

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ERICSSON INC.,
Petitioner

v.

KONINKLIJKE KPN N.V.,
Patent Owner

Case No. IPR2023-00581
Patent No. 8,886,772

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,886,772**

TABLE OF CONTENTS

I.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8.....	1
II.	GROUND FOR STANDING.....	2
III.	INTRODUCTION	3
IV.	OVERVIEW OF THE '772 PATENT	3
	A. Background	3
	B. Purported Invention.....	8
	C. Exemplary Claim.....	12
V.	CLAIM CONSTRUCTION	13
VI.	LEVEL OF ORDINARY SKILL	16
VII.	PRECISE RELIEF REQUESTED AND GROUNDS RAISED.....	16
	A. 35 U.S.C. §325(d) is Inapplicable.....	18
	B. Discretionary Denial Under 35 U.S.C. §314(a) is Unwarranted	19
VIII.	DETAILED EXPLANATION OF GROUNDS.....	19
	A. Ground 1: <i>Angelot</i> Anticipates Claims 2-6, 11, 14 and 16.	20
	1. Claim 1 (cancelled).....	20
	2. Claim 2.....	43
	3. Claim 3	46
	4. Claim 4.....	48
	5. Claim 5.....	49
	6. Claim 6.....	50
	7. Claim 10 (cancelled).....	51
	8. Claim 11	52

Petition for *Inter Partes* Review
Patent No. 8,886,772

9.	Claim 12 (cancelled)	53
10.	Claim 14	54
11.	Claim 15 (cancelled)	54
12.	Claim 16	55
B.	Ground 2: <i>Angelot</i> Renders Obvious Claims 2-6, 11, 14, 16.	55
C.	Ground 3: <i>Angelot</i> in view of <i>Zakurdaev</i> Renders Obvious Claims 2-6, 11, 14, 16.	67
IX.	CONCLUSION.....	72

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	19
<i>Game and Technology Co., Ltd. v. Activision Blizzard Inc.</i> , 926 24 F.3d 1370 (Fed. Cir. 2019)	56
<i>General Plastic Industrial Co., Ltd. v. Canon Kabushiki Kaisha</i> , IPR2016-01357, Paper 19 (PTAB Sept. 6, 2017).....	19, 20
<i>Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson, et al.</i> , No. 2:22-cv-00282-JRG.....	1, 11
<i>Koninklijke KPN NV v. Samsung Electronics America, Inc. et al.</i> , 2-14-cv-01165 (EDTX)	1
<i>Koninklijke KPN NV v. Xiaomi Corporation et al.</i> , 1:21-cv-00041 (DDE)	1
<i>Koninklijke Philips N.V. v. Google LLC</i> , 948 F.3d 1330 (Fed. Cir. 2020)	56
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	61, 63, 66, 72
<i>Merck & Co. v. Biocraft Labs., Inc.</i> , 874 F.2d 804 (Fed. Cir. 1989)	56
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (<i>en banc</i>)	13
<i>Randall Mfg. v. Rea</i> , 733 F.3d 1355 (2013).....	56
<i>Samsung Electronics Co., Ltd. et al. v. Koninklijke KPN NV</i> , PTAB-IPR2016-00808	1

<i>Toyota Motor Corp. v. Cellport Systems, Inc.</i> , IPR2015- 00633	13
<i>Uber Techs., Inc. v. X One, Inc.</i> , 957 F.3d 1334 (Fed. Cir. 2020)	58
<i>Xiaomi Communications Co., Ltd. v. Koninklijke KPN NV</i> , PTAB-IPR2022-00025	1, 2

Statutes

35 U.S.C. § 102(b)	18
35 U.S.C. § 102(e)	16, 18
35 U.S.C. § 103(a)	17
35 U.S.C. §314(a)	19
35 U.S.C. §325(d)	18
35 USC 103	56

Other Authorities

37 C.F.R. § 42.10(b)	2
----------------------------	---

LIST OF EXHIBITS

Ex. 1001	U.S. Patent No. 8,886,772
Ex. 1002	Declaration of Daniel J. Blumenthal, Ph.D.
Ex. 1003	Curriculum Vitae of Daniel J. Blumenthal, Ph.D.
Ex. 1004	Prosecution History of U.S. Patent No. 8,886,772
Ex. 1005	Markman Order from <i>Koninklijke KPN NV v. Samsung Electronics America, Inc. et al.</i> , 2-14-cv-01165-JRG (E.D. Tex.)
Ex. 1006	U.S. Patent Publication No. 2009/0201830 to <i>Angelot</i>
Ex. 1007	U.S. Patent Publication No. 2002/0073182 to <i>Zakurdaev</i>
Ex. 1008	U.S. Patent Publication No. 2003/0061315 to <i>Jin</i>
Ex. 1009	Joint Claim Construction Brief (Dkt. No. 57) filed in <i>KPN v. Xiaomi</i> , 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 <i>KPN v. Xiaomi</i> , 21-cv-00041-GBW-CJB (D. Del. Nov. 28, 2022).
Ex. 1015	An Introduction to Packet Switching (Nick McKeown)

- 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

Ericsson Inc. (“Ericsson” or “Petitioner”) requests *inter partes* review (“IPR”) of claims 2-6, 11, 14, and 16 (the “Challenged Claims”) of U.S. Patent No. 8,886,772 (“the ’772 patent”) (Ex. 1001), which, according to PTO records, is assigned to Koninklijke KPN N.V. (“KPN” or “Patent Owner”). For the reasons set forth below, the Challenged Claims should be found unpatentable and canceled.

I. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8

Real Parties-in-Interest: Petitioner identifies the following as the real parties-in-interest: Telefonaktiebolaget LM Ericsson and Ericsson Inc.

Related Matters: The ’772 patent is asserted against Ericsson in *Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson, et al.*, No. 2:22-cv-00282-JRG.

The ’772 patent was previously at issue in:

- *Xiaomi Corporation, Xiaomi Inc., and Xiaomi Communications Co., Ltd.* in *Koninklijke KPN NV v. Xiaomi Corporation et al.*, 1:21-cv-00041 (DDE) (stayed pending settlement).
- *Koninklijke KPN NV v. Samsung Electronics America, Inc. et al.*, 2-14-cv-01165 (EDTX) (terminated).
- *Samsung Electronics Co., Ltd. et al. v. Koninklijke KPN NV*, PTAB-IPR2016-00808 (not instituted).
- *Koninklijke KPN NV v. u-blox AG et al.*, 1:21-cv-00046 (terminated).

- *Xiaomi Communications Co., Ltd. v. Koninklijke KPN NV*,
PTAB-IPR2022-00025 (claims 1, 7-10. 12. 13 and 15 disclaimed; not
instituted).

Counsel and Service Information:

Petitioners identify lead and backup counsel below. A Power of Attorney is
filed currently herewith under 37 C.F.R. § 42.10(b).

Lead Counsel	Backup Counsel
Scott W. Hejny (Reg. No. 45,882) MCKOOL SMITH P.C. 300 Crescent Court, Suite 1500 Dallas, TX 75201 Telephone: 214.978.4241 Facsimile: 214.978.4044 shejny@McKoolSmith.com Petitioners consent to email service at: Ericsson_KPNII_IPRs@mckoolsmith.com	Nicholas Mathews (Reg. No. 66,067) MCKOOL SMITH P.C. 300 Crescent Court, Suite 1500 Dallas, TX 75201 Telephone: 214.978.4241 Facsimile: 214.978.4044 nmathews@McKoolSmith.com John S. Holley (Reg. No. 65,683) MCKOOL SMITH P.C. 1999 K Street, NW Suite 600 Washington, DC 20006 Telephone: 202.370.8300 Facsimile: 202.370.8300 jholley@McKoolSmith.com

II. GROUNDS FOR STANDING

Petitioner certifies that the '772 patent is available for IPR and Petitioner is
not barred or estopped from requesting IPR on the grounds identified herein.

III. INTRODUCTION

The Challenged Claims are drawn to nothing more than a known system and technique for providing a consumer device with configuration data. The purportedly novel feature in the claims is relaying information from a device to a server and from the server back to the device—“wherein the ACSMD [device] is further configured to *relay the request* to the identified ACS [server]” and wherein the ACSMD is further configured to “*relay the reply* to the manageable electronic device.” (Ex. 1001, cl. 1, 2; *see also* cl. 10, 11, 12, 14-16 (reciting similar features))

But relaying requests and replies was not innovative at the time of the alleged invention. *See, e.g.*, §§IV.A, VIII. The '772 patent even concedes that relaying a request is “known in the art.” (Ex. 1001, 5:56-61 (emphasis added)) In a co-pending district court litigation against another target, KPN argued that “relay” means “send.” (Ex. 1009, 52 fn. 10.) Accordingly, as detailed below, the prior art discussed herein anticipates and/or renders obvious each of the Challenged Claims, either alone or in combination.

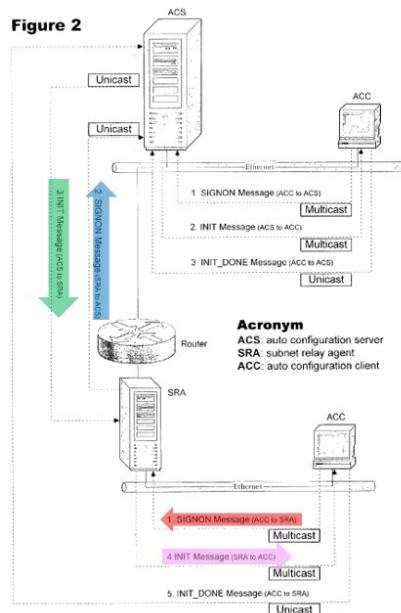
IV. OVERVIEW OF THE '772 PATENT

A. Background

Consumer devices, such as routers, cable set-top boxes, and IP phones, are produced on a production line that gives each device the same operation image. (Ex. 1008 at ¶2.) The devices must undergo a configuration procedure before they can

be fully used by an end user. (*Id.*) In the early 2000s the configuration methods could be “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.” (Ex. 1008 at ¶3.)

Early innovations around improving configuration involved automatic configuration without any user intervention, *e.g.*, plug and play. (*See generally* Ex. 1008; *see also* Ex. 1002, ¶¶69-83.) One early 2000’s disclosure “completely eliminate[d] the need to do any manual configuration on the client side for broadband-based customer devices....” (Ex. 1008, ¶10.) In that system, the administrator uses an auto configuration server (ACS) to configure all of the consumer devices (ACC). (*Id.*; *see also id.*, Fig. 2.)



