for providing configurations settings, as confirmed by *Zakurdaev*. Therefore, a person having ordinary skill in the art would have been motivated based on *Angelot*, *Zakurdaev*, and their knowledge in the art to implement functionality in *Angelot* that relays information between the client (IP phone 12a) and DHCP server (configuration server 20a) using a DHCP Smart Relay, as disclosed in *Zakurdaev*. Such a combined system would have relayed (and sent/passed) the client’s request for configuration data from the DHCP Relay to the DHCP server, and would have relayed the DHCP server’s reply from the DHCP Relay to the client, as required by claim elements 1h, 10h, 12i, 15i and claims 2, 11, 14, 16.

[0173] Given *Zakurdaev*'s teachings and the knowledge of a person having ordinary skill in the art, a person having ordinary skill in the art would have found the above modification to be a predictable approach that would have involved applying basic principles of network communications to configuration systems, such as *Angelot*'s system. In fact, a person having ordinary skill in the art would have understood that DHCP Relay agent in the modified system would have received DHCP messages and then generated a new DHCP message to send out on another (e.g., send the client's request to the configuration server and send the configuration server's reply to the client).

[0174] These basic concepts of the Dynamic Host Configuration Protocol (DHCP), whose details are described in RFC 2131 ("Dynamic Host Configuration Protocol", R. Droms, March 1997) and RFC 2132 ("DHCP Options and BOOTP Vendor Extensions", S. Alexander et al., March 1997), were published by the Internet Engineering Task Force (www.ietf.org). See for example Ex. 1012 at and Ex. 1013 at.

[0175] As known by a person having ordinary skill in the art, a client broadcasts a DHCPDISCOVER message on its local physical subnet. DHCP Relay agent may pass the message on to DHCP servers not on the same physical subnet. A DHCP server may respond with a DHCPOFFER message that includes an available network address. Accordingly, a person having ordinary skill in the art

would have been encouraged to try *Zakurdaev*'s disclosed DHCP communication protocol with a DHCP Relay that relays messages between the client and DHCP server for *Angelot*'s auto-configuration system.

[0176] In my opinion, the use of *Zakurdaev*'s disclosed DHCP Relay for *Angelot*'s server 14 would have been nothing more than the application of a known technique (*Zakurdaev*'s DHCP Relay) to a known device (*Angelot*'s server 14) ready for improvement that would have expectedly resulted in a device communicatively coupled between a client 12a needing configuration data and a configuration server 20a storing the configuration data, which relays communications between the client 12a and configuration server 20a. In my opinion, a person having ordinary skill in the art would have had the knowledge and capability to implement the above-discussed configurations in the combined *Angelot-Zakurdaev* system.

X. CONCLUSION

[0177] In summary, it is my opinion that all of the features recited in claims 2-6, 11, 14 and 16 of the '772 patent are disclosed or suggested by the prior art.

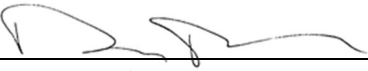
[0178] I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements

Declaration in Support of Petition for *Inter Partes* Review
Patent No. 8,886,772

and the like so made are punishable by fine or imprisonment, or both, under
Section 1001 of Title 18 of the United States Code.

Respectfully submitted,

Dated: February 13, 2023

By: 
Daniel Blumenthal, Ph.D.