

PALM Resource Center

PALM Explorer

- PALM
- General Information
- Employee Locator
- Examiner Docket
- Count Calculator
- IDS Flag Clearance
- Bib Data Sheet
- TSS Activity Record
- Application Information
- Search
- RAM
- Reference
- File/Box Management

Application Number Information

Application Number: 90/012378 Assignments  
 Filing or 371(c) Date: 06/28/2012 eDan  
 Effective Date: 06/28/2012  
 Application Received: 06/28/2012  
 Patent Number:  
 Issue Date: 00/00/0000  
 Date of Abandonment: 00/00/0000  
 Attorney Docket Number: MIPIKU.002RE  
 Status: 420/REEXAM TERMINATED -- REQUEST DENIED IN GROUP  
 Confirmation Number: 2926  
 Title of Invention: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

Examiner Number: 78776 / WORJLOH..JALATEE  
 Group Art Unit: 3992 IFW Madras  
 Class/Subclass: 726/007.000  
 Lost Case: NO  
 Interference Number:  
 Unmatched Petition: NO  
 L&R Code: Secrecy Code: I  
 Third Level Review: NO  
 Secrecy Order: NO  
 Status Date: 11/21/2012

Bar Code	PALM Location	Location Date	Charge to Loc	Charge to Name	Employee Name	Location
----------	---------------	---------------	---------------	----------------	---------------	----------

Appln Info

Search Another: Application#  or Patent#

PCT /  /  or PG PUBS #

Attorney Docket #

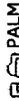
Bar Code #

To go back use Back button on your browser toolbar.

PROCEEDINGS CONCLUDED

PALM Resource Center

PALM Explorer



- General Information
- Employee Locator
- Examiner Docket
- Count Calculator
- IDS Flag Clearance
- Bib Data Sheet
- TSS Activity Record
- Application Information
- Search
- RAM
- Reference
- File/Box Management

# Content Information for 90/012378

Search Another: Application#  or Patent#

PCT /  /  or PG PUBS #

Attorney Docket #

Bar Code #

Contents

- Contents
- Petition
- Application
- Agency Information
- Continuity Data
- Design Data
- Address
- Fee
- Fee Data
- Fee Order
- Fee Order Print

Date	Status	Code	Description
11/21/2012	420	RTRM	RX - TERMINATION OF REEXAM PROCEEDINGS
08/15/2012	416	REXD	RX - EX PARTE REEXAM ORDER - DENIED
07/30/2012		REXN	RX - EXAMINER INTERVIEW SUMMARY RECORD
07/26/2012		DOCK	CASE DOCKETED TO EXAMINER IN GAU
07/24/2012		RXWVST	WAIVER OF OWNERS STATEMENT IN EX PARTE
07/20/2012	412	DOCK	CASE DOCKETED TO EXAMINER IN GAU
07/17/2012		REXN	RX - EXAMINER INTERVIEW SUMMARY RECORD
08/14/2012		NRX.	NOTICE OF REEXAM PUBLISHED IN OFFICIAL GAZETTE
07/10/2012		RXRRLF	REEXAM LITIGATION FOUND
07/10/2012		RXLITSR	REEXAM LITIGATION SEARCH CONDUCTED
07/09/2012	410	RXPCOM	COMPLETION OF PREPROCESSING - RELEASED TO ASSIGNED GAU
07/10/2012		MRXN	REEXAMINATION FORMALITIES NOTICE MAILED
07/10/2012		MRXN	REEXAMINATION FORMALITIES NOTICE MAILED
07/03/2012		RXTTLRPT	TITLE REPORT



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/012,378	06/28/2012	6779118	MIPIKU.002RE	2926
40401	7590	08/15/2012	EXAMINER	
Herskovitz & Associates, LLC 2845 Duke Street Alexandria, VA 22314			ART UNIT	PAPER NUMBER

DATE MAILED: 08/15/2012

Please find below and/or attached an Office communication concerning this application or proceeding.



DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Monument IP Law Group  
1717 Pennsylvania Avenue  
Suite 900  
Washington, DC 20006

**MAILED**

**AUG 15 2012**

**CENTRAL REEXAMINATION UNIT**

## EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. 90/012,378.

PATENT NO. 6779118.

ART UNIT 3992.

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).



Art Unit: 3992

**DETAILED ACTION*****Decision on Request***

No substantial new question of patentability is raised by the request for reexamination and prior art cited therein for the reasons set forth below.

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to “an applicant” and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that *ex parte* reexamination proceedings “will be conducted with special dispatch” (37 CFR 1.550(a)). Extensions of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c).

***References cited in Request***

- U.S. Patent No. 5889958 to Willens (“Willens”);
- U.S. Patent No. 6088451 to He et al. (“He”);
- U.S. Patent No. 6233686 to Zenchelsky et al. (“Zenchelsky”); and
- “The ChoiceNet Administrator’s Guide,” Livingston Enterprises, Jan. 1997 (“ChoiceNet”).

***Issues(s) Raised by Request*****Issue 1: Willens in view of Zenchelsky and the Patent owner’s admissions**

The Requester alleges that Willens in combination with Zenchelsky and the Patent owner's admissions raise(s) a substantial new question of patentability with regard to claims 2-7, 9-14, 16-24, 26-27, 29-32, 34-36, 38-40, 42-51, 53-63, 65-78, 80-87, and

Art Unit: 3992

89-90. The Ikudome patent has an effective filing date of April 21, 1999. Willens and Zenchelsky filing dates are December 20, 1996 and January 17, 1997, respectively.

Thus, the prior art references predate the effective filing date of Ikudome.

Issue 2: Willens in view of He, Zenchelsky, and the Patent owner's admissions

The Requester alleges that Willens in combination with Zenchelsky and the Patent owner's admissions raise(s) a substantial new question of patentability with regard to claims 29, 33, 37, 41, 52, 64, 79, and 87. He has an effective filing date of June 28, 1996. Thus, the prior art references predate the effective filling date of Ikudome.

Issue 3: ChoiceNet in view of Zenchelsky and the Patent owner's admission

The Requester alleges that ChoiceNet in combination with Zenchelsky and the Patent owner's admission raise(s) a substantial new question of patentability with regard to claims 2-7, 9-14, 16-24, 26-27, 29-32, 34-36, 38-40, 42-51, 53-63, 65-78, and 80-87. The prior art references predate the effective filing date of Ikudome.

Issue 4: ChoiceNet in view of He, Zenchelsky, and the Patent owner's admissions

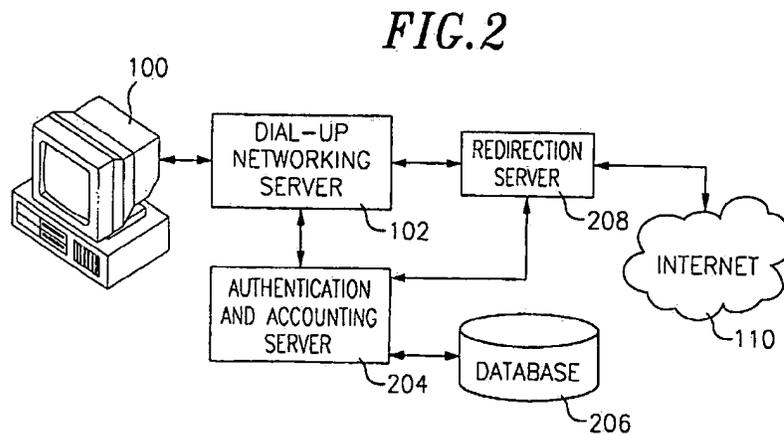
The Requester alleges that ChoiceNet in combination with He, Zenchelsky, and the patent owner's admissions raise(s) a substantial new question of patentability with regard to claims 29, 33, 37, 41, 52, 64, 79, and 87. The prior art references predate the effective filing date of Ikudome.

Art Unit: 3992

**Background**

Claims 2-7, 9-14, 16-24, and 26-90 in the instant request for reexamination are claims in the Ikudome patent issued from 09/295,966.

Ikudome is directed to a user specific automatic data redirection system. The system utilizes a redirection server to redirect user's data based on a stored rule set (see abstract). Ikudome teaches receiving a user's credentials when a user connects to a local network, sending the credentials to an authentication accounting server for verification, communicating the user's rule set to the redirection server from the authentication accounting server, and processing data directed toward the public network from the user's computer according to the rule set. (See claim 8 of Ikudome and col. 2, line 65 - col. 3, line 20). Fig. 2 illustrates one embodiment of the system.



Art Unit: 3992

***Original prosecution***

During the original prosecution of Ikudome patent, a second non-final action was mailed November 6, 2003 rejecting all pending claims. An interview summary was mailed on November 20, 2003 indicating that an agreement was made between the Examiner and the Applicant. Particularly, the summary stated that they are patentable differences between the claimed invention and the prior art of record. On March 16, 2004, a Notice of Allowance was issued allowing claims 1-18 and 20-26. The Notice of Allowance also included an Examiner's Amendment cancelling claims 19 and 29 and amending claims 15 and 26.

The Examiner noted that the closest prior art of record, Grube, fails to teach "wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server, and wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set" with respect to claims 1 and 8.

As per claim 15, it was noted by the original Examiner that Grube does not expressly disclose "wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address."

Regarding claim 26, the Examiner stated that the prior art fails to teach "modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server, and wherein the redirection server has a user side that is connected to a computer using the

Art Unit: 3992

temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server."

***First Reexamination Proceedings (90/009301)***

- An Order was mailed February 27, 2009 indicating that a substantial new question of patentability affecting claims 1-27 of the Ikudome patent was raised.
- A Non-Final action was issued on September 15, 2009 rejecting claims 1-27 under 35 U.S.C. 103(a) as being unpatentable over He in view of Zenchelsky.
- Patent owner filed a response amending claims 15, 18, 21, 26, and 27 and adding claims 28-47.
- A final rejection was mailed August 8, 2010 rejecting claims 1-31, 33-36, 38-41, and 43-46 over He in view of Zenchelsky. Claims 32, 37, 42, and 47 were rejected over He in view of Zenchelsky and further in view of admitted prior art. An After Final amendment was filed October 2, 2010.
- An After Final amendment requesting entry of amendments to claims 15, 18, 21, 26, and 27 and amending claims 28-31, 33-36, and 38-47.
- An Advisory Action mailed November 15, 2010 indicating that Patent owner's proposed response filed October 2, 2010 has overcome the 35 U.S.C. 112, 2nd paragraph rejection and entering the proposed amendments.

Art Unit: 3992

- A Notice of Appeal was filed December 1, 2010 and Appeal Brief filed by Patent owner on February 1, 2011.
- An Examiner's Answer was issued on March 31, 2011 maintaining the rejections of claims 1-47.
- Reply Brief filed May 27, 2011.
- A BPAI decision was issued August 23, 2011. Claims 1 and 32 were the representative claims of the claims on appeal. The Board affirmed the rejection in part and reversed in part with a new ground of rejection. Specifically, claims 32, 37, 42, and 47 were affirmed. As for claims 1, 8, 15, and 25 reversed, but a new ground of rejection was provided. The rejections of the other claims on appeal were reversed.
- An interview was held discussing the Board decision.
- An amendment, dated October 21, 2011, following the BPAI decision was filed cancelling rejected claims 1, 8, 15, 25, 32, 37, 42, and 47 and placing claims 16-23 and 38-41 in independent form. As expressed by Patent owner, new "claims 48-94 corresponding to independent claims 1, 8, 15, and 25 respectively, with additional terms to clarify the 'between' location of the redirection server." "new dependent claims 49-59, 61-71, 73-86, and 88-94 depend from allowable independent claims 48, 60, 72, and 87, respectively, and generally correspond respectively, to dependent claims 2-7, 28-32, 9-14, 33-37, 16-24, 38-42, 26-27 and 43-47, depending from independent claims 1, 8, 15, and 25."
- An interview summary, dated November 8, 2011, stated that Patent owner's proposal would overcome He et al.