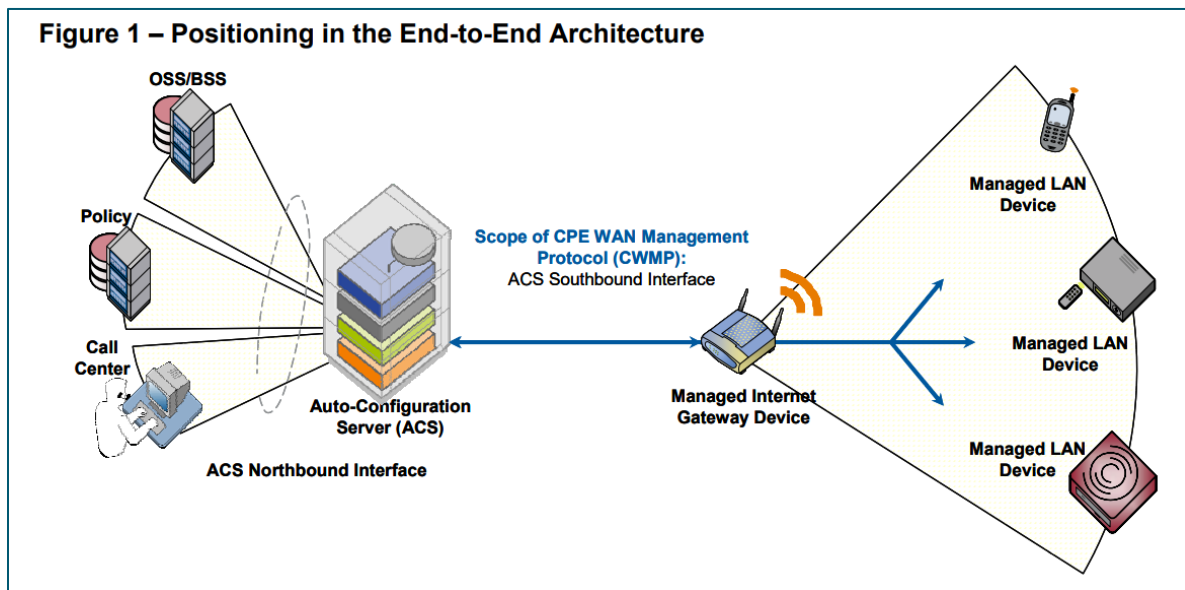
(*Id.*, Fig. 2 (annotated)¹.)

As shown in Figure 2, when a consumer device (ACC) connects to the network it sends a message (red) to a *Relay* Server (SRA) (*id.*, ¶47), the Relay Server relays that message (blue) to an auto-configuration server (ACS) (*id.*, ¶¶48-49), the ACS replies to the Relay Server with a message (green) carrying the configuration data from a configuration database (*id.*, ¶¶51-52), the Relay Server *relays* the message with configuration data (purple) the consumer device (*id.*, ¶53), and the

¹ Throughout this petition, Petitioner uses the same color-coding to show that the claimed signal flow is not innovative.

consumer device configures itself (*id.*, ¶54). (*Id.*, Fig. 2 (annotated above); *see also* Ex. 1002, ¶80-81.)

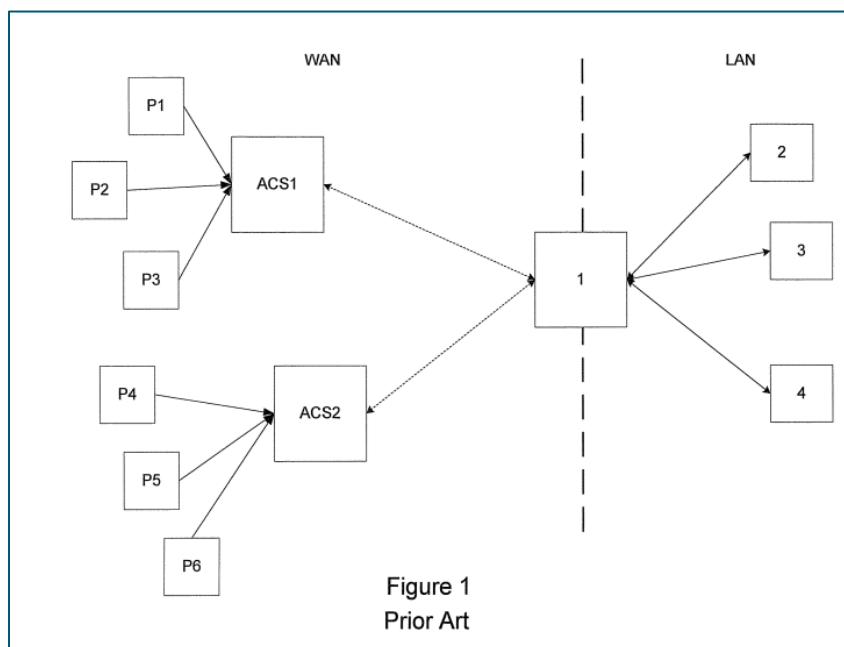
Another known end-to-end architecture for configuring devices is shown in documentation related to the TR-069 communication protocol. (Ex. 1010, 9.)



(*Id.*; *see also* Ex. 1001, Fig. 1 (showing this figure in box form with multiple ACSs).)

In this system, the CPE is preloaded with the IP address of the ACS server that provides the configuration information.

The '772 patent admits that the above-described end-to-end architecture for remote device management (reproduced in Figure 1) is from the prior art. (Ex. 1001, 3:61-62.)



(*Id.*, Fig. 1.) In this architecture, the “ACS is a server that resides in the network and manages devices in or at the subscriber premises.” (Ex. 1010, 9.)

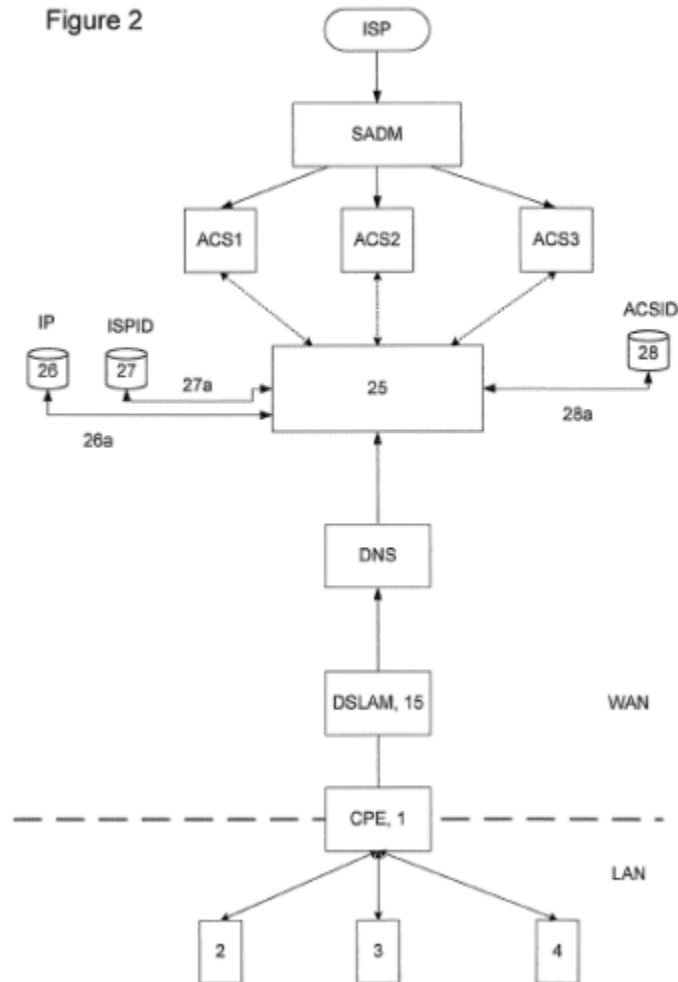
The '772 patent describes a drawback with known configuration technology—it requires each CPE to be pre-configured with the address for the proper ACS. (Ex. 1001, 1:46-53.) The '772 patent explains that there are two known techniques for providing the CPE with the appropriate ACS contact information.

First, the CPE is “pre-programmed” with either a specific IP address or a specific URL for the ACS. (*Id.* 1:53-56.) Second, the CPE is configured with the ACS’s address or URL during installation. (*Id.*, 1:56-60.) As discussed above, it was also known 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. (Ex. 1008, ¶10.)

B. Purported Invention

To overcome the “pre-configuration” problem where the CPE must know the ACS’s address or URL beforehand, the ’772 patent provides a management device between the ACS and CPE to facilitate communication between the ACS and CPE. The ’772 patent calls this management device the “auto-configuration server managing device” (“ACSMD”). (Ex. 1001, Abstract). By virtue of this ACSMD, the ’772 patent purports to improve upon prior art systems by allowing configuration of “any type of manageable electronic device ... without pre-configuring a dedicated address for configuration.” (*Id.* at 2:22–25.)

As shown in Figure 2 of the ’772 patent, reproduced below, there is an ACSMD 25 between the CPE (1 to 4) and ACS1, ACS2, and ACS3.

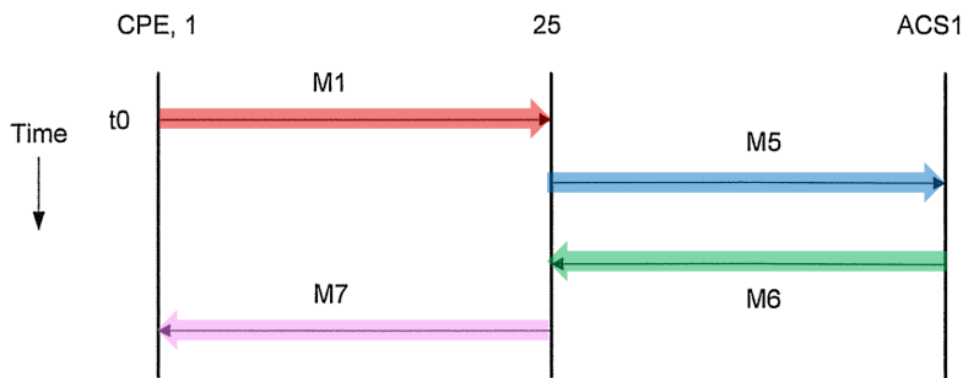


(Ex. 1001, Fig. 2.) As depicted in Figure 2, CPE 1 is communicatively coupled to the ACSMD 25. ACSMD 25, in turn, is arranged for controlling CPE 1's access to the ACSs, *e.g.*, ACS1, ACS2, ACS3. (*Id.*, 5:8–10.)

As depicted in annotated Fig. 5 (below), the CPE 1 sends a first message M1 (red) to the default IP address/URL provided in the CPE 1's memory. (*Id.*, 7:53-63.) This default IP address/URL points to the ACSMD 25. (*Id.*) The first message M1 “comprises a request for configuration data from the dedicated auto-configuration server.” (*Id.*, 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.” (*Id.*, 7:65-8:3.)

Figure 5



(*Id.*, Fig. 5 (annotated).) The “first message M1 [red] 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] to the dedicated auto configuration server ... if the first message M1 contains a valid request.” (*Id.*, 8:4-12.) “The first relayed message M5 [blue] comprises at least the request from the requesting manageable electronic device 1.” (*Id.*, 8:12-14.) “Next, the dedicated auto-configuration server ACS1 ... receives the first relayed message M5.” (*Id.*, 8:20-21.) “In response, the dedicated auto-configuration server ACS1 transmits a reply M6 [green] to the first relayed message to the auto configuration server

manager 25.” (*Id.*, 8:21-24.) “The reply M6 [green] 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].” (*Id.*, 8:25-31.) “The second relayed message M7 [pink] comprises the configuration data requested by the manageable electronic device.” (*Id.*, 8:32-33.)

The ’772 patent describes the communication flow in Fig. 5 as advantageously allowing any type of 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.” (*Id.*, 2:22-32.).

During prosecution, Applicant overcame prior art by arguing that “relaying” a message is different from “forwarding” a message. (Ex. 1004, 21-62, 85-87). In another litigation, however, *KPN* argued that “*relay*” means “*send*.”

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

(Ex. 1009, 52 fn. 10.) *KPN* provided the following annotated figure to support its assertion that “relay” means “send.” In *KPN*’s view, the issue is “no more complicated than ... the message is *passed* from one device to another....” (*Id.*, 55 (emphasis added).) As detailed below, sending/passing/relaying a message or reply is not innovative.

C. Exemplary Claim

Patent Owner previously cancelled independent claims 1, 10, 12, and 15. Patent Owner also cancelled dependent claims 7-9, and 13. Claim 2 is exemplary of claims 11, 14 and 16, and recites:

1. A system for remote device management comprising:
a plurality of auto-configuration servers (ACSs);
a manageable electronic device;
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
at least one database communicatively coupled to the ACSMD and storing information for the identification of electronic devices,
wherein the manageable electronic device is configured to send a request for configuration data to the ACSMD,²
wherein configuration data comprise data for configuring the manageable electronic device, and
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

² This request is “M1” in Fig. 5.

wherein the ACSMD is further configured to **relay** the request to the identified ACS.³

2. The system according to claim 1, wherein the ACSMD is further configured to receive a reply from the identified ACS,⁴ and **relay** the reply to the manageable electronic device.⁵

V. CLAIM CONSTRUCTION

For IPR proceedings, the Board applies the claim construction standard set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). Under *Phillips*, claim terms are typically given their ordinary and customary meanings, as would have been understood by a POSITA, at the time of the invention, having taken into consideration the language of the claims, the specification, and the prosecution history of record. *Phillips*, 415 F.3d at 1313; *see also Id.* at 1312-16. The Board, however, only construes the claims when necessary to resolve the underlying controversy. *Toyota Motor Corp. v. Cellport Systems, Inc.*, IPR2015- 00633, Paper 11 at 16 (Aug. 14, 2015) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). Several claim terms have previously been construed by a district court, as summarized in the following table:

Term	Construction
Preamble	limiting

³ The relayed request is “M5” in Fig. 5.

⁴ This reply is “M6” in Fig. 5.

⁵ This reply is “M7” in Fig. 5.

	(Ex. 1005, 38)
“manageable electronic device”	“electronic device that can be configured over a network” (<i>Id.</i> , 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” (<i>Id.</i> , 46.)
“auto-configuration server managing device (ACSMD)”	“hardware and/or software that relays configuration requests to the auto-configuration servers” (<i>Id.</i> , 48.)
“computer” and “processing unit”	“plain meaning” (<i>Id.</i> , 51.)
“controlling access”	“remaining in contact with the manageable electronic device and the ACS, and controlling whether the manageable electronic device gains access”

	(<i>Id.</i> , 54.)
“configuration data” and “configuration data comprises data for configuring the manageable electronic device”	“plain meaning” (<i>Id.</i> , 57.)
“request for configuration data” and “request from a manageable electronic device for configuration data”	“plain meaning” (<i>Id.</i> , 59.)
“relay” ⁶	“change, process, or otherwise manage a request based at least in part on its payload.” (<i>Id.</i> , 61.)

Here, given the close correlation and substantial identity between the references, the '772 patent, and the terms listed in the above table, the Board need not construe any of the terms listed in the above table to resolve the underlying controversy, as any reasonable construction reads on the prior art. Nonetheless, out of an abundance of caution, Petitioner analyzes the Challenged Claims under the

⁶ 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”).)

plain meaning of the terms listed in the above table, under the district court constructions discussed in this Section, and under KPN's current understanding that "relay" means "send" or "pass."

VI. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art at the time of the alleged invention of the '772 patent ("POSITA"), which for purposes of this proceeding is the late 2000s (including July 31, 2008), would have had a B.S. in Electrical Engineering or a related field with at least five years of experience in designing communication systems. (Ex. 1002, ¶¶34-39.)⁷ More education can supplement practical experience and *vice versa*. (*Id.*)

VII. PRECISE RELIEF REQUESTED AND GROUNDS RAISED

Claims 2-6, 11, 14, and 16 should be cancelled based on the following grounds:

Ground 1: Claims 2-6, 11, 14, and 16 are unpatentable under pre-AIA 35 U.S.C. § 102(e) as being anticipated by *Angelot* (U.S. Patent Publication No. 2009/0201830) (Ex. 1006);

⁷ Petitioner submits the declaration of Dr. Blumenthal (Ex. 1002), an expert in the field of the '772 patent. (Ex. 1002, ¶¶3-18, 40-84; Ex. 1003.)

Ground 2: Claims 2-6, 11, 14, and 16 are unpatentable under pre-AIA 35 U.S.C. § 103(a) as being obvious in view of *Angelot* and the knowledge of a POSITA.

Ground 3: Claims 2-6, 11, 14, and 16 are unpatentable under pre-AIA 35 U.S.C. § 103(a) as being obvious in view of *Angelot* and *Zakurdaev* (U.S. Patent Publication No. 2002/0073182) (Ex. 1007);

The '772 patent issued from U.S. Application No. 12/512,242 (“the '242 application”) filed July 30, 2009 and claims the benefit of European Patent Application EP 08013735.9, filed in the European Patent Office on July 31, 2008, and to European Patent Application EP08161850.6, filed in the European Patent Office on August 5, 2008. (Ex. 1001, Cover) For purposes of this proceeding, Petitioner assumes the earliest effective filing date of the '772 patent is July 31, 2008.⁸

Angelot was filed on October 26, 2007, and claims priority to a provisional application filed on October 31, 2006. *Angelot* published on August 13, 2009. Thus,

⁸ Petitioner does not concede that any challenged claim is, in fact, entitled to an effective filing date of July 31, 2008, and reserves the right to challenge any claim of priority in this or any other proceeding involving the '772 patent.

Angelot qualifies as prior art to the '772 patent at least under pre-AIA § 35 U.S.C. § 102(e). *Zakurdaev* published on June 13, 2002. Thus, *Zakurdaev* qualifies as prior art to the '772 patent at least under pre-AIA § 35 U.S.C. § 102(b). None of the references being relied upon in this petition were considered by the Patent Office during prosecution of the '772 patent. (*See generally* Ex. 1001, References Cited.)

A. 35 U.S.C. §325(d) is Inapplicable

These references were not in an IDS filed during the prosecution of the '772 patent, and the Examiner never identified them or used them to reject claims during the prosecution. (*See generally* Exs. 1001 (cover), 1004.) The Examiner also never considered the testimony of Petitioner's expert, Dr. Blumenthal (Ex. 1002), regarding these references and the knowledge of a POSITA. The grounds in this petition are not cumulative of any prior art the Board considered and are not substantially the same as prior art or arguments the Office previously considered. In fact, the principal references disclose the claimed "relay" features the patentee used to distinguish the prior art cited by the Examiner. (Ex. 1004, 21-62, 85-87.) Neither the petition Samsung filed six years ago (IPR2016-00808) nor the petition Xiaomi filed last year (IPR2022-00025) asserted *Angelot* or *Zakurdaev*. Thus, 35 U.S.C. §325(d) is inapplicable to this case.

B. Discretionary Denial Under 35 U.S.C. §314(a) is Unwarranted

The co-pending district court litigation does not warrant the exercise of discretion under 35 U.S.C. §314(a). *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020). Petitioner intends to seek a stay of the district court litigation if the PTAB decides to institute this IPR. And the parties only recently had a scheduling conference, where jury selection was tentatively set for April 1, 2024. The earlier Xiaomi and Samsung petitions also do not warrant the exercise of discretion under 35 U.S.C. §314(a). *See General Plastic Industrial Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 (PTAB Sept. 6, 2017). Patent Owner did not assert the '772 patent against Petitioner until 2022, and that assertion is why Petitioner is now filing this petition. Thus, the Board should not deny institution of this petition under §314(a).

VIII. DETAILED EXPLANATION OF GROUNDS

Notably, during prosecution of a subsequent and related patent application with substantially similar claims to those at issue here, the USPTO's Office of Patent Quality Assurance (OPQA) identified a version of *Angelot*'s disclosure that resulted in an earlier Notice of Allowance being withdrawn. (Ex. 1019, 67; Ex. 1002, ¶¶98-100.) The Examiner subsequently rejected the nearly identical claims in view of *Angelot* and a secondary reference that was relied upon for the concept of relaying a message. (*Id.*, 41-45.) In response, Applicant did not dispute the Examiner's

characterizations of *Angelot*, which largely align to the mappings below. (*Id.*, 28-31.) Instead, Applicant argued against the Examiner’s combination. (*Id.*) The primary difference between the Examiner’s mapping of *Angelot* and the mapping set forth below in Ground 1 is whether *Angelot* discloses the claimed relaying. At the time of the *Angelot* rejection in the subsequent application, the Examiner did not have the Eastern District’s construction of “relay” or KPN’s litigation read of “relay,” which is simply “send.” With the benefit of the construction and/or KPN’s litigation understanding of “relay,” the Examiner would have rejected the claims as anticipated as set forth below. And, in any event, relaying is not an inventive feature, as the ’772 patent admits, and (if necessary) it would have been obvious to modify *Angelot* to include relaying as set forth in Grounds 2 and 3.

A. Ground 1: *Angelot* Anticipates Claims 2-6, 11, 14 and 16.

1. Claim 1 (cancelled)

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

Angelot discloses this feature. (Ex. 1002, ¶¶98-106; *see also* Ex. 1019, 41.) For instance, *Angelot* discloses a system for “configuring network entities with the requisite settings in order to participate within a network.” (Ex. 1006, ¶3.) This is an example of a “system for remote device management.” *Angelot* discloses that the remote configuration is automatic, unlike prior art 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.” (*Id.*, ¶7.)

To overcome the prior art problem of manual configuration, *Angelot* discloses a system 10 for “automatically configuring at least one network entity,” e.g., a network device 12a to 12c, such as the phone 12a⁹ (red in annotated Fig. 1 below), where the phone 12a is “associated 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. (*Id.*, ¶¶11-15.)

⁹ 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-top boxes, game consoles, gateways, soft phones, firewalls, access-points, modems, network appliances, or any combination(s) thereof”).)