Art Unit: 3992

- A supplemental response was filed by Patent owner requesting the Examiner to reopen prosecution in order to enter the claim amendments in the October 21 response and proposed amendment and to confirm patentability of claims 2-7, 9-14, 16-24, 26-31, 33-36, 38-41, 43-46, and 48-94.
- A NIRC was issued January 6, 2012. The status of the claims is as follows:
  - Patent claim(s) confirmed: 2-7, 9-14, 26, and 27.
  - Patent claim(s) amended (including dependent on amended claim(s)): 16-24.
  - Newly presented claim(s) patentable: 28-31, 33-36, 38-41, 43-46, and 48-94.
  - Newly presented canceled claims: 32, 37, 42, and 47.

In the reasons for confirmation and patentability section, it was noted that in light of the BPAI decision and remaining prior art of record not raising further issues beyond those already addressed by the BPAI, claims 2-7, 9-14, and 24 are confirmed. Claims 16-23 and 26-31, 33-36, 38-41 and 43-46, 48, 60, 72, 87, 49-59, 61-71, 73-86, and 88-94 are patentable.

Additionally, as per claims 48, 60, 72, and 87, the Examiner noted that "these claims include the original language of claims 1, 8, 15, and 25 respectively, except that the redirection server is defined as being between the dial up network server and the public network (claims 48 and 60), or between the user computer and the public network (claims 72 and 87). This distinguishes from the network topology of He et al., applied as the primary prior art reference at the time of appeal."

Art Unit: 3992

### ***Scope of Reexamination***

On November 2, 2002, Public Law 107-273 was enacted. Title III, Subtitle A, Section 13105, part (a) of the Act revised the reexamination statute by adding the following new last sentence to 35 U.S.C. 3030(a) and 312(a):

The existence of a substantial new question of patentability is not precluded by the fact that a patent or printed publication was previously cited by or to the Office or considered by the Office.

For any reexamination ordered on or after November 2, 2002, the effective date of the statutory revision, reliance on previously cited/considered art, i.e. "old art," does not necessarily preclude the existence of a substantial new question of patentability (SNQ) that is based exclusively on the old art. Rather, determinations on whether a SNQ exists in such an instance shall be based upon a fact-specific inquiry done on a case-by-case basis.

### ***Analysis***

#### Willens

Willens is directed to a network access control system and process. One object of the system is to use an extension of firewall filtering to implement content monitoring (see col. 2, lines 59-61). Willens teaches utilizing a user's profile to authenticate the user upon logging into a communications server. The user's profile also identifies the filter that controls access to Internet sites (see col. 5, lines 9-25).

Art Unit: 3992

Zenchelsky

Zenchelsky is directed to a system and method for providing peer level access control on a network. Zenchelsky discloses "a filter that efficiently stores, implements and maintains access rules specific to an individual computer on a network with rapidly changing configurations and security needs." See col. 4, lines 55-58. In the system, upon a network access request, each individual peer is authenticated. "The peer's local rule base is then loaded into the filter of the present invention, either from the peer itself, or from another user, host or peer. When the peer is no longer authenticated to the POP (e.g., the peer loses connectivity or logs off from the POP), the peer's local rule base is ejected (deleted) from the filter." See col. 5, lines 17-24.

He

He is directed to a security system and method for network element access. "The network security mechanisms include: an authentication server responsible for authentication of the network users to network elements, a credential server responsible for controlling the network user credentials or privileges, and a network element access server responsible for controlling of access to the network elements by the user elements." See abstract.

ChoiceNet

"ChoiceNet provides a mechanism to filter network traffic on dial-up remote access, filter information is stored in a central location server as the ChoiceNet synchronous leased line, or asynchronous connection." See page 1-1.

Art Unit: 3992

He and Zenchelsky are old art previously cited by the Examiner in previous reexamination proceedings. Willens and ChoiceNet are old art that were previously before the Examiner, but not used in the context of a rejection.

The Requester asserts that "the Board's decision casts all prior art references in a new light because the Board stated that redirection is obvious in the prior art as admitted by Patent Owner." See page 9. The alleged substantial new question of patentability views the prior art in view of the Board decision. The request notes, as expressed to the Board, redirection is an obvious extension of blocking.

However, He and Zenchelsky are not being viewed in a new light. These references were considered during the first reexamination proceedings and a co-pending *ex parte* reexamination proceeding (90/012378). Additionally, claim 29 recites "wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set." During the first reexamination proceedings, the Examiner relied on He for teaching this feature (see Examiner's Answer) and the Board reversed the rejection.

In the instant request, the Requester asserts that "He teaches a first rule set which allows access to network elements which can expire after a defined amount of time wherein a second rule set is applied which denies access to network elements. Hence, it would have been obvious to modify the rule sets in Willens to include a temporary rule set for an initial period of time and a standard rule set thereafter, as taught in He." (See page 102 of the Request). The Requester is therefore alleging that He teaches utilizing

Art Unit: 3992

"the temporary rule set for an initial period of time and to thereafter utilize the standard rule set," as recited in the claim. As mentioned above, He was previously considered by the Examiner in the previous proceedings for teaching "the temporary rule set for an initial period of time and to thereafter utilize the standard rule set" such rejection was reserved by the Board (see BPAI decision issued August 23, 2011). An old art must "be presented/viewed in a new light, or in a different way, as compared with its use in the earlier concluded examination(s)."

As for Willens and ChoiceNet, these references are cumulative to Radia (U.S. Patent 5848233), which were cited in the co-pending proceeding. That is, Radia discloses "a method and apparatus for filtering IP packets based on events within a computer network." See abstract. In the system, when a user logs in, his/hers filter profile is retrieved and downloaded to the access network control. Next, the network components are reconfigured (see Fig. 9 & related text). Similarly to Radia, upon logging into the system, Willens uses the user's profile for authentication and to identify the filter that controls access. "ChoiceNet can use filter names specified by the Remote Authentication Dial-In User Service (Radius) user record." See page 1-1.

"A prior art patent or printed publication raises a substantial question of patentability where there is a substantial likelihood that a reasonable examiner would consider the prior art patent or printed publication important in deciding whether or not the claim is patentable. If the prior art patents and/or publications would be considered important, then the examiner should find "a substantial new question of patentability"

Art Unit: 3992

unless the same question of patentability has already been decided as to the claim in a final holding of invalidity by the Federal court system or by the Office in a

previous examination. For example, the same question of patentability may have already been decided by the Office where the examiner finds the additional (newly provided) prior art patents or printed publications are merely cumulative to similar prior art already fully considered by the Office in a previous examination of the claim." MPEP 2241.

Further, He and Zenchelsky were already considered by the Office in previous examination of the claims and are not being presented in a new light. As for Willens and ChoiceNet, these references are "cumulative to similar prior art already fully considered by the Office in a previous examination" of the claims.

Thus, it is not agreed that the prior art references raises a substantial likelihood that a reasonable examiner would consider these teachings as important in determining the patentability of the claims of Ikudome patent. That is, a new substantial question of patentability is not being raised because the references were either fully considered in a prior examination and not being presented in a new light or are cumulative to those fully considered.

#### ***Waiver of Right to File Patent Owner Statement***

In a reexamination proceeding, Patent Owner may waive the right under 37 C.F.R. 1.530 to file a Patent Owner Statement. The document needs to contain a statement that Patent Owner waives the right under 37.C.R. 1.530 to file a Patent Owner

Art Unit: 3992

Statement and proof of service in the manner provided by 37 C.F.R. 1.248, if the request for reexamination was made by a third party requester, see 37 C.F.R. 1.550. The Patent Owner may consider using the following statement in a document waiving the right to file a Patent Owner Statement: Patent Owner waives the right under 37 C.F.R. 1.530 to file a Patent Owner Statement.

### ***Amendment in Reexamination Proceedings***

Patent owner is notified that any proposed amendment to the specification and/or claims in this reexamination proceeding must comply with 37 CFR 1.530(d)-(j), must be formally presented pursuant to 37 CFR §1.52(a) and (b), and must contain any fees required by 37 CFR §1.20(c). See MPEP §2250(IV) for examples to assist in the preparation of proper proposed amendments in reexamination proceedings.

### ***Service of Papers***

After the filing of a request for reexamination by a third party requester, any document filed by either the patent owner or the third party requester must be served on the other party (or parties where two or more third party requester proceedings are merged) in the reexamination proceeding in the manner provided in 37 CFR 1.248. See 37 CFR 1.550.

### ***Notification of Concurrent Proceedings***

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent

Art Unit: 3992

proceeding, involving Patent No. 6,779,118 throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceedings throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282, and 2286.

All correspondence relating to this ex parte reexamination proceeding should be directed:

By Mail to:

Mail Stop Ex Parte Reexam  
Central Reexamination Unit  
Commissioner of Patents  
United States Patent & Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450

By FAX to:

(571) 273-9900  
Central Reexamination Unit

By Hand:

Customer Service Window  
Randolph Building  
401 Dulany Street  
Alexandria, VA 22314

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

<https://efs.uspto.gov/efile/myportal/efs-registered>

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Art Unit: 3992

Any inquiry concerning this communication should be directed to the Central  
Reexamination Unit at (571) 272-7705.

/Jalatee Worjloh/

Patent Reexamination Specialist, Art Unit 3992

Conferees:



**ANDREW J. FISCHER**   
Supervisory Patent Reexamination Specialist  
CRU -- Art Unit 3992

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		
	First Named Inventor	Koichiro Ikudome	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	MIPIKU.002RE	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	5889958		1990-03-30	Willens	
	2	6088451		2000-07-11	He et al.	
	3	6233686		2011-05-15	Zenchelsky et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup>	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>
	1							<input type="checkbox"/>

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		
	First Named Inventor	Koichiro Ikudome	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	MIPIKU.002RE	

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>
	1	"The ChoiceNet(TM) Administrator's Guide," Livingston Enterprises, 88 pages, January 1997	<input type="checkbox"/>
	2	Ex parte Linksmart Wireless Technology, LLC, No. 2011-009566 (B.P.A.I., August 23, 2011)	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

**EXAMINER SIGNATURE**

Examiner Signature	/Jalatee Worjloh/	Date Considered	08/01/2012
--------------------	-------------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

<b>Search Notes</b>  	<b>Application/Control No.</b> 90012378	<b>Applicant(s)/Patent Under Reexamination</b> 6779118
	<b>Examiner</b> JALATEE WORJLOH	<b>Art Unit</b> 3992

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>

<b>SEARCH NOTES</b>			
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>	
review of patented file's prosecution history	8/2/2012	/J.W./	

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>

--	--

<b>Reexamination</b> 90/012,378	Application/Control No.	Applicant(s)/Patent Under Reexamination 6,779,118
	Certificate Date	Certificate Number

**Requester Correspondence Address:**       Patent Owner       Third Party

MONUMENT IP LAW GROUP  
1717 PENNSYLVANIA AVENUE  
SUITE 900  
WASHINGTON, DC 20006

<b>LITIGATION REVIEW</b> <input checked="" type="checkbox"/>	/J.W./ (examiner initials)	8/1/2012 (date)
Case Name		Director Initials
(OPEN) 8:12cv522, Linksmart Wireless Technology LLC v. T-Mobile USA Inc. et al., U.S. District-California Central (Southern Division)		COT for I. Y ↓
(CLOSED) 2:10cv277, Linksmart Wireless Technology LLC vs. TJ Hospitality Ltd et al., U.S. District-Texas Eastern (Marshall)		
(CLOSED) 2:09cv26, Linksmart Wireless Technology LLC v. Six Continents Hotels Inc. et al., U.S. District-Texas Eastern (Marshall)		
(CLOSED) 2:09cv385, Linksmart Wireless Technology, LLC v. SBC Internet Services, Inc., U.S. District-Texas Eastern (Marshall)		
(CLOSED) 2:08cv304, Linksmart Wireless Technology, LLC v. Cisco Systems, Inc. et al., U.S. District-Texas Eastern (Marshall)		
(CLOSED) 2:08cv264, Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc et al., U.S. District-Texas Eastern (Marshall)		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
Ex parte reexamination	90/012,342

--	--



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/012,378	06/28/2012	6779118	MIPIKU.002RE	2926

40401            7590            07/30/2012  
Herskovitz & Associates, LLC  
2845 Duke Street  
Alexandria, VA 22314

EXAMINER

ART UNIT            PAPER NUMBER

DATE MAILED: 07/30/2012

Please find below and/or attached an Office communication concerning this application or proceeding.