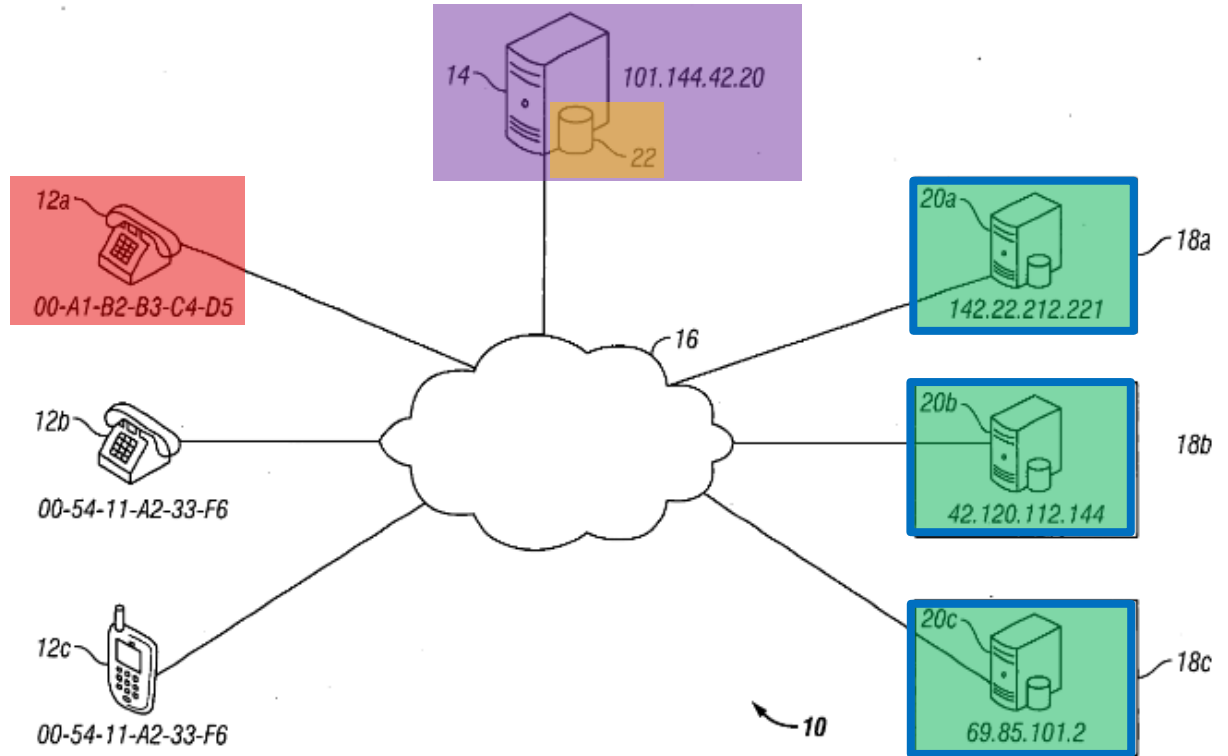


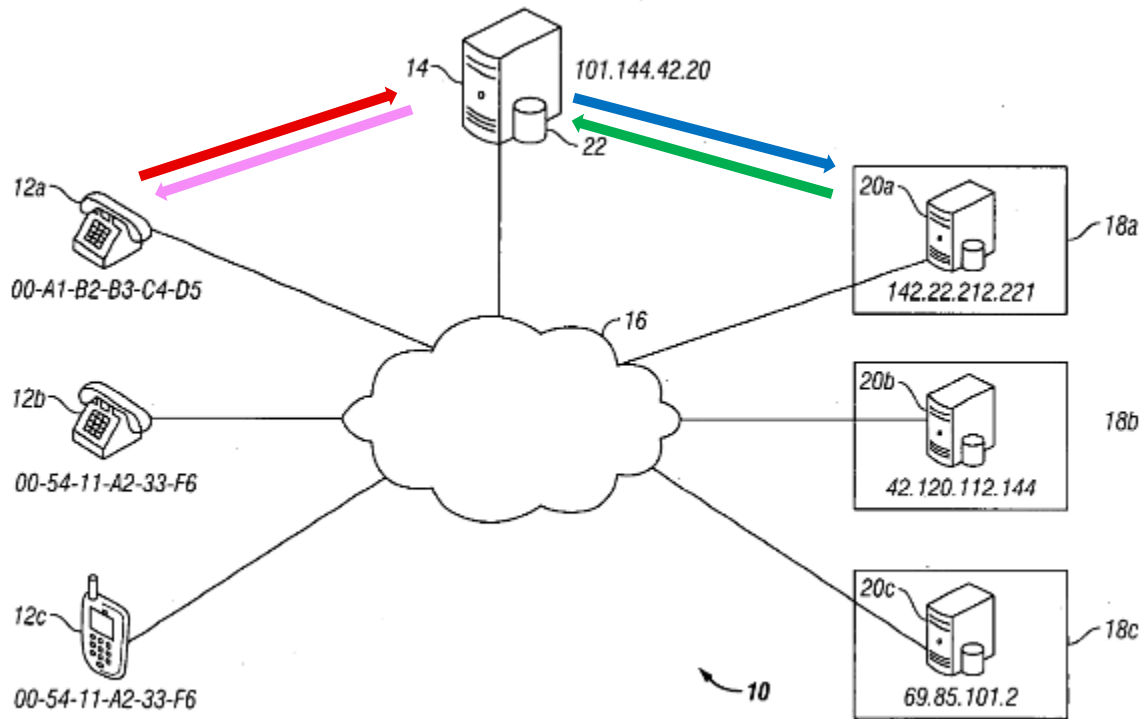
FIG. 1

(*Id.*, Fig. 1 (annotated).)

To make the configuration automatic, the network entity, e.g., “the IP phone 12a” (red), is “included with factory-set default configuration data, such as, DHCP settings (enabled), a URI to a central server 14 [purple] having information related to the IP phone 12a’s configuration settings.” (*Id.*, ¶50.) Specifically, “[t]he IP phone 12a [red] 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].” *Id.* The central server 14 (purple) controls access to the various service providers 18 [blue] and their corresponding configuration server’s 20 [green]. (*Id.*).

“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 “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.” (*Id.*, ¶51.) Thus, *Angelot* discloses the features of claim element 1pre. And, like the ’772 patent, *Angelot* advantageously 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. (Ex. 1006, ¶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.”))

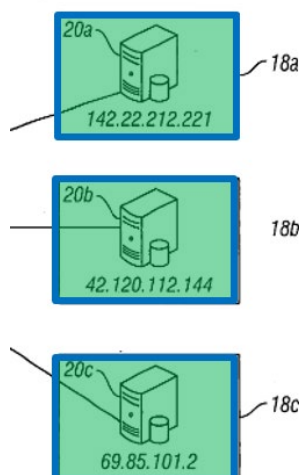
As shown in annotated Fig. 1 (below) and discussed in more detail for claim elements 1e, 1h and 2, *Angelot*’s IP phone 12 sends a message (red) to the central server 14, the central server 14 relays that message (blue) to the relevant configuration server 20, the relevant configuration server replies (green) with configuration information, and the central server 14 relays the configuration information (pink) to the IP phone 12.



(*Id.*, Fig. 1 (annotated).)

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

Angelot discloses this feature. (Ex. 1002, ¶¶98-100, 107-110; *see also* Ex. 1019, 41.) For instance, as shown below, *Angelot* discloses a plurality of service providers 18a to 18c (blue) each having a configuration server 20a to 20c (green).



(*Id.*, Fig. 1 (excerpted and annotated).) Each configuration server 20a to 20c corresponds to an auto-configuration server (ACS). (*Id.*, ¶52 (“The configuration server 20a, 20b or 20c includes configuration settings specific to the IP phone 12 a with specific MAC addresses.”).)

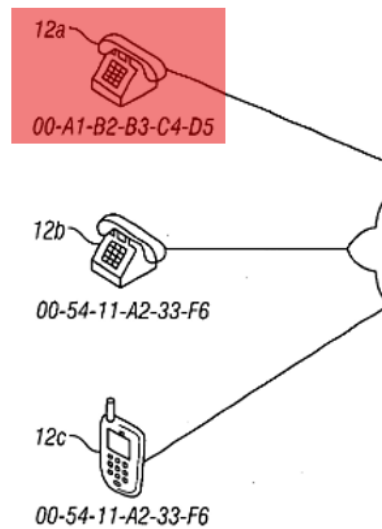
Configuration settings for the network entities 12 are stored on the configuration servers 20. For example, “each IP phone 12a is typically identified by its MAC address,” so “the configuration files on the configuration server 20a may be named using this information, for example, *a configuration file 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.*” (*Id.*, 52 (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.” (*Id.*)

Given that the configuration settings are stored on the configuration servers, the configuration servers 20a to 20c meet the district court’s construction of “two or more systems of hardware and/or software, each of which is capable of automatically configuring a manageable electronic device.” (Ex. 1005, 46.) For instance, “the configuration settings” stored by the configuration servers 20a to 20c “are provided to the network entity 12a, 12b, or 12c, and so each of the network entities 12a, 12b, or 12c is automatically configured without requiring any manual input of settings by the user.” (Ex. 1006, ¶47.) Thus *Angelot* discloses a plurality of ACSs as required by claim element 1a.

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

Angelot discloses this feature. (Ex. 1002, ¶¶98-100, 111; *see also* Ex. 1019, 41.) For instance, *Angelot* discloses a network entity 12a, which may be a mobile phone, set-top box, gateway, etc. (*Id.*, ¶43.) The network entity 12a, such as an IP phone (red), corresponds to the claimed “manageable electronic device.”



(*Id.*, Fig. 1 (excerpted and annotated).) This device is a manageable device because it requests “configuration settings from the central server 14” and, eventually, “the configuration settings are provided to the network entity 12a” so that it is “automatically configured without requiring any manual input of settings by the user.” (*Id.*, ¶¶46-47.) In other words, this device is an “electronic device that can be configured over a network” as required by the district court claim construction. (Ex. 1005, 42.) Thus, *Angelot* discloses the features of claim element 1b.

- 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**

Angelot discloses this feature. (Ex. 1002, ¶¶98-100, 112-114; *see also* Ex. 1019, 41.) For instance, *Angelot* discloses re-direct server 14 (purple), that 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).

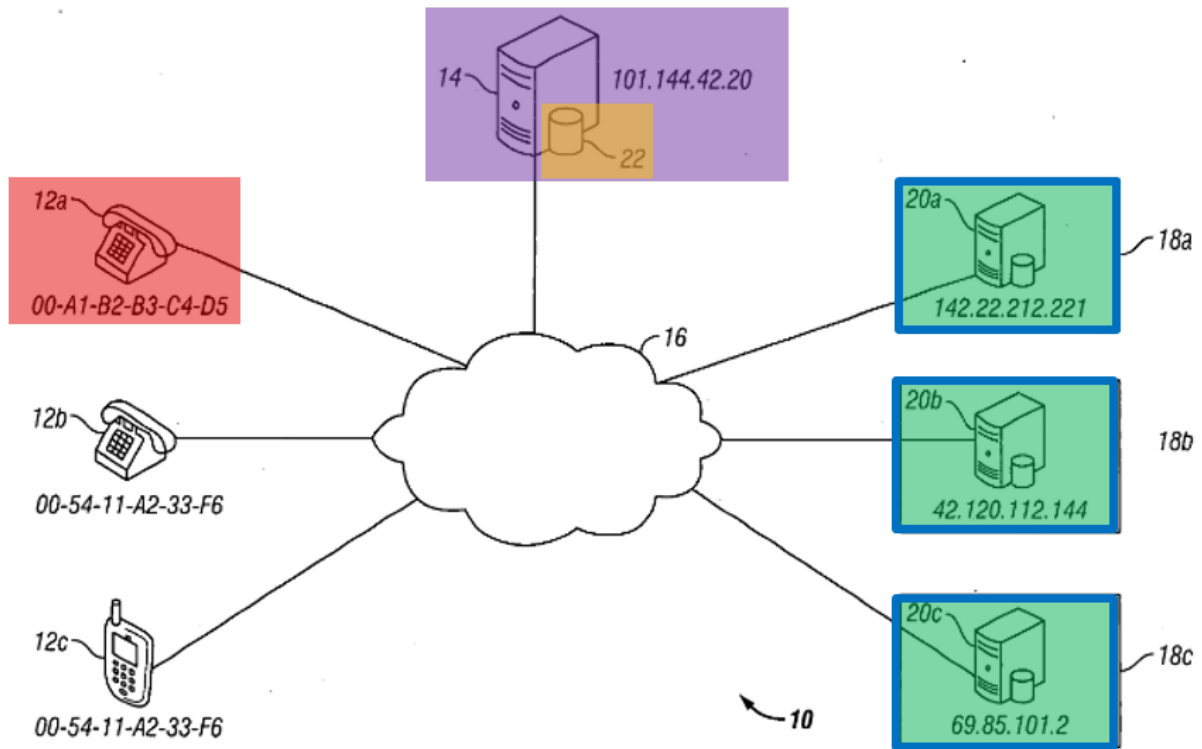


FIG. 1

(Ex. 1006, Fig. 1 (annotated).) Specifically, the “server 14 [purple] redirects any configuration related queries from the network entity 12a, 12b, or 12c [red] to the configuration server 20a, 20b, 20c [green],” and this redirecting is “based on the identity of the network entity 12a, 12b, or 12c.” (*Id.*, ¶47.)

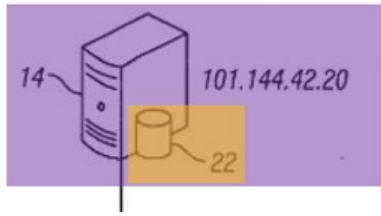
“Upon receipt of the request, the central server 14 [purple] processes the request to ... determine[] which of the plurality of service providers 18a, 18b, 18c [blue] the MAC address belongs to. Once such a determination has been established, the central server 14 [purple] then *redirects the request 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....” (*Id.*, ¶54.) Thus, 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, 48.)

Given that the server 14 (purple) *processes* the requests based on the network entity’s MAC address and directs the requests to the relevant service provider/configuration server (blue/green), the server 14 (purple) controls whether the IP phone 12a (red) gains access to the configuration servers 20 (green). (Ex. 1006, ¶54.) The server 14 (purple) also remains in contact with the IP phone 12a (red) and the configuration servers (green) via the network 16. Thus, the server 14 (purple) controls access to the configuration servers (green) in the manner required by the district court’s construction of “controlling access.” (Ex. 1005, 54.) Thus, *Angelot* discloses the features of claim element 1c.

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

Angelot discloses this feature. (Ex. 1002, ¶98-100, 115; *see also* Ex. 1019, 41.) For instance, *Angelot* discloses database 22 (orange) communicatively coupled to the central server 14 (purple).



(Ex. 1006, Fig. 1 (excerpted and annotated).) The database 22 corresponds to the claimed “at least one database.” The “server 14 [purple] includes a database 22 [orange] for storing the records of the MAC addresses and the associated service provider 18a, 18b, or 18c, such as a first mapping table ..., as shown in FIG. 3a.” (*Id.*, ¶51.) Thus, *Angelot* discloses “at least one database” 22 “communicatively coupled to the ACSM[D],” i.e., the database 22 (orange) is included in the server 14 (purple) and is used by the server 14 (purple) 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

(*Id.*, Fig. 3a.) As shown in Fig. 3a, the database 22 stores IP Device MAC addresses, e.g., “information for the identification of electronic devices,” and corresponding configuration server IP addresses. Thus, *Angelot* discloses the features of claim element 1d.

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

Angelot discloses this feature. (Ex. 1002, ¶¶98-100, 115; *see also* Ex. 1019, 41.) For instance, *Angelot* discloses that “the IP phone 12a [red] ... transmit[s] a first signal to request configuration settings associated with the IP phone 12a []from the central server 14,” which “receives a request for configuration settings from the IP phone 12a” including the phone’s “identity data” such as its “unique MAC address.” (*Id.*, ¶54.) In other words, the IP phone 12a (a manageable electronic device) sends a request for configuration settings (a request for configuration data) to the server 14 (ACSMD). (*Id.*)

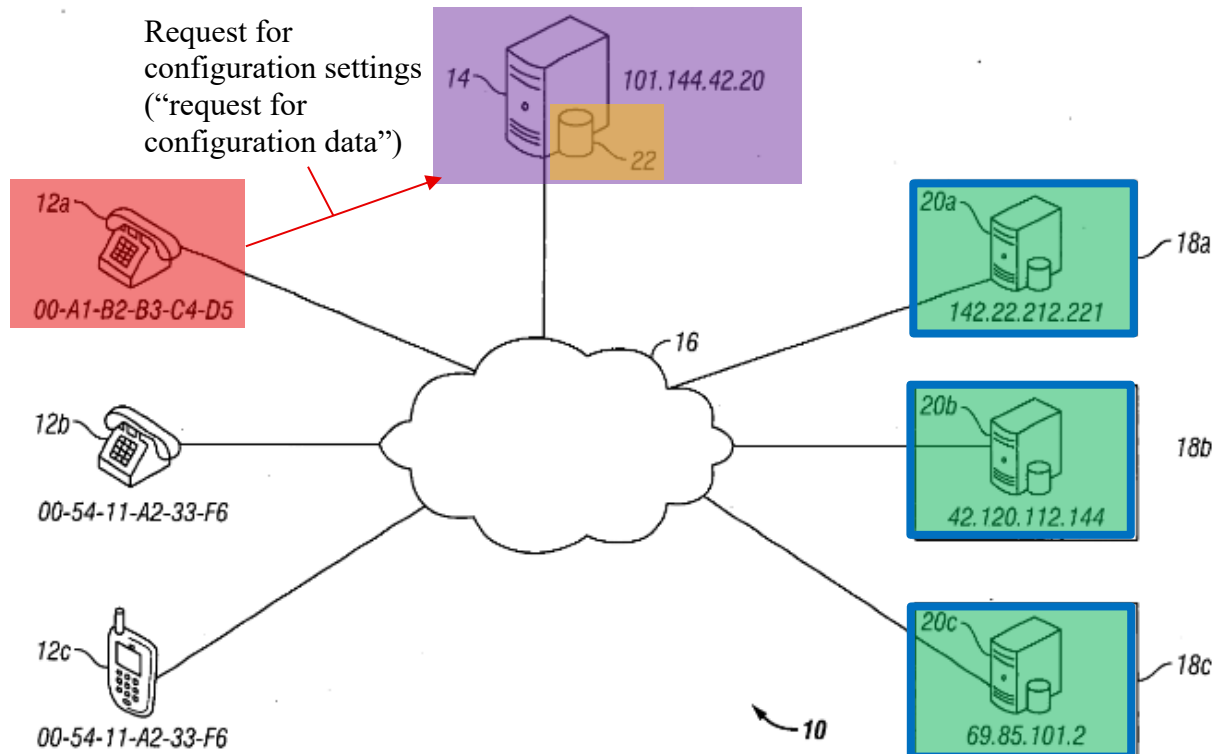


FIG. 1

(*Id.*, Fig. 1 (annotated); *see also id.*, Fig. 2 (110 – “cause the network entity 12a to automatically request configuration settings from the central server 14 via the URI” that is included in the entity’s software (102).) Thus, *Angelot* discloses the features of claim element 1e.

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

Angelot discloses this feature. (Ex. 1002, ¶¶98-100, 117-20; *see also* Ex. 1019, 41-42.) For instance, *Angelot* discloses that the network device 12a “is auto-configured in the background and without user input.” (*Id.*) This auto-configuration is a result of the configuration data from the configuration server 20 of a service provider 18. Specifically, 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.” (*Id.*, ¶52.)

Since the configuration settings are associated with a specific device’s MAC address, the configuration settings are for configuring that device. (*See, e.g., id.*, ¶54 (“service provider 20a, 20b or 20c, selects *the configuration settings for the IP phone 12a* with that specific MAC address...”) (emphasis added); ¶55 (“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); ¶62 (“[T]he redirect server 14 serves as ... [an] intermediary,¹⁰ 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 12a.”)

Thus, the configuration settings data corresponds to the claimed “configuration data” that includes “data for configuring the manageable electronic device.” For instance, “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.” (*Id.*, ¶52.) “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,

¹⁰ 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, 6:63-7:3; *see also id.*, 8:4-14.)

XML services and applications, SIP registration information, usernames and passwords, phone book directory, speaker volume settings and so forth.” (*Id.*)

Accordingly, *Angelot* discloses the features of claim element 1f.

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

Angelot discloses this feature. (Ex. 1002, ¶¶98-100, 121-126; *see also* Ex. 1019, 41.) To begin, the server 14 (ACSMD) receives a request for configuration data as discussed above with respect to claim elements 1e and 1f. As shown in Fig. 2, the network entity 12a (manageable electronic device) “automatically request[s] configuration settings from the central server 14 (ACSMD) via the URI” and the server 14 (ACSMD) processes the request to determine the corresponding service provider 18a and “redirect[s the] request to [the] appropriate configuration server 20a.”

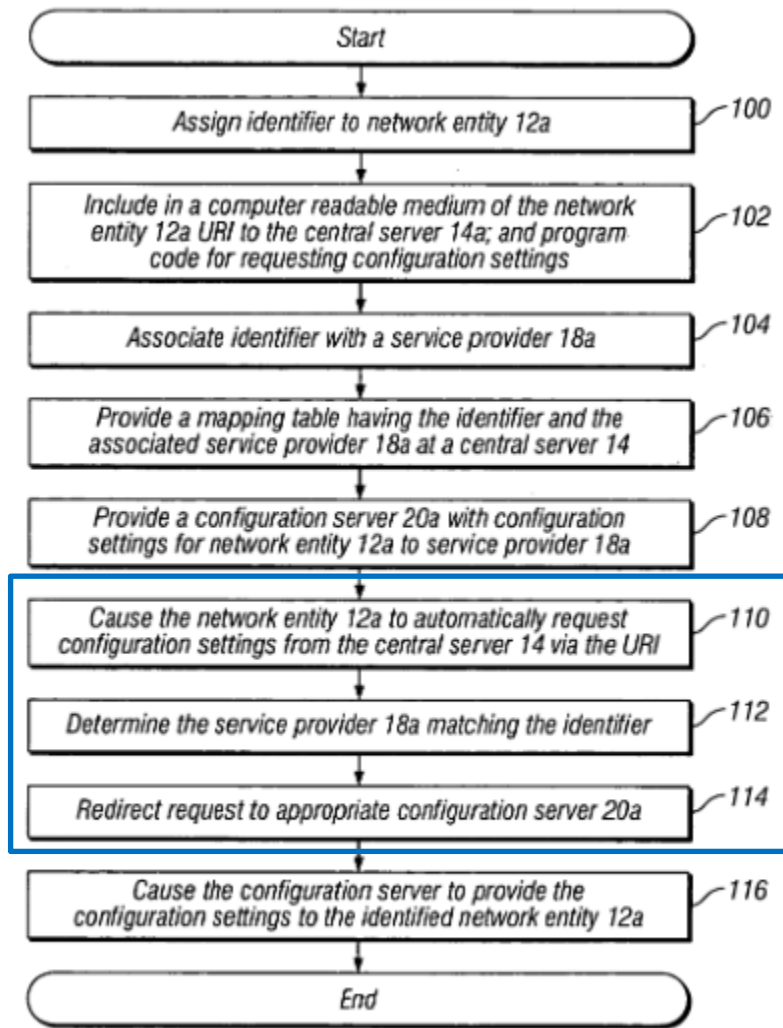


FIG. 2

(*Id.*, Fig. 2 (step 110); *see also id.*, ¶54 (describing steps 110 o 114).)