Commissioner for Patents  
United States Patents and Trademark Office  
P.O.Box 1450  
Alexandria, VA 22313-1450  
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS

MONUMENT IP LAW GROUP  
1717 PENNSYLVANIA AVENUE  
SUITE 900  
WASHINGTON, DC 20006

Date:

**MAILED**

**JUL 3 0 2012**

**CENTRAL REEXAMINATION UNIT**

**EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM**

REEXAMINATION CONTROL NO. : 90012378

PATENT NO. : 6779118

ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified ex parte reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the ex parte reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

<b>Ex Parte Reexamination Interview Summary – Pilot Program for Waiver of Patent Owner's Statement</b>	Control No.	Patent For Which Reexamination is Requested
	90/012,378 Examiner	6,799,118 Art Unit  3993

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

**All participants (USPTO official and patent owner):**

- (1) Patricia Martin, CRU (3)  
(2) Abraham Hershkovitz, 45294 (4)

Date of Telephonic Interview: 7/24/12.

The USPTO official requested waiver of the patent owner's statement pursuant to the pilot program for waiver of patent owner's statement in *ex parte* reexamination proceedings.\*

- The patent owner **agreed** to waive its right to file a patent owner's statement under 35 U.S.C. 304 in the event reexamination is ordered for the above-identified patent.
- The patent owner **did not agree** to waive its right to file a patent owner's statement under 35 U.S.C. 304 at this time.

The patent owner is not required to file a written statement of this telephone communication under 37 CFR 1.560(b) or otherwise. However, any disagreement as to this interview summary must be brought to the immediate attention of the USPTO, and no later than one month from the mailing date of this interview summary. Extensions of time are governed by 37 CFR 1.550(c).

\*For more information regarding this pilot program, see *Pilot Program for Waiver of Patent Owner's Statement in Ex Parte Reexamination Proceedings*, 75 Fed. Reg. 47269 (August 5, 2010), available on the USPTO Web site at <http://www.uspto.gov/patents/law/notices/2010.jsp>.

- USPTO personnel were unable to reach the patent owner.

The patent owner may contact the USPTO personnel at the telephone number provided below if the patent owner decides to waive the right to file a patent owner's statement under 35 U.S.C. 304.

/Patricia Martin/  
Paralegal Specialist 571-272-5004  
Signature and telephone number of the USPTO official who contacted or attempted to contact the patent owner.

cc: Requester (if third party requester)



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/012,378	06/28/2012	6779118	MIPIKU.002RE	2926
40401	7590	07/17/2012	EXAMINER	
Hershkovitz & Associates, LLC 2845 Duke Street Alexandria, VA 22314			ART UNIT	PAPER NUMBER

DATE MAILED: 07/17/2012

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

---

Commissioner for Patents  
United States Patents and Trademark Office  
P.O.Box 1450  
Alexandria, VA 22313-1450  
www.uspto.gov

**MAILED**

Date: JUL 17 2012

**CENTRAL REEXAMINATION UNIT**

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS  
MONUMENT IP LAW GROUP  
1717 PENNSYLVANIA AVENUE  
SUITE 900  
WASHINGTON, DC 20006

**EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM**

REEXAMINATION CONTROL NO. : 90012378  
PATENT NO. : 6779118  
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified ex parte reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the ex parte reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

---

<b>Ex Parte Reexamination Interview Summary – Pilot Program for Waiver of Patent Owner's Statement</b>	Control No. 90/012,378	Patent For Which Reexamination is Requested 6,799,118
	Examiner	Art Unit 3993

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

**All participants (USPTO official and patent owner):**

- (1) Patricia Martin, CRU (3)  
(2) Abraham HersHKovitz, 45294 (4)

Date of Telephonic Interview: 7/11/12.

The USPTO official requested waiver of the patent owner's statement pursuant to the pilot program for waiver of patent owner's statement in *ex parte* reexamination proceedings.\*

- The patent owner **agreed** to waive its right to file a patent owner's statement under 35 U.S.C. 304 in the event reexamination is ordered for the above-identified patent.
- The patent owner **did not agree** to waive its right to file a patent owner's statement under 35 U.S.C. 304 at this time.

The patent owner is not required to file a written statement of this telephone communication under 37 CFR 1.560(b) or otherwise. However, any disagreement as to this interview summary must be brought to the immediate attention of the USPTO, and no later than one month from the mailing date of this interview summary. Extensions of time are governed by 37 CFR 1.550(c).

\*For more information regarding this pilot program, see *Pilot Program for Waiver of Patent Owner's Statement in Ex Parte Reexamination Proceedings*, 75 Fed. Reg. 47269 (August 5, 2010), available on the USPTO Web site at <http://www.uspto.gov/patents/law/notices/2010.jsp>.

- USPTO personnel were unable to reach the patent owner.

The patent owner may contact the USPTO personnel at the telephone number provided below if the patent owner decides to waive the right to file a patent owner's statement under 35 U.S.C. 304.

/Patricia Martin/  
Paralegal Specialist 571-272-5004  
Signature and telephone number of the USPTO official who contacted or attempted to contact the patent owner.

cc: Requester (if third party requester)



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
90/012,378	06/28/2012	6779118

MONUMENT IP LAW GROUP  
1717 PENNSYLVANIA AVENUE  
SUITE 900  
WASHINGTON, DC 20006

**CONFIRMATION NO. 2926**  
**REEXAMINATION REQUEST**  
**NOTICE**



Date Mailed: 07/10/2012

**NOTICE OF REEXAMINATION REQUEST FILING DATE**

*(Third Party Requester)*

Requester is hereby notified that the filing date of the request for reexamination is 06/28/2012, the date that the filing requirements of 37 CFR § 1.510 were received.

A decision on the request for reexamination will be mailed within three months from the filing date of the request for reexamination. (See 37 CFR 1.515(a)).

A copy of the Notice is being sent to the person identified by the requester as the patent owner. Further patent owner correspondence will be the latest attorney or agent of record in the patent file. (See 37 CFR 1.33). Any paper filed should include a reference to the present request for reexamination (by Reexamination Control Number).

cc: Patent Owner  
40401  
Hershkovitz & Associates, LLC  
2845 Duke Street  
Alexandria, VA 22314

/rbell/

Legal Instruments Examiner  
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
90/012,378	06/28/2012	6779118

40401  
Hershkovitz & Associates, LLC  
2845 Duke Street  
Alexandria, VA 22314

**CONFIRMATION NO. 2926**  
**REEXAM ASSIGNMENT NOTICE**



Date Mailed: 07/10/2012

**NOTICE OF ASSIGNMENT OF REEXAMINATION REQUEST**

The above-identified request for reexamination has been assigned to Art Unit 3992. All future correspondence to the proceeding should be identified by the control number listed above and directed to the assigned Art Unit.

A copy of this Notice is being sent to the latest attorney or agent of record in the patent file or to all owners of record. (See 37 CFR 1.33(c)). If the addressee is not, or does not represent, the current owner, he or she is required to forward all communications regarding this proceeding to the current owner(s). An attorney or agent receiving this communication who does not represent the current owner(s) may wish to seek to withdraw pursuant to 37 CFR 1.36 in order to avoid receiving future communications. If the address of the current owner(s) is unknown, this communication should be returned within the request to withdraw pursuant to Section 1.36.

cc: Third Party Requester(if any)  
MONUMENT IP LAW GROUP  
1717 PENNSYLVANIA AVENUE  
SUITE 900  
WASHINGTON, DC 20006

/rbell/

Legal Instruments Examiner  
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

# Litigation Search Report CRU 3999

**Reexam Control No. 90/012,378**

**TO:**  
**Location: CRU**  
**Art Unit: 3992**  
**Date: July 10, 2012**

**From: Patricia Martin**  
**Location: CRU 3999**  
**MDW-7C55**  
**Phone: (571) 272-7705**

**U.S. Patent Number: 6,779,118**

## Search Notes

- 1) I performed a Key Cite Search in Westlaw, which retrieves all history on the patent including any litigation.
- 2) I performed a search in Lexis in the Federal Courts and Administrative Materials databases for any cases found.
- 3) I performed a search in Lexis in the IP Journal and Periodicals database for any articles on the patent.
- 4) I performed a search in Lexis in the news databases for any articles about the patent or any articles about litigation on this patent.
- 5) I performed a search on the patent in Lexis Court Link for any open dockets or closed cases.

### **Litigation was found involving:**

**8:12cv522 – Open**  
**2:10cv277 – Closed**  
**2:09cv26 – Closed**  
**2:08cv385 – Closed**  
**2:08cv304 – Closed**  
**2:08cv264 – Closed**



Date of Printing: Jul 10, 2012

**KEYCITE**

**H US PAT 6779118 USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM, Assignee: Auriq Systems, Inc. (Aug 17, 2004)**

**History****Direct History**

=> 1 **USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM, US PAT 6779118, 2004 WL 1841593 (U.S. PTO Utility Aug 17, 2004)**

*Construed by*

**H** 2 Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc., 2010 WL 2640402, 2010 Markman 2640402 (E.D.Tex. Jun 30, 2010) (NO. 2:08-CV-264-DF-CE) (Markman Order Version)

**Related References**

**H** 3 Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc., 2010 WL 3816679 (E.D.Tex. Sep 02, 2010) (NO. 208CV264)

*Report and Recommendation Adopted by*

**H** 4 Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc., 2010 WL 3816677 (E.D.Tex. Sep 27, 2010) (NO. 208CV264)

**Court Documents****Trial Court Documents (U.S.A.)****E.D.Tex. Trial Pleadings**

- 5 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. 1. T-MOBILE USA, INC.; 2. Wayport, Inc.; 3. AT&T, Inc.; 4. AT&T Mobility, LLC; 5. Lodgenet Interactive Corp.; 6. Ibahn General Holdings Corp.; 7. Ethostream, LLC; 8. Hot Point Wireless, Inc.; 9. Netnearu Corp.; 10. Pronto Networks, Inc.; 11. Aptilo N, 2008 WL 3538408 (Trial Pleading) (E.D.Tex. Jul. 1, 2008) **Complaint and Demand for Jury Trial** (NO. 08CV00264)
- 6 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2008 WL 4355636 (Trial Pleading) (E.D.Tex. Aug. 21, 2008) **Linksmart Wireless Technology, LLC'S Reply to Ethostream, LLC'S Counterclaim** (NO. 208CV00264)
- 7 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2008 WL 4355637 (Trial Pleading) (E.D.Tex. Aug. 29, 2008) **Answer and Counterclaim** (NO. 208CV00264)
- 8 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. (1) T-MOBILE USA, INC., (2) Wayport, Inc., (3) AT&T, Inc., (4) AT&T Mobility, LLC, (5) Lodgenet Interactive Corp., (6)

© 2012 Thomson Reuters. All rights reserved.