The server 14 “receives a request for configuration settings from the IP phone 12a,” and the “request includes the identity data of the IP phone 12a, such as the unique MAC address.” (Ex. 1006, ¶54.) In response to receiving that request, the server 14 (ACSMD) identifies the IP phone 12a (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).

As shown in Fig. 3a, the server's 14 database 22 includes the device's unique MAC address. (*Id.*, ¶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

(*Id.*, Fig. 3a (annotated).) Thus, in response to receiving the configuration data request from the device 12a (manageable electronic device), the server 14 (ACSMD) identifies the device 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).

In response to receiving that request, the server 14 (ACSMD) 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). Specifically, as shown in annotated Fig. 3a below, “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]....” (*Id.*, ¶23; *see also id.*, ¶54 (“a configuration server 20a, 20b or 20c, associated with the appropriate service provider [], selects the configuration settings for the IP phone 12 a with that specific MAC address...”).) “The 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.” (*Id.*, ¶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

(*Id.*, Fig. 3a (annotated).) Accordingly, the server 14 (ACSMD) receives the request for configuration settings from the 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 (information for the identification of electronic devices) which is stored in database 22 (the at least one database).

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 18a, 18b or 18c, as per first mapping table (step 114).” (*Id.*, ¶54.) Accordingly, the server 14 (ACSMD) receives the request for configuration settings from the phone 12a (manageable network device) and, in response, the server 14 is configured to identify a 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). Accordingly, *Angelot* discloses the features of claim element 1g.

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

Angelot discloses this feature. (Ex. 1002, ¶¶98-100, 127-132.) For instance, as discussed above, the server 14 is coupled to the configuration servers 20 such that requests for configuration settings are redirected to the relevant configuration server based on the first mapping table shown in Fig. 3a. As shown in step 114 of Fig. 2, the server 14 (ACSMD) redirects (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).

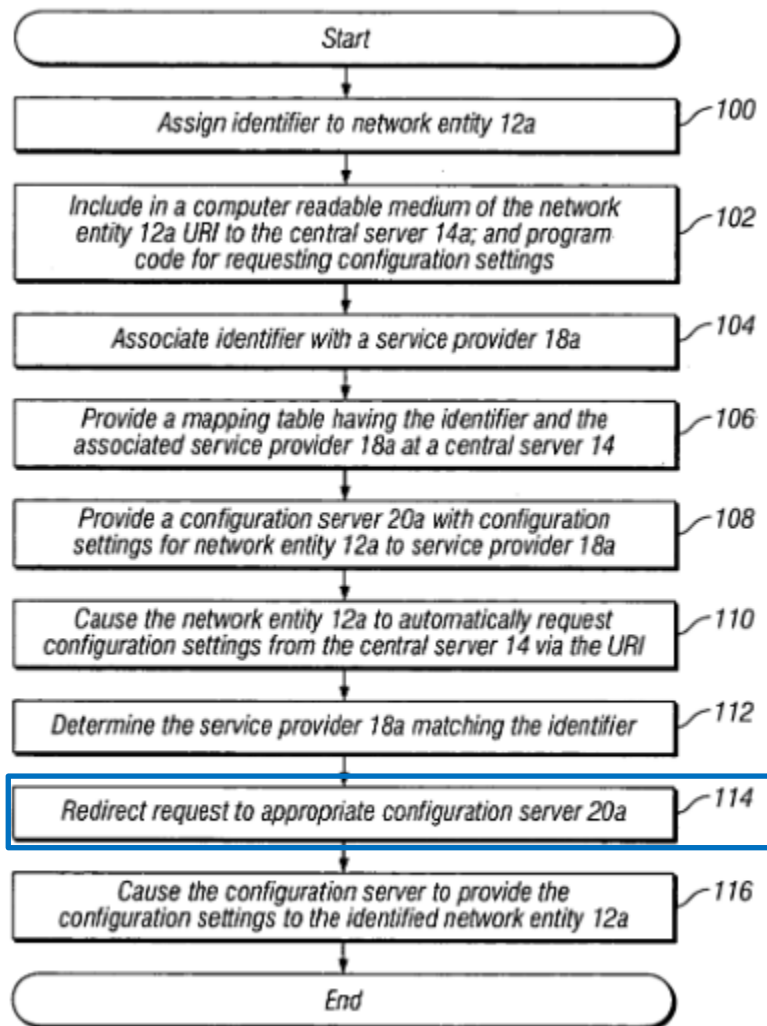


FIG. 2

(Ex. 1006, Fig. 2 (annotated).)

As *Angelot* explains, the “server [ACSMD] redirect[s] the request to an appropriate configuration server having the configuration settings data specific to

the identifier.” (*Id.*, ¶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.” (*Id.*, ¶25.) The “server 14 redirects any configuration related queries from the network entity 12a, 12b, or 12c to the configuration server 20a, 20b, 20c.” (*Id.*, ¶47.) “The 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.***” (*Id.*, ¶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...” (*Id.*, ¶62.)

Thus, the server 14 “relays” the phone 12a’s request to the configuration server (identified ACS) identified in the first mapping table. 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.” (Ex. 1005, 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 18a, 18b,

18c the MAC address belongs to... [then] a configuration server 20a, 20b or 20c, associated with the appropriate service provider 20a, 20b or 20c, selects the configuration settings for the IP phone 12a with that specific MAC address as per second mapping table...” (Ex. 1006, ¶54.)

The sending of the request from the server 14 to the configuration server 20a meets the KPN’s understanding of “relay” because the server sends/passes the request to the configuration server 20a. (*Id.*, ¶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 12a”); *see also id.*, ¶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 12a, 12b, 12c, 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*”).)

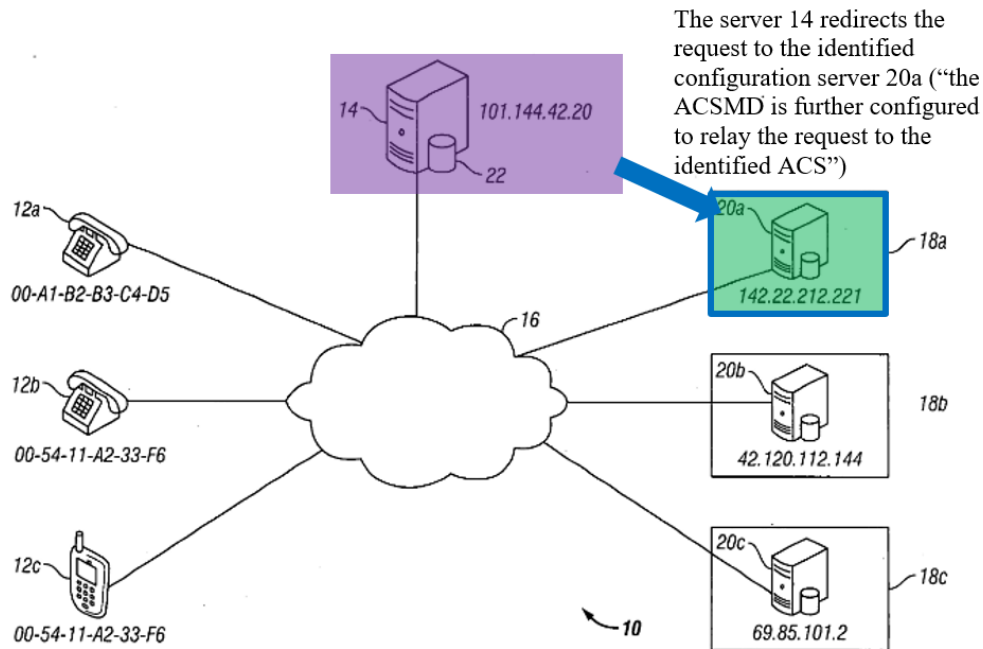


FIG. 1

(*Id.*, Fig. 1 (annotated).)

By way of 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...” (Ex. 1006, ¶55 (emphasis added).) The same is true for IP phone 12a’s request being relayed to configuration server 20a by the central server 14. Accordingly, *Angelot* discloses the features of claim element 1j.

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.**

Angelot discloses this feature. (Ex. 1002, ¶¶133-136; *see also* Ex. 1019, 43.)

For instance, the server 14 (ACSMD) 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, ¶62.) This is an example of the server 14 *sending/passing* the configuration setting data (“the reply”) to the IP phone 12a (“the manageable electronic device”), and this communication between the network entity and server 14 falls under KPN’s definition of “reply.” (Ex. 1002, ¶132.)

As explained above, *Angelot* processes the IP phone 12a’s request to determine the proper configuration server 20a by using the first look-up table (Fig. 3a), and then relays the request to the relevant server, e.g., sever 20a. (*Id.*, ¶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), ¶¶51-52 (the server 14 knows which configuration server 20 to send the query to by using a “first mapping table” stored in the database 22, which correlates the network entity 12a’s MAC address with the IP address of the configuration server 20a). In the same way, “[t]he configuration settings may include phone specific configuration

information, and ... ***central server(s) URIs...***” (*Id.*, ¶ 52 (emphasis added).) Thus, the configuration server 20a knows where (central server 14) to send the configuration settings data. (Ex. 1002, ¶133.) When the 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 network entity having said identifier.” (Ex. 1006, cl. 13 as originally filed.)

The 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. (Ex. 1002, ¶134.) Specifically, the configuration setting data (reply) from the identified configuration server 20a is (1) acquired by the server 14 from the configuration server 20a and then (2) “***provided to the IP phone 12a based on the MAC address.***” (*Id.*, ¶¶52, 62. (emphasis added).) *Thus, the server 14 relays/sends/passes the configuration setting data to the phone 12a based on its MAC address.* So the server 14 is processing or otherwise managing the reply based on its payload, as required in the Texas construction.

The server 14 passes the configuration settings to the IP phone 12a (“wherein the ACSMD is further configured to ... relay the reply to the manageable electronic device.”)

The server 14 acquires the configuration setting data from the identified configuration server 20a (“wherein the ACSMD is further configured to receive a reply from the identified ACS”)

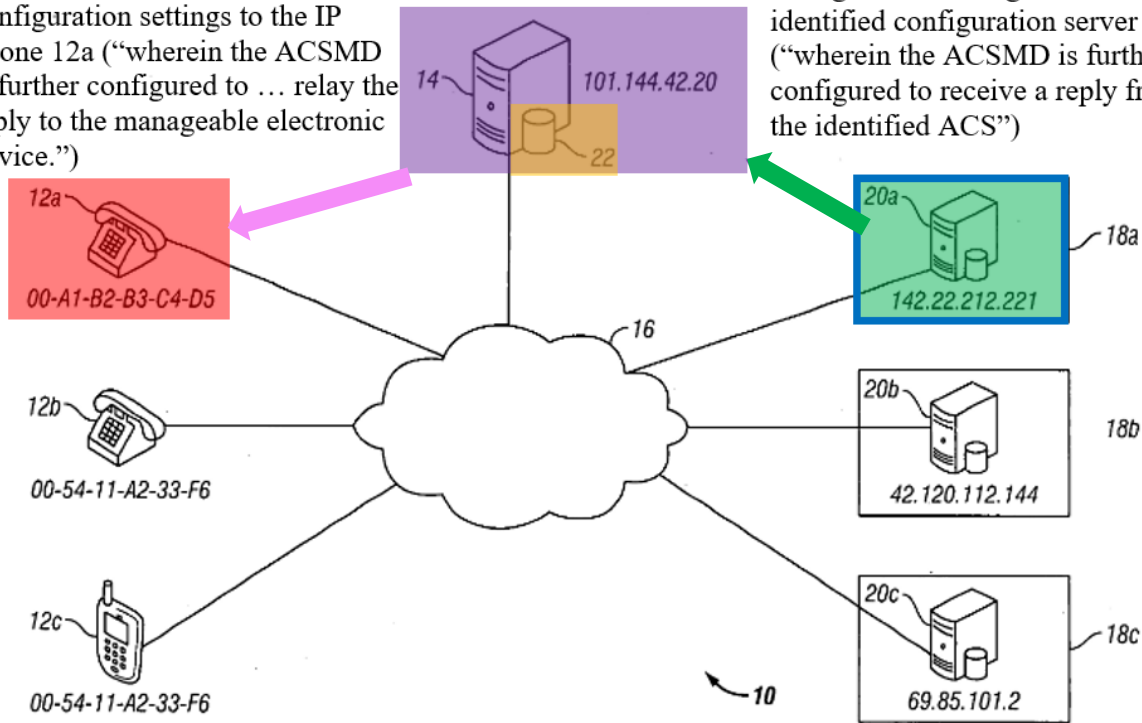


FIG. 1

(*Id.*, Fig. 1 (cropped and annotated).) For example, the 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 12a having `00-a1-b2-b3-c4-d5` as its MAC address.” (*Id.*, ¶52 (emphasis added).) Thus, 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. (Ex. 1002, ¶135.)

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

(*Id.*, Fig. 3a (annotated).) Accordingly, *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.**

Angelot discloses this feature. (Ex. 1002, ¶¶137-140; *see also* Ex. 1019, 43.)

For instance, *Angelot* discloses that IP phone 12a's MAC address (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, ¶49.)

“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 C, 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.” (*Id.*, ¶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.” (*Id.*)

“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.” (*Id.*, ¶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.” (*Id.*) “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.” (*Id.*, ¶55.)

In short, the server 14 (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, in the request (a network address of the manageable electronic device in the request) with the MAC addresses in the database 22 (a predetermined plurality of network addresses in the at least one database). Accordingly, *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.**

Angelot discloses this feature. (Ex. 1002, ¶141; *see also* Ex. 1019, 43.) As discussed above 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 discussed above for claim 3 and claim elements related to 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		yy.yyy.y.yyy

FIG. 3a

Accordingly, *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.**

Angelot discloses this feature. (Ex. 1002, ¶142; *see also* Ex. 1019, 44.) As discussed above, 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

Accordingly, *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.

Angelot discloses this feature. (Ex. 1002, ¶¶143; *see also* Ex. 1019, 44-45.)

See citations and analysis for claim 5.

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.

Angelot discloses the features of claim elements 10pre to 10h for the same reasons discussed above for claim elements 1pre to 1h. (*See supra* Parts VII.A.1.a–

i; Ex. 1002, ¶¶97-131, 143.) Moreover, *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 instance, 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, ¶45.) Thus, *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.**

Angelot discloses the features of claim 11 for the same reasons discussed above for claim 2. (See *supra* Part VIII.A.2; Ex. 1002, ¶¶132-135, 144.)

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.

Angelot discloses the features of claim elements 12pre to 12i for the same reasons discussed above for claim elements 1pre to 1h, and claim 10. (*See supra* Parts VIII.A.1.a–i, IX.A.7; Ex. 1002, ¶¶97-131, 145.)

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.**

Angelot discloses the features of claim 14 for the same reasons discussed above for claim 2. (*See supra* Part VIII.A.2; Ex. 1002, ¶¶132-135, 146.)

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.

Angelot discloses the features of claim elements 15pre to 15i for the same reasons discussed above for claim elements 1pre to 1h. (*See supra* Parts VIII.A.1.a–i; Ex. 1002, ¶¶97-131, 147.)

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.**

Angelot discloses the features of claim 16 for the same reasons discussed above for claim 2. (*See supra* Part VIII.A.2; Ex. 1002, ¶¶132-135, 149.)

B. Ground 2: *Angelot* Renders Obvious Claims 2-6, 11, 14, 16.

To the extent Patent Owner contends 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), such modification to *Angelot* would have been obvious to implement. (Ex. 1002, ¶¶150-165.) *See Merck & Co. v. Biocraft Labs., Inc.*, 874 F.2d 804, 807 (Fed. Cir. 1989) (“[T]he question under 35 USC 103 is not merely what the references expressly teach but what they would have suggested to one of ordinary skill in the art at the time the invention was made.”).

It is well settled that a “patent can be obvious in light of a single prior art reference if it would have been obvious to modify that reference to arrive at the patented invention.” *Game and Technology Co., Ltd. v. Activision Blizzard Inc.*, 926 F.3d 1370, 1381 (Fed. Cir. 2019). This is particularly true where the difference between the alleged invention and a prior art reference is “a prevalent, perhaps even predominant, [technique],” *Randall Mfg. v. Rea*, 733 F.3d 1355, 1363 (2013), and a POSITA “would have been motivated to combine [the reference] with his knowledge of conventional [techniques] to achieve the claimed invention.” *Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1338 (Fed. Cir. 2020).

To the extent that a POSITA would need to “modify” *Angelot* to arrive at the alleged invention of the Challenged Claims, the modification—i.e., 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 both

“conventional” and “predominant.” (Ex. 1002, ¶150-53.) To begin, there is nothing innovative about “relaying” information from one server to another or from a server to a device. (*See generally* discussion of *Jin*’s Subnet Relay Agent (SRA) in §VII.A; *see also* Ex. 1002, ¶¶79-81.) Indeed, the ’772 patent admits 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, 5:56-61 (emphasis added).) KPN, as discussed above, now contends that relaying is simply sending or passing. (Ex. 1009, 54 fn. 10.) A POSITA 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, and (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. (Ex. 1002, ¶¶151-53.)

Where, as here, the prior art teaches a minimal number of “known, finite, predictable solutions for solving the same problem,” the Federal Circuit has held that a POSITA has ample reason to substitute one option for the other. *Uber Techs., Inc. v. X One, Inc.*, 957 F.3d 1334, 1340–41 (Fed. Cir. 2020). Because the claimed “relay” is “known in the art” and the step of relaying “the request to the identified ACS” and relaying “the reply to the manageable electronic device” is, at most, “a predictable variation of [*Angelot*’s] system,” claim element 1h (and somewhat similarly claim elements 10h, 12i, 15i) and claim 2 (and somewhat similarly claims 11, 14, 16) of the ’772 patent are rendered obvious by *Angelot* in view of the knowledge of a POSITA. *Uber Techs.*, 957 F.3d at 1340.

Moreover, a POSITA would have recognized that there is good reason for the central server 14 to “relay” messages between the consumer device 12a and the configuration server 20a. (Ex. 1002, ¶¶152-54.) The 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. (*Id.*; Ex. 1006, ¶¶45, 46.) Thus, in response to receiving the request, the server 14 must ascertain where to send the request by looking at the table 3a stored in database 22. (*Id.*; Ex. 1006, ¶¶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....”) It would have been obvious 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. (Ex. 1002, ¶154-55; Ex. 1006, ¶¶51, 54, Fig. 2 (steps 104, 106, 110, 112, 114).) This relaying is an example of the server 14 changing, processing, or otherwise managing the request based at least in part on its payload. (Ex. 1002, ¶154.) This is also an example of simply sending or passing the request from one device 12a to another 20a. (*Id.*)

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, Fig. 3a (annotated).) It would have been obvious to a POSITA, in view of *Angelot* and the knowledge of a POSITA, to modify *Angelot*’s server 14 to relay the network device 12’s request for configuration settings after changing/processing that request. As Dr. Blumenthal explains, doing so would have ensured that the request is sent/passed to the appropriate configuration server 20a and a POSITA would have been encouraged to make such a modification to acquire the correct

configuration file from the configuration server identified in the table 3a. (Ex. 1002, ¶154-55; Ex. 1006, ¶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”); ¶54 (“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 18a, 18b, 18c the MAC address belongs to... the central server 14 then redirects the request to an appropriate service provider 18a, 18b or 18c, 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.”).)

Indeed, 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, ¶21; Ex. 1002, ¶155.)

As Dr. Blumenthal explains, a POSITA 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 it “is automatically configured without requiring any manual input of settings by the use.” (Ex. 1006, ¶47; *see also id.*, ¶54, cl. 1; Ex. 1002, ¶¶155-56.) Such a modification would have been obvious to a POSITA because it would have amounted to no more than applying a known technique (modifying a request before relaying it to its destination) to a known device (*Angelot*’s server 14) to yield predictable results (ensuring that the proper configuration server receives the request for configuration settings from the network device 12a). (Ex.1002, ¶¶155-165.) *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). Given the disclosures of *Angelot* and the knowledge of a POSITA, Dr. Blumenthal explains that a POSITA would have found using such techniques as discussed above a predictable implementation at the time of the alleged invention of the ’772 patent. (Ex.1002, ¶¶160-65.)

Modifying the 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 obvious. (Ex. 1002, ¶157-58.) *Angelot* does not expressly disclose that the server 14 provides the configuration server 20a with the IP address of the requesting device 12a. (*Id.*) Thus, 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 obvious to modify the server 14 to compare the configuration file name

to the IP Device MAC addresses in the database's table (Fig. 3a), 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. 1002, ¶¶157-59; Ex. 1006, 52 (emphasis added).)

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

(Ex. 1002, ¶¶157-59 (annotating Fig. 3a from Ex. 1006).) In other words, it would have been obvious to configure the 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. (Ex. 1002, ¶159.)