- ibahn General Holdings Corp., (7) Ethostream, LLC, (8) Hot Point Wireless, Inc., (9) Netnearu Corp., (10) Pronto Networks, Inc. (11, 2008 WL 5369919 (Trial Pleading) (E.D.Tex. Sep. 12, 2008) **Defendant ibahn General Holdings Corp.'s Answer and Counterclaims to Linksmart Wireless Technology, LLC's Complaint** (NO. 208-CV-00264-TJW-CE)
- 9 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC.; Wayport, Inc.; At&t, Inc.; AT&T Mobility, LLC; Lodgenet Interactive Corporation; Ibahn General Holdings Corp.; Ethostream, LLC; Hot Point Wireless, Inc.; Netnearu Corp.; Pronto Networks, Inc.; Aptilo Networks, Inc.; Freefi Network, 2008 WL 5369920 (Trial Pleading) (E.D.Tex. Sep. 12, 2008) **Defendant Aptilo Networks, Inc.'s Answer, Affirmative Defenses and Counterclaims to Plaintiff's Complaint for Patent Infringement** (NO. 208-CV-264TJW-CE)
- 10 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. 1. T-MOBILE USA, INC.; 2. Wayport, Inc.; 3. AT&T, Inc.; Jury 4. AT&T Mobility, LLC; 5. Lodgenet Interactive Corp.; 6. Ibahn General Holdings Corp.; 7. Ethostream, LLC; 8. Hot Point Wireless, Inc.; 9. Netnearu Corp.; 10. Pronto Networks, Inc.; 11. Apt, 2008 WL 5369909 (Trial Pleading) (E.D.Tex. Sep. 15, 2008) **Defendant Marriott International, Inc.'s Answer and Counterclaims to Linksmart Wireless Technology, LLC's Complaint** (NO. 208-CV-00264-TJW-CE)
- 11 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2008 WL 5369910 (Trial Pleading) (E.D.Tex. Sep. 15, 2008) **Wayport, Inc.'s Answer, Defenses, and Counterclaims to Complaint** (NO. 208-CV-00264-TJW-CE)
- 12 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC. et al., Defendants., 2008 WL 5369911 (Trial Pleading) (E.D.Tex. Sep. 15, 2008) **Defendant Barnes & Noble Booksellers, Inc. Answer to Plaintiff's Complaint** (NO. 208-CV-00264-TJW-CE)
- 13 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2008 WL 5369912 (Trial Pleading) (E.D.Tex. Sep. 15, 2008) **Mcdonald's Corp.'s Answer, Defenses, and Counterclaims to Complaint** (NO. 208-CV-00264-TJW-CE)
- 14 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2008 WL 5369913 (Trial Pleading) (E.D.Tex. Sep. 15, 2008) **Meraki, Inc.'s Answer, Defenses, and Counterclaims to Complaint** (NO. 208-CV-00264-TJW-CE)
- 15 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2008 WL 5369914 (Trial Pleading) (E.D.Tex. Sep. 15, 2008) **Best Western International, Inc.'s Answer to Plaintiff's Complaint and Counterclaims** (NO. 208-CV-00264-TJW-CE)
- 16 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC.; et al., Defendants., 2008 WL 5369921 (Trial Pleading) (E.D.Tex. Sep. 15, 2008) **T-Mobile USA, Inc.'s Answer and Counterclaims** (NO. 208-CV-00264-TJW-CE)
- 17 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, Inc. et al., Defendants., 2008 WL 5369922 (Trial Pleading) (E.D.Tex. Sep. 15, 2008) **Defendant Mail Boxes Etc., Inc.'s Answer to Plaintiff's Complaint** (NO. 208-CV-00264-TJW)
- 18 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC.; Wayport, Inc.; AT&T, Inc.; AT&T Mobility, LLC; Lodgenet Interactive Corporation; Ibahn General Holdings Corp.; Ethostream, LLC; Hot Point Wireless, Inc.; Netnearu Corp.; Pronto Networks, Inc.; Aptilo Networks, Inc.; Freefi Network, 2008 WL 5369915 (Trial Pleading) (E.D.Tex. Sep. 19, 2008) **Ramada Worldwide, Inc.'s Answer to Complaint and Counterclaims** (NO.

- 208-CV-00264-TJW-CE)
- 19 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2008 WL 5369916 (Trial Pleading) (E.D.Tex. Sep. 19, 2008) **Pronto Networks, Inc.'s Answer, Defenses, and Counterclaims to the Complaint** (NO. 208-CV-00264-TJW-CE)
  - 20 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. 1. T-MOBILE USA, INC.; 2. Wayport, Inc.; 3. AT&T, Inc.; 4. AT&T Mobility, LLC; 5. Lodgenet Interactive Corp.; 6. Ibahn General Holdings Corp.; 7. Ethostream, LLC; 8. Hot Point Wireless, Inc.; 9. Netnearu Corp.; 10. Pronto Networks, Inc.; 11. Aptilo N, 2008 WL 5369917 (Trial Pleading) (E.D.Tex. Sep. 22, 2008) **Defendant Freefi Networks. Inc.'s Answer and Counterclaims to Original Complaint** (NO. 208CV00264TJW)
  - 21 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. BEST WESTERN INTERNATIONAL, INC., Third-Party Plaintiff, v. BESTCOMM NETWORKS, INC. and Nomadix, Inc., Third-Party Defendants., 2009 WL 5819738 (Trial Pleading) (E.D.Tex. Nov. 13, 2009) **Third Party Complaint of Best Western International, Inc.** (NO. 208CV00264)
  - 22 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendant., 2009 WL 5819739 (Trial Pleading) (E.D.Tex. Nov. 20, 2009) **Ramada Worldwide, Inc.'s Amended Answer to Complaint and Counterclaims** (NO. 208CV00264)
  - 23 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendant., 2009 WL 5819740 (Trial Pleading) (E.D.Tex. Nov. 20, 2009) **Ethostream, LLC's Amended Answer and Counterclaim** (NO. 208CV00264)
  - 24 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 3050903 (Trial Pleading) (E.D.Tex. May 7, 2010) **Best Western International, Inc.'s First Amended Answer, Defenses and Counterclaims** (NO. 208-CV-00264-TJW-CE)
  - 25 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. Best Western International, Inc., Third-Party Plaintiff, v. Bestcomm Networks, Inc. and Nomadix, Inc., Third-Party Defendants., 2010 WL 4953062 (Trial Pleading) (E.D.Tex. Oct. 7, 2010) **First Amended Third Party Complaint of Best Western International, Inc.** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)

#### E.D.Tex. Expert Testimony

- 26 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. And Related Counterclaims., 2008 WL 8039590 (Expert Report and Affidavit) (E.D.Tex. 2008) **Declaration of Tal Lavian, Ph.D. in Support of Plaintiff Linksmart Wireless Technology, LLC's Response to Defendants' Motion for Partial Summary Judgment of Invalidity for Indefiniteness Under 35 U.S.** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 27 LINKSMART WIRELESS TECHNOLOGIES, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 3711476 (Expert Report and Affidavit) (E.D.Tex. Apr. 14, 2010) **Declaration of Kevin Jeffay, Ph.D.** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)

- 28 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., Wayport, Inc., At&t, Inc., At&t Mobility, LLC, Lodgenet Interactive Corporation, Ibahn General Holdings Corp., Ethostream, LLC, Hot Point Wireless Inc., Netnearu Corp., Pronto Networks, Inc., Aptilo Networks, Inc., Freefi Networks,, 2010 WL 3842257 (Expert Deposition) (E.D.Tex. Apr. 22, 2010) (**Deposition of Kevin Jeffay, Ph.D.**) (NO. 208-CV-00264-TJW-CE)
- 29 LINKSMART WIRELESS TECHNOLOGY LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendant., 2010 WL 3711477 (Expert Report and Affidavit) (E.D.Tex. Apr. 30, 2010) **Declaration Of Tal Lavian, Ph.D. in Support of Plaintiff Linksmart Wireless Technology, LLC'S Reply Claim Construction Brief** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)

#### E.D.Tex. Trial Motions, Memoranda And Affidavits

- 30 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, Inc. et al., Defendants., 2008 WL 5369918 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Sep. 22, 2008) **Defendant At&T Mobility LLC's Motion to Dismiss** (NO. 208-CV-00264-TJW-CE)
- 31 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC.; et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. Cisco Systems, Inc.; Et Al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. SBC Internet Services, Inc. d/b/a AT&T Internet Services, Defendants;, 2009 WL 721149 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Jan. 23, 2009) **Joint Motion to Consolidate** (NO. 208-CV-002640TJW-CE, 208-CV-00304-DF-CE, 208-CV-00385-TJW, 209-CV-00026-TJW-CE)
- 32 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC.; et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. Cisco Systems, Inc.; et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. SBC Internet Services, Inc. d/b/a At&t Internet Services, Defendants;, 2009 WL 721433 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Jan. 23, 2009) **Joint Motion to Consolidate** (NO. 208-CV-00264-TJW-CE, 208-CV-00304-DF-CE, 208-CV-00385-TJW, 209-CV-00026-TJW-CE)
- 33 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2009 WL 714069 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Feb. 27, 2009) **Plaintiff Linksmart Wireless Technology, LLC's Motion for Default Judgment Against Hot Point Wireless, Inc. and Second Rule LLC** (NO. 208-CV-00264-DF-CE)
- 34 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al, Defendants. Best Western International, Inc., Third-Party Plaintiff, v. Bestcomm Networks, Inc. and Nomadix, Inc., Third-Party Defendants., 2010 WL 974673 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Feb. 25, 2010) **Third-Party Defendant Nomadix, Inc.'s Motion to Strike or Dismiss Third-Party Complaint of Best Western International, Inc.** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 35 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 2155255 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Mar. 19, 2010) **Plaintiff Linksmart Wireless Technology, LLC's Opening Claim Construction Brief** (NO. 208CV00264)
- 36 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. BEST WESTERN INTERNATIONAL, INC., Third-Party Plaintiff, v. BESTCOMM

- NETWORKS, INC. and Nomadix, Inc., Third-Party Defendants., 2010 WL 2155256 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Mar. 31, 2010) **Best Western International's Opposition to Nomadix's Motion to Strike or Dismiss Third Party Complaint** (NO. 208CV00264)
- 37 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. BEST WESTERN INTERNATIONAL, INC., Third-Party Plaintiff, v. BESTCOMM NETWORKS, NOMADIX, INC., Third-Party Defendants. BESTCOMM NETWORKS, INC., Third-Party Defendant, v. NOMADIX, INC., Third-Party Defendant., 2010 WL 2155257 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Apr. 16, 2010) **Nomadix, Inc.'s Motion to Dismiss Bestcomm Networks, Inc.'s Crossclaims** (NO. 208CV00264)
- 38 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 2155258 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Apr. 16, 2010) **Claim Construction Brief of Defendants** (NO. 208CV00264)
- 39 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 2155259 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Apr. 19, 2010) **Best Western's Supplemental Claim Construction Brief** (NO. 208CV00264)
- 40 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 2155260 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Apr. 29, 2010) **Defendants' Motion to Exclude the Expert Declaration of Dr. Tal Lavian in Support of Plaintiff's Claim Construction Reply Brief** (NO. 208CV00264)
- 41 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 2155261 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Apr. 30, 2010) **Plaintiff Linksmart Wireless Technology, LLC's Reply Claim Construction Brief** (NO. 208CV00264)
- 42 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. And Related Counterclaims., 2010 WL 3050762 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. May 7, 2010) **iBAHN's Claim Construction Surreply Brief** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 43 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. And Related Counterclaims., 2010 WL 3050763 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. May 11, 2010) **Claim Construction Sur-Reply Brief of Defendants** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 44 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 3050764 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. May 17, 2010) **Defendants' Motion for Partial Summary Judgment of Invalidity for Indefiniteness under 35 U.S.C. | 112, ¶2** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 45 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. And Related Counterclaims., 2010 WL 3050765 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. May 17, 2010) **Plaintiff Linksmart Wireless Technology, LLC's Response to Defendants' Motion to Exclude the Expert Declaration of Dr. Tal LA Vian Addressing the Declaration of Dr. Kevin Jeffay** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)

- 46 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al, Defendants. And Related Counterclaims., 2010 WL 3050766 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. May 23, 2010) **Plaintiff Linksmart Wireless Technology, LLC's Response to Defendants' Motion for Partial Summary Judgment of Invalidity for Indefiniteness under 35 U.S.C. | 112, ¶2** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 47 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al, Defendants., 2010 WL 3050767 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Jun. 2, 2010) **Defendants' Reply in Support of Their Motion for Partial Summary Judgment of Invalidity for Indefiniteness under 35 U.S.C. | 112, ¶2** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 48 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. And Related Counterclaims., 2010 WL 4927709 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Sep. 15, 2010) **Defendants' Motion for a Stay Pending the Reexamination of the Patent in Suit** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 49 LINKSMART WIRELESS TECHNOLOGY, LLC, Linksmart, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 4927710 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Oct. 7, 2010) **Defendant Choice Hotels International, Inc.'s Reply in Support of Its Motion for Summary Judgment of Non-Infringement** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)

#### **E.D.Tex. Exhibits**

- 50 LINKSMART WIRELESS TECHNOLOGY, LLC, v. T-MOBILE USA, INC. et al., 2010 WL 4024689 (Exhibit) (E.D.Tex. Mar. 31, 2010) **Direct Sales Agreement** (NO. 208CV00264)
- 51 LINKSMART WIRELESS TECHNOLOGY, LLC, v. T-MOBILE USA, INC. et al., 2010 WL 4024690 (Exhibit) (E.D.Tex. Mar. 31, 2010) **Nomadix, Inc. Reseller Agreement** (NO. 208CV00264)

#### **E.D.Tex. Expert Resumes**

- 52 Kevin Jeffay, curriculum vitae filed in Linksmart Wireless Technology, LLC V. T-Mobile USA, Inc. et al, 2010 WL 5779215 (Court-filed Expert Resume) (E.D.Tex. Jan. 18, 2010) **Expert Resume of Kevin Jeffay** (NO. 208CV00264)
- 53 Tal Lavian, Ph.D., curriculum vitae filed in Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc., et al, 2010 WL 3515006 (Court-filed Expert Resume) (E.D.Tex. May 23, 2010) **Expert Resume of Tal Lavian** (NO. 208CV00264)

#### **E.D.Tex. Trial Filings**

- 54 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. Cisco Systems, Inc., et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. SBC Internet Services, Inc. D/B/A AT&T Internet Services, Defendants;, 2009 WL 3147057 (Trial Filing) (E.D.Tex. Jun. 1, 2009)

- Joint Case Management Report** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 55 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. Cisco Systems, Inc., et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. SBC Internet Services, Inc. D/B/A AT&T Internet Services, Defendants,; 2009 WL 3147069 (Trial Filing) (E.D.Tex. Jun. 1, 2009) **Joint Case Management Report** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 56 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. Cisco Systems, Inc., et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. SBC Internet Services, Inc. D/B/A AT&T Internet Services, Defendants,; 2009 WL 3147139 (Trial Filing) (E.D.Tex. Jun. 1, 2009) **Joint Case Management Report** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 57 LINKSMART WIRELESS TECHNOLOGY, LLC, v. T-MOBILE USA, INC. et al., 2010 WL 1733529 (Trial Filing) (E.D.Tex. Feb. 19, 2010) **Claim Construction Chart** (NO. 208CV00264)
- 58 LINKSMART WIRELESS TECHNOLOGY, LLC, v. T-MOBILE USA, INC., et al., 2010 WL 3053062 (Trial Filing) (E.D.Tex. May 14, 2010) **Agreed Constructions** (NO. 08CV00264)

#### **E.D.Tex. Verdicts, Agreements and Settlements**

- 59 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC.; Wayport, Inc.; AT&T, Inc.; AT&T Mobility, LLC; Lodgenet Interactive Corp.; Ibahn General Holdings Corp.; Ethostream, LLC; Hot Point Wireless, Inc.; Netnearu Corp.; Pronto Networks, Inc.; Freefi Networks, Inc.; Meraki, Inc. Second, 2008 WL 5533263 (Verdict, Agreement and Settlement) (E.D.Tex. Dec. 9, 2008) **Jury** (NO. 208CV00264)
- 60 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. Cisco Systems, Inc., et al., Defendants; Linksmart Wireless Technology, LLC, Plaintiff, v. SBC Internet Services, Inc. d/b/a AT&T Internet Services, Defendants,; 2009 WL 3147112 (Verdict, Agreement and Settlement) (E.D.Tex. Jun. 1, 2009) **Joint Case Management Report** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 61 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. And Related Counterclaims., 2012 WL 2091453 (Verdict, Agreement and Settlement) (E.D.Tex. Apr. 4, 2012) **Joint Motion to Dismiss All Remaining Defendants** (NO. 208CV00264JRGRSP, 2:08-CV-00304-DF-CE, 2:08-CV-00385-DF-CE, 2:09-CV-00026-DF-CE)
- 62 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. Best Western International, Inc., Third-Party Plaintiff, v. Bestcomm Networks, Inc. and Nomadix, Inc., Third-Party Defendants. Bestcomm Networks, Inc., Third-Party Defendant, v. Nomadix, Inc., Third-Party Defen, 2012 WL 2091454 (Verdict, Agreement and Settlement) (E.D.Tex. Apr. 4, 2012) **Stipulated Dismissal of Third-Party Complaint and Cross Claim Without Prejudice** (NO. 2:08-CV-00264-DF-CE, 2:08-CV-00304-DF-CE, 2:08-CV-00385-DF-CE, 2:09-CV-00026-DF-CE)

**Dockets (U.S.A.)****E.D.Tex.**

- 63 LINKSMART WIRELESS TECHNOLOGY, LLC v. T-MOBILE USA, INC. ET AL, NO. 2:08cv00264 (Docket) (E.D.Tex. Jul. 1, 2008)

**Expert Court Documents (U.S.A.)****E.D.Tex. Expert Testimony**

- 64 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants. And Related Counterclaims., 2008 WL 8039590 (Expert Report and Affidavit) (E.D.Tex. 2008) **Declaration of Tal Lavian, Ph.D. in Support of Plaintiff Linksmart Wireless Technology, LLC's Response to Defendants' Motion for Partial Summary Judgment of Invalidity for Indefiniteness Under 35 U.S.** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 65 LINKSMART WIRELESS TECHNOLOGIES, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 3711476 (Expert Report and Affidavit) (E.D.Tex. Apr. 14, 2010) **Declaration of Kevin Jeffay, Ph.D.** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)
- 66 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., Wayport, Inc., At&t, Inc., At&t Mobility, LLC, Lodgenet Interactive Corporation, Ibahn General Holdings Corp., Ethostream, LLC, Hot Point Wireless Inc., Netnearu Corp., Pronto Networks, Ic., Aptilo Networks, Inc., Freefi Networks., 2010 WL 3842257 (Expert Deposition) (E.D.Tex. Apr. 22, 2010) **(Deposition of Kevin Jeffay, Ph.D.)** (NO. 208-CV-00264-TJW-CE)
- 67 LINKSMART WIRELESS TECHNOLOGY LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendant., 2010 WL 3711477 (Expert Report and Affidavit) (E.D.Tex. Apr. 30, 2010) **Declaration Of Tal Lavian, Ph.D. in Support of Plaintiff Linksmart Wireless Technology, LLC'S Reply Claim Construction Brief** (NO. 208-CV-00264-DF-CE, 208-CV-00304-DF-CE, 208-CV-00385-DF-CE, 209-CV-00026-DF-CE)

**E.D.Tex. Trial Motions, Memoranda And Affidavits**

- 68 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 2155260 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Apr. 29, 2010) **Defendants' Motion to Exclude the Expert Declaration of Dr. Tal Lavian in Support of Plaintiff's Claim Construction Reply Brief** (NO. 208CV00264)
- 69 LINKSMART WIRELESS TECHNOLOGY, LLC, Plaintiff, v. T-MOBILE USA, INC., et al., Defendants., 2010 WL 2155261 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Apr. 30, 2010) **Plaintiff Linksmart Wireless Technology, LLC's Reply Claim Construction Brief** (NO. 208CV00264)

**E.D.Tex. Expert Resumes**

© 2012 Thomson Reuters. All rights reserved.

- 70 Kevin Jeffay, curriculum vitae filed in Linksmart Wireless Technology, LLC V. T-Mobile USA, Inc. et al; 2010 WL 5779215 (Court-filed Expert Resume) (E.D.Tex. Jan. 18, 2010) **Expert Resume of Kevin Jeffay** (NO. 208CV00264)
- 71 Tal Lavian, Ph.D., curriculum vitae filed in Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc., et al, 2010 WL 3515006 (Court-filed Expert Resume) (E.D.Tex. May 23, 2010) **Expert Resume of Tal Lavian** (NO. 208CV00264)

**E.D.Tex.**

- 72 LINKSMART WIRELESS TECHNOLOGY, LLC v. T-MOBILE USA, INC. ET AL, NO. 2:08cv00264 (Docket) (E.D.Tex. Jul. 1, 2008)

**Patent Family**

- 73 AUTOMATIC DATA REDIRECTION SYSTEM FOR INTERNET COMMUNICATION, Derwent World Patents Legal 2000-072306+

**Assignments**

- 74 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).  
Number of Pages: 012, (DATE RECORDED: Jul 02, 2008)
- 75 ACTION: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).  
NUMBER OF PAGES: 003, (DATE RECORDED: Jun 29, 1999)

**Patent Status Files**

- .. Request for Re-Examination, (OG DATE: Apr 10, 2012)
- .. Re-Examination Certificate, (OG DATE: Mar 27, 2012)
- .. Patent Suit(See LitAlert Entries),
- .. Request for Re-Examination, (OG DATE: Dec 02, 2008)
- .. Patent Suit(See LitAlert Entries),

**Docket Summaries**

- 84 LINKSMART WIRELESS TECHNOLOGY LLC v. T-MOBILE USA INC ET AL, (C.D.CAL. Apr 05, 2012) (NO. 8:12CV00522), (28 USC 1331)
- 85 LINKSMART WIRELESS TECHNOLOGY LLC v. TJ HOSPITALITY LTD ET AL, (E.D.TEX. Jul 29, 2010) (NO. 2:10CV00277), (15 USC 1126 PATENT INFRINGEMENT)
- 86 LINKSMART WIRELESS TECHNOLOGY LLC v. SIX CONTINENTS HOTELS INC ET AL, (E.D.TEX. Jan 21, 2009) (NO. 2:09CV00026), (28 USC 1338 PATENT INFRINGEMENT)
- 87 LINKSMART WIRELESS TECHNOLOGY, LLC v. SBC INTERNET SERVICES, INC., (E.D.TEX. Oct 09, 2008) (NO. 2:08CV00385), (15 USC 1126 PATENT INFRINGEMENT)

- 88 LINKSMART WIRELESS TECHNOLOGY, LLC v. CISCO SYSTEMS, INC. ET AL, (E.D.TEX. Aug 04, 2008) (NO. 2:08CV00304), (35 USC 271 PATENT INFRINGEMENT)
- 89 LINKSMART WIRELESS TECHNOLOGY, LLC v. T-MOBILE USA, INC. ET AL, (E.D.TEX. Jul 01, 2008) (NO. 2:08CV00264), (15 USC 1126 PATENT INFRINGEMENT)

#### Litigation Alert

- 90 Derwent LitAlert P2012-16-134 (Apr 05, 2012) Action Taken: CAUSE - 28 USC 1331 - COMPLAINT FOR PATENT INFRINGEMENT
- 91 Derwent LitAlert P2010-36-12 (Jul 29, 2010) Action Taken: 15 USC 1126 - COMPLAINT FOR PATENT INFRINGEMENT
- 92 Derwent LitAlert P2009-07-58 (Jan 21, 2009) Action Taken: Complaint
- 93 Derwent LitAlert P2009-06-09 (Aug 04, 2008) Action Taken: Complaint
- 94 Derwent LitAlert P2008-47-12 (Jul 01, 2008) Action Taken: Complaint

#### Prior Art (Coverage Begins 1976)

- C** 95 METHOD OF PROVIDING TEMPORARY ACCESS OF A CALLING UNIT TO AN ANONYMOUS UNIT, US PAT 6157829 Assignee: Motorola, Inc., (U.S. PTO Utility 2000)
- C** 96 SECURITY SYSTEM FOR INTERNET PROVIDER TRANSACTION, US PAT 5845070 Assignee: Auric Web Systems, Inc., (U.S. PTO Utility 1998)
- C** 97 SYSTEM AND METHOD FOR DATABASE ACCESS CONTROL, US PAT 5696898 Assignee: Lucent Technologies Inc., (U.S. PTO Utility 1997)
- C** 98 SYSTEM AND METHOD FOR PROVIDING PEER LEVEL ACCESS CONTROL ON A NETWORK, US PAT 6233686 Assignee: AT & T Corp., (U.S. PTO Utility 2001)

© 2012 Thomson Reuters. All rights reserved.