Specifically, it would have been obvious to a POSITA, in view of *Angelot* and the knowledge of a POSITA, to modify *Angelot*'s server 14 to transmit 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. A POSITA would have been encouraged to make such a modification 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. (Ex. 1002, ¶159.) Indeed, a POSITA would have understood that 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, ¶21; Ex. 1002, ¶¶155-65.) A POSITA would 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, ¶47; *see also id.*, ¶54, cl. 1; Ex. 1002, ¶¶156-60.)

Such a modification would have been obvious to a POSITA because it would have amounted to no more than applying a known technique (relaying a reply from one server to a device) to a known device (*Angelot*’s server 14) to yield predictable results (ensuring that the proper network device 12a receives configuration file it requested). (Ex.1002, ¶160; *see also id.*, ¶¶73-83.) *KSR*, 550 U.S. at 416. Given the disclosures of *Angelot* and the knowledge of a POSITA, such a skilled person would

have found using such techniques as discussed above a predictable implementation at the time of the alleged invention of the '772 patent. (Ex.1002, ¶¶160-65.) For the above-described reasons, the Challenged Claims are obvious in view of *Angelot* and the knowledge of a POSITA.

Moreover, *Angelot* discloses that the server 14 functions as a “proxy” or an “intermediary.” (Ex. 1006, ¶62.) It would have been obvious to set the server 14 as a “proxy” that relays information from the network device to the configuration server and from the configuration server to the network device. (Ex. 1002, ¶162.) As Applicant conceded during prosecution, 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. (Ex. 1004, Response dated July 30, 2014, 11-12.) Indeed, as shown in Ex. 1011 (MSFT Dictionary), 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, 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.” (*Id.* (emphasis added).)

It would have been obvious to a POSITA 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, have their requests for configuration data serviced and sent/passed to a configuration server 20. (Ex. 1002, ¶163.) Such a configuration would have been desirable because it would have ensured that only appropriate configuration files from known configuration servers are sent/passed to the network devices. (*Id.*)

A POSITA 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 device’s from being configured with malicious configuration data and (2) setting up such a proxy server was well-known at the time of the alleged invention and would have provided an extra layer of protection for network providers and their end users. (Ex. 1002, ¶164.) Indeed, a POSTIA would have been motivated to ensure that *Angelot*’s server 14 evaluates (1) requests from network devices 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 network devices and networks on which they reside. (Ex. 1002, ¶164.) By setting *Angelot*’s server as a proxy server a POSITA

would have beneficially provided a firewall that not only prevented unauthorized devices from obtaining configuration data, but also prevented nefarious configuration data from being supplied to the network devices. (Ex. 1002, ¶164.)

Indeed, in the above-discussed modified system of *Angelot* the 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. 1002, ¶165.) This 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). (*Id.*) Such a modification would have been obvious because it would have amounted to no more than applying a known technique (checking incoming and outgoing messages determining whether or not to relay them) to a known device (*Angelot*'s server 14) to yield predictable results (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 the network devices with configuration files). (Ex.1002, ¶165.) *KSR*, 550 U.S. at 416. Given the disclosures of *Angelot* and the knowledge of a POSITA, such a skilled person would have found using such techniques as discussed above a predictable implementation at the time of the alleged invention of the '772 patent. (Ex.1002, ¶165.)

For the above-described reasons, the Challenged Claims are obvious in view of *Angelot* and the knowledge of a POSITA.

C. Ground 3: *Angelot* in view of *Zakurdaev* Renders Obvious Claims 2-6, 11, 14, 16.

To the extent the Board disagrees with KPN’s position that “relay” means “send” or “pass,” or finds that *relaying* of communications does not occur as discussed above in Grounds 1 or 2, such modification would have been obvious to implement in view of *Angelot* and *Zakurdaev*.

Similar to *Angelot*, *Zakurdaev* is directed to facilitating the provisioning of configuration data to a consumer device. (Ex. 1007, ¶¶2-11.) Therefore, a POSITA would have had reason to consider the teachings of *Zakurdaev* when implementing *Angelot*’s system. (Ex. 1002, ¶166-68.) Indeed, *Angelot*’s IP phone (12a) has “factory-set default configuration data, such as, DHCP settings (enabled).” (Ex. 1006, ¶50.)

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, ¶12; Ex. 1002, ¶168.) 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, ¶12; Ex. 1002, ¶168.) “[T]he ISP equipment responds” by “generat[ing] an IP address for delivery to the user terminal that generated the

request.” (Ex. 1007, ¶12.) Like the first table (Fig. 3a) 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, ¶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.” (*Id.*) “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.” (*Id.*, *see also id.*, ¶¶27, 37, 41, 42, Fig. 2.)

As shown in *Zakurdaev*’s Fig. 2 (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). (Ex. 1007, ¶24.) The request (red) is provided to a DHCP Relay. (Ex. 1007, ¶25.) Like *Angelot*’s server 14, *Zakurdaev*’s DCHP 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, ¶26.) The DCHP Relay then relays the DHCPDISCOVER (blue) to the DHCP server at the ISP. (Ex. 1007, ¶27.) The ISP 216 then “generates a DHCPOFFER signal [green]

that is transmitted back to the Smart DHCP Relay 212.” (*Id.*) “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.” (*Id.*) After this processing, the DHCP Relay relays the DHCPOFFER signal (pink) to the terminal 204. (*Id.*)

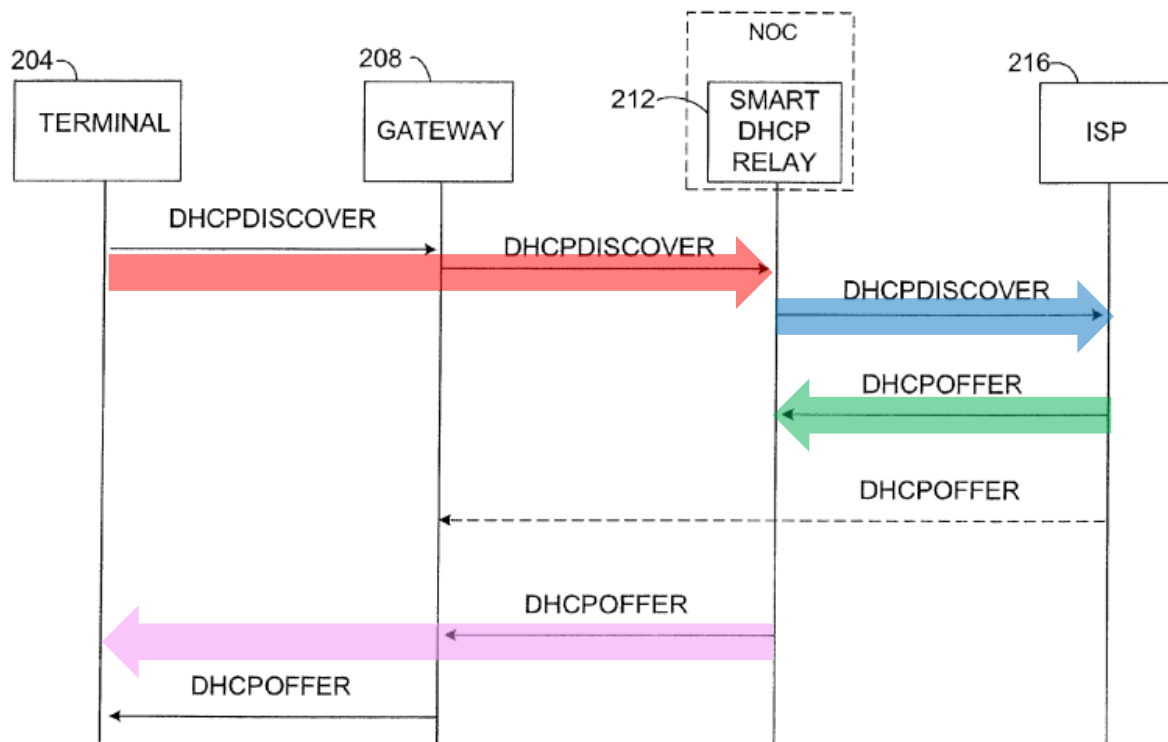


FIG. 2

(Ex. 1007, Fig. 2 (annotated).)

A POSITA would have been motivated to take these teachings from *Zakurdaev* and apply them to *Angelot* such that *Angelot*’s server 14 is able to “provide a capability for automatically loading IP addresses into a user’s terminal.” (Ex. 1007, ¶47; Ex. 1002, ¶171.) A POSITA 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, ¶47; Ex. 1002, ¶171.) A POSITA 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.” (Ex. 1007, ¶47; Ex. 1002, ¶171.) 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 POSITA would have understood that DHCP communications were a well-known communication technique in the art. (Ex. 1002, ¶172.) That is, DHCP communications techniques could be used in a system for providing configuration settings, as confirmed by *Zakurdaev*. Therefore, a POSITA 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*. (Ex. 1002, ¶172.) Such a combined system would have relay (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.

Given *Zakurdaev*'s teachings and the knowledge of a POSITA, a POSITA 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. (Ex. 1002, ¶173.) Indeed, a POSITA 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). (Ex. 1002, ¶173.) This is a basic concept 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), published by the Internet Engineering Task Force (www.ietf.org). See, e.g., (Ex. 1012; Ex. 1013.)

As known by a POSITA, 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 POSITA would have found it obvious to try *Zakurdaev* disclosed DHCP communication protocol with a DHCP Relay that relays messages between the client

and DHCP server for *Angelot*'s auto-configuration system. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007).

Indeed, 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. (Ex. 1002, ¶176.) *See KSR*, 550 U.S. at 415-421. A POSITA would have had the knowledge and capability to implement the above-discussed configurations in the combined *Angelot-Zakurdaev* system. (*Id.*)

IX. CONCLUSION

For the reasons given above, Petitioner requests institution of *inter partes* review and cancellation claims of the Challenged Claims of the '772 patent based on each of the grounds specified in this petition.

Respectfully submitted,

Dated: February 14, 2023

By: /Scott Hejny/
Scott W. Hejny (Reg. No. 45,882)
Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), the undersigned certifies that the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 8,886,772 contains, as measured by the word processing system used to prepare this paper, 12,895 words. This word count does not include the items excluded by 37 C.F.R. § 42.24 as not counting towards the word limit.

Respectfully submitted,

Dated: February 14, 2023

By: /Scott Hejny/
Scott W. Hejny (Reg. No. 45,882)
Counsel for Petitioner

CERTIFICATE OF SERVICE

I hereby certify that on February 14, 2023, I caused a true and correct copy of the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 8,886,772 and supporting exhibits were served on the following parties via Federal Express or Express Mail:

20306 - MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL
UNITED STATES

A courtesy copy was also sent via electronic mail to Patent Owner's litigation counsel listed below:

Lexie G. White
Savannah Ezelle
Andres C. Healy
Tamar Lusztig
Susman Godfrey L.L.P.

lwhite@susmangodfrey.com
sezelle@susmangodfrey.com
ahealy@susmangodfrey.com
tlusztig@susmangodfrey.com

S. Calvin Capshaw
Capshaw Derieux, LLP

ccapshaw@capshawlaw.com

By: /Scott Hejny/
Scott W. Hejny (Reg. No. 45,882)
Counsel for Petitioner