Switch Client | Preferences | Help | Sign Out

<b>My Lexis™</b>	<b>Search</b>	<b>Get a Document</b>	<b>Shepard's®</b>	<b>More</b>	<b>History</b>	<b>Alerts</b>
------------------	---------------	-----------------------	-------------------	-------------	----------------	---------------

<b>All</b>	<b>Legal</b>	<b>News &amp; Business</b>	<b>Public Records</b>	<b>Patent Law</b>	<b>Find A Sour</b>	Add/Edit Subtabs
------------	--------------	----------------------------	-----------------------	-------------------	--------------------	------------------

Legal > / ... / > Utility, Design and Plant Patents

**Search** View Tutorial | Help

**Select Search Type and Enter Search Terms**

<b>Terms &amp; Connectors</b>	6779118 or 6,779,118	<input type="button" value="Suggest terms for my search"/>	<input type="button" value="Search"/>
<input type="checkbox"/> Natural Language		<input type="checkbox"/> Check spelling	
<input type="checkbox"/> Easy Search™			
<input type="checkbox"/> Semantic Search			
<input type="checkbox"/> What's this?			

**Restrict by Document Segment**

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment

**Note:** Segment availability differs between sources. Segments may not be applied consistently across sources.

**Restrict by Date**

No Date Restrictions  From  To  Date formats...

---

<p><b>Search Connectors</b></p> <p>and      and                      w/p      in same paragraph</p> <p>or        or                                  w/seg    in same segment</p> <p>w/N      within N words                  w/s      in same sentence</p> <p>pre/N    precedes by N words          and not   and not</p> <p>More Connectors &amp; Commands...</p>	<p><b>How Do I...?</b></p> <p>Combine sources?</p> <p>Restrict by date?</p> <p>Restrict by document segment?</p> <p>Use wildcards as placeholders for one or more characters in a search term?</p> <p>View Tutorials</p>
---	--

In

About LexisNexis | Privacy Policy | Terms & Conditions | Contact Us  
Copyright © 2012 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

Switch Client | Preferences | Help | Sign Out

<b>My Lexis™</b>	<b>Search</b>	<b>Get a Document</b>	<b>Shepard's®</b>	<b>More</b>	<b>History Alerts</b>
------------------	---------------	-----------------------	-------------------	-------------	-----------------------

**FOCUS™** Terms  Search Within   Using Semantic Concepts What's this? [Advanced...](#)

[View Tutorial](#)

Source: **Legal > / . . . / > Utility, Design and Plant Patents**

Terms: **6779118 or 6,779,118** (Suggest Terms for My Search)

Select for FOCUS™ or Delivery

1. 6,779,118, REEXAMINATION CERTIFICATE C1 (8926th), Mar. 27, 2012, User Specific Automatic Data Redirection System, Ikudome, Koichiro, Arcadia, California, United States Yeung, Moon Tai, Alhambra, California, United States, Linksmart Wireless Technology, LLC, Pasadena, California, United States

... Patent No.: **6,779,118** ...

2. 6,130,892, REEXAMINATION CERTIFICATE C1 (7203rd), Dec. 1, 2009, Nomadic Translator Or Router, Short, Joel E., Los Angeles, California, United States Kleinrock, Leonard, Los Angeles, California, United States, Nomadix, Inc., Westlake Village, California, United States

... **6,779,118** B1 8/2004 Ikudome et al. ...

3. 8196180, June 5, 2012, Authorization and authentication of user access to a distributed network communication system with roaming feature, Keeler, James D., Austin, Texas, United States of America(US), United States of America(); Krenzer, Matthew M., Cedar Park, Texas, United States of America(US), United States of America(); 556620, Wayport, Inc., Foreign company or corporation

**CORE TERMS:** network, provider, user's, wireless, roaming, identification, internet, authentication, partner, channel, software, message, wired, geographic, computer, password, username, customer's, session, router, card, web, memory, airport, subscriber, computing, authorization, billing, send, server

... 6636894, October 21, 2003, Short et al., United States of America (US) **6779118**, August 17, 2004, Ikudome et al., United States of America (US) 6804720, ...

4. 8156246, April 10, 2012, Systems and methods for providing content and services on a network system, Short, Joel E., Los Angeles, California, United States of America(US), United States of America(); Pagan, Florence C. I., Los Angeles, California, United States of America(US), United States of America(); Goldstein, Josh J., Agoura Hills, California, United States of America(US), United States of America(); 244866, NOMADIX, Inc., Agoura Hills, California, United States of America(US), United States company or corporation

**CORE TERMS:** network, user, gateway, computer, subscriber, packet, router, server, profile, host, database, internet, nomadic, billing, bandwidth, communicate, destination, authorization, online, protocol, hotel, port, authentication, control

panel, provider, pop-up, configured, xml, computer system, portable

... States of America (US) 6779035, August 17, 2004, Gbadegesin, United States of America (US) **6779118**, August 17, 2004, Ikudome et al., United States of America (US), 726#7 ...

5. 8027339, September 27, 2011, System and method for establishing network connection, Short, Joel E., Los Angeles, California, United States of America(US), United States of America(US); Kleinrock, Leonard, Los Angeles, California, United States of America(US), United States of America(US); 240427, September 29, 2008, ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., NOMADIX, INC., SUITE 100, 1100 BUSINESS CENTER CIRCLE, NEWBURY PARK, CALIFORNIA, UNITED STATES OF AMERICA(US), 91320, reel-frame:021601/0450, NOMADIX, Inc., Agoura Hills, California, United States of America(US), United States company or corporation

**CORE TERMS:** router, nomadic, network, host, computer, packet, user, protocol, layer, interface, mobile, translation, terminal, configured, internet, module, card, destination, functionality, automatically, substrate, remote, wireless, laptop, transport, software, utilize, stored, communicate, processing

... States of America (US) 6775267, August 10, 2004, Kung, United States of America (US) **6779118**, August 17, 2004, Ikudome et al., United States of America (US) 6785730, ...

6. 7925693, April 12, 2011, NAT access control with IPSec, Swander, Brian, Bellevue, WASHINGTON, United States of America(US), United States of America(US); Lamb, Richard, Seattle, WASHINGTON, United States of America(US), United States of America(US); Guzovsky, Eduard, Weston, MASSACHUSETTS, United States of America(US), United States of America(US); 627510, March 19, 2007, ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., MICROSOFT CORPORATION, ONE MICROSOFT WAY, REDMOND, WASHINGTON, UNITED STATES OF AMERICA(US), 98052, reel-frame:019029/0931, Microsoft Corporation, Redmond, WASHINGTON, United States of America(US), United States company or corporation

**CORE TERMS:** gateway, network, packet, computer, server, destination, memory, media, bus, interface, user, session, disk, disk drive, filtering, magnetic, remote, wireless, storage, module, credential, personal computer, optical, proxy, exemplary, port, appreciated, protocol, computer-readable, additionally

... 6742044, May 25, 2004, Aviani et al., United States of America (US) **6779118**, August 17, 2004, Ikudome et al., United States of America (US) 7051365, ...

7. 7921175, April 5, 2011, Requesting a service from a service providing apparatus by a service request apparatus, Noguchi, Toshiyuki, Ohta-ku, Japan(JP), Japan(JP); 563093, December 30, 2005, ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., CANON KABUSHIKI KAISHA, 3-30-2, SHIMOMARUKO, OHTA-KU, TOKYO, JAPAN( ), reel-frame:017436/0875, Canon Kabushiki Kaisha, Tokyo, Japan(JP), Foreign company or corporation

**CORE TERMS:** printer, ink, server, tank, support service, terminal, user, retailer, numeral, denotes, www, display, expendable, browser, displayed, monitor, acquired, network, disk, button, icon, launched, driver, print, specifying, interface,

recording, software, medium, recommendation

6310692, October 30, 2001, Fan et al., United States of America (US) **6779118**, August 17, 2004, Ikudome et al., United States of America (US) 6782495, ...



8. 7853523, December 14, 2010, Secure networked transaction system, Krueger, Scott, 630 Grenfall Rd., #14, Palm Springs, California, United States of America (US), 92262, United States of America(); Goodman, Daniel, 17241 NE. 13th Ave., N. Miami Beach, Florida, United States of America(US), 33162, United States of America(); 356868, January 27, 2009, ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., DEBIT.NET, INC., 16750 NE 10TH AVENUE, NORTH MIAMI BEACH, FLORIDA, UNITED STATES OF AMERICA(US), 33162, reel-frame:022159/0572; March 24, 2009, ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., UCETRANS KG, LIMITED LIABILITY COMPANY, 160 GREENTREE DRIVE, SUITE 101, DOVER, DELAWARE, UNITED STATES OF AMERICA(US), 19904, reel-frame:022445/0053, KRUEGER SCOTT; GOODMAN DANIEL

**CORE TERMS:** verification, merchant's, card, customer, computer, debit, user, string, pin, credit cards, web, identifier, network, account number, processing, backbone, site, server, expiration date, trusted, browser, optionally, processor, redirect, retrieve, passing, message, bank, financial institutions, computer system

... 6636833, October 21, 2003, Flitcroft et al., United States of America (US) **6779118**, August 17, 2004, Ikudome et al., United States of America (US) 6789068, ...



9. 7765593, July 27, 2010, Rule set-based system and method for advanced virus protection, Lowe, Joseph C., Aloha, Oregon, United States of America(US), United States of America(); Edwards, Jonathan L., Portland, Oregon, United States of America(US), United States of America(); Woodruff, Andrew A., Portland, Oregon, United States of America(US), United States of America(); Spurlock, Joel R., Portland, Oregon, United States of America(US), United States of America(); 876524, June 24, 2004, ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., NETWORKS ASSOCIATES TECHNOLOGY, INC., 3965 FREEDOM CIRCLE, SANTA CLARA, CALIFORNIA, UNITED STATES OF AMERICA(US), 95054, reel-frame:015523/0373; June 23, 2005, MERGER (SEE DOCUMENT FOR DETAILS)., MCAFEE, INC., 3965 FREEDOM CIRCLE, SANTA CLARA, CALIFORNIA, UNITED STATES OF AMERICA(US), 95054, reel-frame:016646/0513, McAfee, Inc., Santa Clara, California, United States of America(US), United States company or corporation

**CORE TERMS:** network, computer, malware, user, executable, directory, attachment, sending, virus, unrecognized, electronic, internet, message, infected, viruses, interface, e-mail, communicating, mass-mailing-type, graphical, infection, protocol, remote, aforementioned, port, optionally, utilizing, spread, white list, conditionally

... States of America (US) 6611925, August 26, 2003, Spear, United States of America (US) **6779118**, August 17, 2004, Ikudome et al., United States of America (US) 6954858, ...



10. 7748028, June 29, 2010, Authentication method, terminal device, relay device and authentication server, Sato, Atsushi, Yokohama-shi, Japan(JP), Japan(JP); Noguchi,

Katsuhiro, Yokohama-shi, Japan(JP), Japan(JP); Aono, Hiroshi, Yokohama-shi, Japan(JP), Japan(JP); Ohtsuki, Katsunobu, Yokohama-shi, Japan(JP), Japan(JP); 167345, August 22, 2005, ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., NTT DOCOMO, INC., 11-1, NAGATACHO 2-CHOME, CHIYODA-KU, TOKYO 100-6150, JAPAN( ), reel-frame:016910/0266, NTT DoCoMo, Inc., Tokyo, Japan(JP), Foreign company or corporation

**CORE TERMS:** authentication, server, user, terminal, processing, proxy, configured, network, forward, relay, telecommunications, communicate, carrier, storage unit, forwarding, transmitting, randomly, performing, information received, transmitter, travel, generating, gateway, update, information transmitted, above-described, tunnel, aaa, communicating, periodically

... 6643782, November 4, 2003, Jin et al., United States of America (US)  
**6779118**, August 17, 2004, Ikudome et al., United States of America (US)  
7184418, ...

Source: **Legal > / . . . / > Utility, Design and Plant Patents** 

Terms: **6779118 or 6,779,118** (Suggest Terms for My Search)

View: Cite

Date/Time: Tuesday, July 10, 2012 - 10:00 AM EDT

In

About LexisNexis | Privacy Policy | Terms & Conditions | Contact Us  
Copyright © 2012 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

My Lexis™ Search Get a Document Shepard's® More History Alerts

All Legal News & Business Public Records Patent Law Find A Sour Add/Edit Subtabs

Legal > Area of Law - By Topic > Patent Law > Find Cases > Patent Cases, Administrative Decisions and Regulatory Materials

**Search** View Tutorial | Help

**Broaden this search with additional sources**

- Patent Cases, Administrative Decisions and Regulatory Materials (Source you selected)
- Chisum on Patents
- Patent Law Digest
- Patent Case Management Judicial Guide
- Intellectual Property Counseling and Litigation
- Court of Appeals for the Federal Circuit Practice & Procedure

[View all sources](#)

**Select Search Type and Enter Search Terms**

<b>Terms &amp; Connectors</b>	6779118 or 6,779,118	<input type="button" value="Search"/>
Natural Language		Suggest terms for my search
Easy Search™		Check spelling

**Restrict by Document Segment**

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment

**Note:** Segment availability differs between sources. Segments may not be applied consistently across sources.

**Restrict by Date**

No Date Restrictions  From  To  Date formats...

---

<p><b>Search Connectors</b></p> <p>and    and                    w/p    in same paragraph</p> <p>or     or                        w/seg   in same segment</p> <p>w/N    within N words            w/s    in same sentence</p> <p>pre/N   precedes by N words   and not   and not</p> <p><a href="#">More Connectors &amp; Commands...</a></p>	<p><b>How Do I...?</b></p> <p>Combine sources?</p> <p>Restrict by date?</p> <p>Restrict by document segment?</p> <p>Use wildcards as placeholders for one or more characters in a search term?</p> <p><a href="#">View Tutorials</a></p>
---	--

In

<b>My Lexis™</b>	<b>Search</b>	<b>Get a Document</b>	<b>Shepard's®</b>	<b>More</b>	<b>History Alerts</b>
------------------	---------------	-----------------------	-------------------	-------------	-----------------------

**FOCUS™** Terms  Search Within Original Results (1 - 3)  View Tutorial

Source: **Legal > Area of Law - By Topic > Patent Law > Find Cases > Patent Cases, Administrative Decisions and Regulatory Materials** 

Terms: **6779118 or 6,779,118** (Suggest Terms for My Search)

 Select for FOCUS™ or Delivery

-  1. Nomadix, Inc. v. Hewlett-Packard Co., Case No. CV 09-08441 DDP (VBKx), UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA, 2012 U.S. Dist. LEXIS 40154, March 22, 2012, Decided, March 22, 2012, Filed, Motion denied by Nomadix, Inc. v. Hewlett-Packard Co., 2012 U.S. Dist. LEXIS 64101 (C.D. Cal., May 7, 2012)

**CORE TERMS:** invalidity, prior art, patent, discovery, good cause, supplemental, deposition, diligence, invalid, deposed ...

... U.S. Patent No. 6,636,894 ("894 Patent") is invalid in light of U.S. Patent No. **6,779,118** ("118 Patent"); and 2) U.S. Patent No. 7,689,716 ("716 Patent") ...

-  2. Linksmart Wireless Tech., LLC v. T-Mobile USA, Inc., CASE NO. 2:08-CV-264-DF-CE, UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS, MARSHALL DIVISION, 2010 U.S. Dist. LEXIS 65424, June 30, 2010, Decided, June 30, 2010, Filed, Magistrate's recommendation at Linksmart Wireless Tech., LLC v. T-Mobile USA, Inc., 2010 U.S. Dist. LEXIS 101444 (E.D. Tex., Sept. 1, 2010)

**CORE TERMS:** user, server, network, redirection, specification, assigned, session, database, individualized, invention ...

... Networks, Inc. infringe various claims of United States Patent No. **6,779,118** ("the '118 patent"). This memorandum addresses the parties' various claim ...

- 3. Ex parte LINKSMART WIRELESS TECHNOLOGY, LLC (U.S. Patent 6,779,118), Appeal 2011-009566 Reexamination 90/009,301 Technology Center 3900, Board of Patent Appeals and Interferences, 2011 Pat. App. LEXIS 21572, August 23, 2011, Decided

**CORE TERMS:** server, redirection, user, network, examiner, authentication, individualized, credential, database, teach ...

... K. Ikudome & M.T. Yeung, User specific automatic data redirection system, US **6,779,118** B1 (granted 17 August 2004). OPINION INTRODUCTION Rejections ...

Source: **Legal > Area of Law - By Topic > Patent Law > Find Cases > Patent Cases, Administrative Decisions and Regulatory Materials** 

Terms: **6779118 or 6,779,118** (Suggest Terms for My Search)

View: Cite

Date/Time: Tuesday, July 10, 2012 - 10:00 AM EDT

\* Signal Legend:

-  - Warning: Negative treatment is indicated
  -  - Questioned: Validity questioned by citing refs
  -  - Caution: Possible negative treatment
  -  - Positive treatment is indicated
  -  - Citing Refs. With Analysis Available
  -  - Citation information available
- \* Click on any *Shepard's* signal to *Shepardize*® that case.

In

About LexisNexis | Privacy Policy | Terms & Conditions | Contact Us  
Copyright © 2012 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

Switch Client | Preferences | Help | Sign Out

<b>My Lexis™</b>	<b>Search</b>	<b>Get a Document</b>	<b>Shepard's®</b>	<b>More</b>	<b>History</b>	<b>Alerts</b>
<b>All</b>	<b>Legal</b>	<b>News &amp; Business</b>	<b>Public Records</b>	<b>Patent Law</b>	<b>Find A Sour</b>	Add/Edit Subtabs

Legal > Area of Law - By Topic > Patent Law > Search News > Patent, Trademark & Copyright Periodicals, Combined

**Search** View Tutorial | Help

**Select Search Type and Enter Search Terms**

<b>Terms &amp; Connectors</b>	6779118 or 6,779,118	Suggest terms for my search
Natural Language		Check spelling
Easy Search™		

**Search**

**Restrict by Document Segment**

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment  **Add**

**Note:** Segment availability differs between sources. Segments may not be applied consistently across sources.

**Restrict by Date**

No Date Restrictions  From  To  Date formats...

---

<p><b>Search Connectors</b></p> <p>and      and                      w/p      in same paragraph</p> <p>or        or                                w/seg    in same segment</p> <p>w/N      within N words                w/s      in same sentence</p> <p>pre/N    precedes by N words        and not    and not</p> <p>More Connectors &amp; Commands...</p>	<p><b>How Do I...?</b></p> <p>Combine sources?</p> <p>Restrict by date?</p> <p>Restrict by document segment?</p> <p>Use wildcards as placeholders for one or more characters in a search term?</p> <p>View Tutorials</p>
--	--

In

About LexisNexis | Privacy Policy | Terms & Conditions | Contact Us  
Copyright © 2012 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

<p><b>No Documents Found</b></p> <p>No documents were found for your search terms <b>"6779118 or 6,779,118"</b></p> <p>Click "Save this search as an Alert" to schedule your search to run in the future.</p> <p>- OR -</p> <p>Click "Search Using Natural Language" to run your search as Natural Language search.</p> <p>- OR -</p> <p>Click "Edit Search" to return to the search form and modify your search.</p> <p>Suggestions:</p> <ul style="list-style-type: none"><li>● Check for spelling errors.</li><li>● Remove some search terms.</li><li>● Use more common search terms, such as those listed in "Suggested Words and Concepts."</li><li>● Use a less restrictive date range.</li><li>● Use "OR" in between terms to search for one term or the other.</li></ul> <p>  <a href="#">Save this Search as an Alert</a>    <a href="#">Search Using Natural Language</a>    <a href="#">Edit Search</a>  </p>
--

In

[About LexisNexis](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Contact Us](#)  
Copyright © 2012 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

<b>My Lexis™</b>	<b>Search</b>	<b>Get a Document</b>	<b>Shepard's®</b>	<b>More</b>	<b>History</b>	<b>Alerts</b>
<b>All</b>	<b>Legal</b>	<b>News &amp; Business</b>	<b>Public Records</b>	<b>Patent Law</b>	<b>Find A Sour</b>	Add/Edit Subtabs

News & Business > Combined Sources > News, All (English, Full Text)

**Search** View Tutorial | Help

**Select Search Type and Enter Search Terms**

<b>Terms &amp; Connectors</b>	6779118 or 6,779,118	<input type="button" value="Suggest terms for my search"/>	<input type="button" value="Search"/>
<input type="checkbox"/> Natural Language		<input type="checkbox"/> Check spelling	
<input type="checkbox"/> Easy Search™			

**Restrict by Document Segment**

Select a document segment, enter search terms for the segment, then click Add.

**Note:** Segment availability differs between sources. Segments may not be applied consistently across sources.

**Restrict by Date**

No Date Restrictions  From  To  Date formats...

---

<p><b>Search Connectors</b></p> <p>and      and                      w/p      in same paragraph</p> <p>or        or                                w/seg    in same segment</p> <p>w/N      within N words                w/s      in same sentence</p> <p>pre/N    precedes by N words        and not    and not</p> <p>More Connectors &amp; Commands...</p>	<p><b>How Do I...?</b></p> <p>Combine sources?</p> <p>Restrict by date?</p> <p>Restrict by document segment?</p> <p>Use wildcards as placeholders for one or more characters in a search term?</p> <p>View Tutorials</p>
--	--

In

Switch Client | Preferences | Help | Sign Out

<b>My Lexis™</b>	<b>Search</b>	<b>Get a Document</b>	<b>Shepard's®</b>	<b>More</b>	<b>History</b>
					<b>Alerts</b>

**FOCUS™** Terms  Search Within Original Results (1 - 5)  View Tutorial  
 Advanced...

Source: **News & Business > Combined Sources > News, All (English, Full Text)** 

Terms: **6779118 or 6,779,118** (Suggest Terms for My Search)

Duplicate Options **off**

 What's this?

 Select for FOCUS™ or Delivery

- 1. Patent Law Practice Center, July 3, 2012 Tuesday 6:06 PM EST, , 684 words, Google Request for Reexamination of Walker Digital Patent, among those Filed Week of June 25, 2012  
  
... HyTest Oy. (3) 90/012,378 (electronically filed) U.S. Patent No. **6,779,118** entitled USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM and owned by Linksmart ...
- 2. Patent Law Practice Center, June 12, 2012 Tuesday 5:52 AM EST, , 676 words, Troll Busters® Attack on Nucleic Acid Patent One of the Reexamination Requests Filed the Week of June 4, 2012  
  
... Troll Busters. (7) 90/012,342 (electronically filed) U.S. Patent No. **6,779,118** entitled USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM and owned by Linksmart ...
- 3. Patent Law Practice Center, February 18, 2011 Friday 7:33 AM EST, , 895 words, Facebook Challenges To Three æHuman Relationships Patents, Among Reexamination Requests Filed Week Of FEBRUARY 7th, Stefanie Levine  
  
... 2011. (9) 90/011,485 (electronically filed) " U.S. Patent No. **6,779,118** entitled USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM and owned by Koichiro ...
- 4. Southeast Texas Record, August 5, 2010 Thursday, 2048 words, Recent patent infringement/false marking cases filed in the Eastern District of Texas, Michelle Massey, East Texas Bureau  
  
... Inc.The plaintiff alleges that the defendants are willfully infringing on U.S. Patent No. **6,779,118** issued on Aug. 17, 2004 for User Specific Automatic Data ...
- 5. PR Newswire US, May 8, 2007 Tuesday 11:00 AM GMT, , 2229 words, NxStage Medical Reports First Quarter 2007 Results; Company Signs Six Strategic Agreements in Q1 to Drive Growth and Increase Gross Margins , LAWRENCE, Mass. May 8  
  
... Other assets **6,779,118** 546,178 ...

Source: **News & Business > Combined Sources > News, All (English, Full Text)** 

Terms: **6779118 or 6,779,118** (Suggest Terms for My Search)

View: Cite

Date/Time: Tuesday, July 10, 2012 - 10:00 AM EDT

In

[About LexisNexis](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Contact Us](#)  
Copyright © 2012 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

---

**US District Court Civil Docket**

**U.S. District - California Central  
(Southern Division)**

**8:12cv522**

**Linksmart Wireless Technology Llc v. T-Mobile USA Inc et al**

**This case was retrieved from the court on Tuesday, July 10, 2012**

---

<b>Date Filed: 04/05/2012</b>	<b>Class Code: OPEN</b>
<b>Assigned To: Judge Josephine Staton Tucker</b>	<b>Closed: No</b>
<b>Referred To: Magistrate Judge Arthur Nakazato</b>	<b>Statute: 28:1331</b>
<b>Nature of suit: Patent (830)</b>	<b>Jury Demand: Both</b>
<b>Cause: Fed. Question: Trademark</b>	<b>Demand Amount: \$75,000</b>
<b>Lead Docket: None</b>	<b>NOS Description: Patent</b>
<b>Other Docket: None</b>	
<b>Jurisdiction: Federal Question</b>	

**Litigants**

**Attorneys**

Linksmart Wireless Technology Llc  
Plaintiff

Andrew David Weiss  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12th Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
fax: 310-826-6991  
email: Aweiss@raklaw.Com

Irene Y Lee  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: ILEE@RAKLAW.COM

Marc A Fenster  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: MFENSTER@RAKLAW.COM

T-Mobile USA Inc  
Defendant

Adam P Romero  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP

399 Park Avenue  
New York , NY 10022  
USA  
212-295-6422  
fax: 212-230-8888  
<i>pro Hac Vice</ I>  
email: Adam.Romero@wilmerhale.Com

David Bassett  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
399 Park Avenue  
New York , NY 10022  
USA  
212-230-8800  
fax: 212-230-8888  
<i>pro Hac Vice</ I>  
email: David.Bassett@wilmerhale.Com

Erin Greenfield Mehta  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
399 Park Avenue  
New York , NY 10022  
USA  
212-295-644  
fax: 213-230-8888  
<i>pro Hac Vice</ I>  
email: Erin.Mehta@wilmerhale.Com

Kate Saxton  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
60 State Street  
Boston , MA 02109  
USA  
617-526-6253  
fax: 617-526-5000  
<i>pro Hac Vice</ I>  
email: Kate.Saxton@wilmerhale.Com

Michael D Jay  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
350 South Grand Avenue Suite 2100  
Los Angeles , CA 90071  
USA  
213-443-5300  
fax: 213-443-5400  
email: Michael.Jay@wilmerhale.Com

Noah A Levine  
[COR LD NTC]  
Wilmer Cutler Pickering Hale & Dorr  
399 Park Avenue  
New York , NY 10022  
USA  
212-230-8875  
fax: 212-230-8888  
<i>pro Hac Vice</ I>  
email: Noah.Levine@wilmerhale.Com

Sadaf R Abdullah  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
399 Park Avenue  
New York , NY 10022

Lodgenet Interactive Corp  
Defendant

USA  
212-937-7247  
fax: 212-230-8888  
<i>pro Hac Vice</ I>  
email: Sadaf.Abdullah@wilmerhale.Com

Douglas J Beteta  
[COR LD NTC]  
Morrison and Foerster LLP  
555 West 5TH Street Suite 3500  
Los Angeles , CA 90013-1024  
USA  
213-892-5200  
Fax: 213-892-5454  
Email: DBETETA@MOFO.COM

Mark E Ungerman  
[COR LD NTC]  
Morrison and Foerster LLP  
2000 Pennsylvania Avenue Nw  
suite 5500  
Washington , DC 20006-1888  
USA  
202-887-1535  
fax: 202-887-0763  
email: Mungerman@mofo.Com

Ibahn General Holdings Corp  
Defendant

Grant E Kinsel  
[COR LD NTC]  
Perkins Coie LLP  
1888 Century Park East Suite 1700  
Los Angeles , CA 90067  
USA  
310-788-3215  
Fax: 310-843-1273  
Email: GKINSEL@PERKINSCOIE.COM

Michael D Broaddus  
[COR LD NTC]  
Perkins Coie LLP  
1201 Third Avenue Suite 4900  
Seattle , WA 98101-3099  
USA  
206-359-8694  
fax: 206-359-9694  
<i>pro Hac Vice</ I>  
email: Mbroaddus@perkinscoie.Com

Ethostream Llc  
Defendant

Brian G Gilpin  
[COR LD NTC]  
Godfrey and Kahn SC  
780 North Water Street  
Milwaukee , WI 53202  
USA  
414-273-3500  
fax: 414-273-5198  
<i>pro Hac Vice</ I>  
email: Bgilpin@gklaw.Com

David M Stein  
[COR LD NTC]  
Akin Gump Strauss Hauer and Feld LLP  
633 West Fifth Street Suite 5000  
Los Angeles , CA 90071

USA  
213-254-1200  
fax: 213-229-1001  
email: Dstein@akingump.Com

James D Peterson  
[COR LD NTC]  
Godfrey and Kahn SC  
One East Main Street  
po Box 2719  
Madison , WI 53701-2719  
USA  
608-257-3911  
fax: 608-257-0609  
<i>pro Hac Vice</ I>  
email: Jpeterson@gklaw.Com

Ramada Worldwide Inc  
Defendant

Brian G Gilpin  
[COR LD NTC]  
Godfrey and Kahn SC  
780 North Water Street  
Milwaukee , WI 53202  
USA  
414-273-3500  
fax: 414-273-5198  
<i>pro Hac Vice</ I>  
email: Bgilpin@gklaw.Com

David M Stein  
[COR LD NTC]  
Akin Gump Strauss Hauer and Feld LLP  
633 West Fifth Street Suite 5000  
Los Angeles , CA 90071  
USA  
213-254-1200  
fax: 213-229-1001  
email: Dstein@akingump.Com

James D Peterson  
[COR LD NTC]  
Godfrey and Kahn SC  
One East Main Street  
po Box 2719  
Madison , WI 53701-2719  
USA  
608-257-3911  
fax: 608-257-0609  
<i>pro Hac Vice</ I>  
email: Jpeterson@gklaw.Com

Marriott International Inc  
Defendant

Brian M Koide  
[COR LD NTC]  
Crowell and Moring LLP  
1001 Pennsylvania Avenue NW  
Washington , DC 20004  
USA  
202-624-2931  
Fax: 949-263-8414  
<i>pro Hac Vice</ I>  
Email: BKOIDE@CROWELL.COM

Craig P Lytle  
[COR LD NTC]  
Crowell and Moring LLP  
1001 Pennsylvania Avenue Nw

Washington , DC 20004  
USA  
202-624-2533  
fax: 202-628-5116  
<i>pro Hac Vice</ I>  
email: Clytle@crowell.Com

Jeffrey Ahdoot  
[COR LD NTC]  
Crowell and Moring LLP  
1001 Pennsylvania Avenue Nw  
Washington , DC 20004  
USA  
202-624-2500  
fax: 202-628-5116  
<i>pro Hac Vice</ I>  
email: Jahdoot@crowell.Com

John L Cuddihy  
[COR LD NTC]  
Crowell and Moring LLP  
1001 Pennsylvania Avenue Nw  
Washington , DC 20004  
USA  
202-624-2500  
fax: 202-628-5116  
<i>pro Hac Vice</ I>  
email: Jcuddihy@crowell.Com

John S Gibson  
[COR LD NTC]  
Crowell and Moring LLP  
3 Park Plaza 20th Floor  
Irvine , CA 92614-8414  
USA  
949-263-8400  
fax: 949-263-8414  
email: Jgibson@crowell.Com

Six Continents Hotels Inc  
Defendant

Erin Paige Gibson  
[COR LD NTC]  
Dla Piper LLP (Us)  
401 B Street, Ste 1700  
San Diego , CA 92101  
USA  
619-699-2862  
email: Erin.Gibson@dlapiper.Com

John M Guaragna  
[COR LD NTC]  
Gray Cary Ware & Freidenrich  
4365 Executive Drive, Ste 1100  
San Diego , CA 92121-2133  
USA  
858-677-1400  
Email: JOHN.GUARAGNA@DLAPIPER.COM

Intercontinental Hotels Group Resources Inc  
Defendant

Erin Paige Gibson  
[COR LD NTC]  
Dla Piper LLP (Us)  
401 B Street, Ste 1700  
San Diego , CA 92101  
USA  
619-699-2862  
email: Erin.Gibson@dlapiper.Com

John M Guaragna  
[COR LD NTC]  
Gray Cary Ware & Freidenrich  
4365 Executive Drive, Ste 1100  
San Diego , CA 92121-2133  
USA  
858-677-1400  
Email: JOHN.GUARAGNA@DLAPIPER.COM

Choice Hotels International Inc  
Defendant

George B Newhouse , Jr  
[COR LD NTC]  
Brown White and Newhouse LLP  
333 South Hope Street 40th Floor  
Los Angeles , CA 90071-1406  
USA  
213-613-9474  
fax: 213-613-0550  
email: Gnewhouse@brownwhitelaw.Com

Gregory R Lyons  
[COR LD NTC]  
Wiley Rein LLP  
1776 K Street Nw  
Washington , DC 20006  
USA  
202-719-7000  
fax: 202-719-7049  
<i>pro Hac Vice</ I>  
email: Glyons@wileyrein.Com

Kevin P Anderson  
[COR LD NTC]  
Wiley Rein LLP  
1776 K Street NW  
Washington , DC 20006  
USA  
202-719-7000  
Fax: 202-719-7049  
<i>pro Hac Vice</ I>  
Email: KANDERSON@WILEYREIN.COM

Best Western International Inc  
Defendant

David E Rogers  
[COR LD NTC]  
Snell and Wilmer LLP  
400 East Van Buren  
Phoenix , AZ 85004-2202  
USA  
602-382-6225  
fax: 602-382-6070  
<i>pro Hac Vice</ I>  
email: Drogers@swlaw.Com

Elizabeth M Weldon  
[COR LD NTC]  
Snell and Wilmer LLP  
600 Anton Boulevard Suite 1400  
Costa Mesa , CA 92626-7689  
USA  
714-427-7000  
Fax: 714-427-7799  
Email: EWELDON@SWLAW.COM

Sid Leach  
[COR LD NTC]



Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: MFENSTER@RAKLAW.COM

Six Continents Hotels Inc  
Counter Claimant

Erin Paige Gibson  
[COR LD NTC]  
Dla Piper LLP (Us)  
401 B Street, Ste 1700  
San Diego , CA 92101  
USA  
619-699-2862  
email: Erin.Gibson@dlapiper.Com

John M Guaragna  
[COR LD NTC]  
Gray Cary Ware & Freidenrich  
4365 Executive Drive, Ste 1100  
San Diego , CA 92121-2133  
USA  
858-677-1400  
Email: JOHN.GUARAGNA@DLAPIPER.COM

Intercontinental Hotels Group Resources Inc  
Counter Claimant

Erin Paige Gibson  
[COR LD NTC]  
Dla Piper LLP (Us)  
401 B Street, Ste 1700  
San Diego , CA 92101  
USA  
619-699-2862  
email: Erin.Gibson@dlapiper.Com

John M Guaragna  
[COR LD NTC]  
Gray Cary Ware & Freidenrich  
4365 Executive Drive, Ste 1100  
San Diego , CA 92121-2133  
USA  
858-677-1400  
Email: JOHN.GUARAGNA@DLAPIPER.COM

Linksmart Wireless Technology Llc  
Counter Defendant

Andrew David Weiss  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12th Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
fax: 310-826-6991  
email: Aweiss@raklaw.Com

Irene Y Lee  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: ILEE@RAKLAW.COM

Marc A Fenster  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: MFENSTER@RAKLAW.COM

Ramada Worldwide Inc  
Counter Claimant

Brian G Gilpin  
[COR LD NTC]  
Godfrey and Kahn SC  
780 North Water Street  
Milwaukee , WI 53202  
USA  
414-273-3500  
fax: 414-273-5198  
<i>pro Hac Vice</ I>  
email: Bgilpin@gklaw.Com

David M Stein  
[COR LD NTC]  
Akin Gump Strauss Hauer and Feld LLP  
633 West Fifth Street Suite 5000  
Los Angeles , CA 90071  
USA  
213-254-1200  
fax: 213-229-1001  
email: Dstein@akingump.Com

James D Peterson  
[COR LD NTC]  
Godfrey and Kahn SC  
One East Main Street  
po Box 2719  
Madison , WI 53701-2719  
USA  
608-257-3911  
fax: 608-257-0609  
<i>pro Hac Vice</ I>  
email: Jpeterson@gklaw.Com

Linksmart Wireless Technology Llc  
Counter Defendant

Andrew David Weiss  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12th Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
fax: 310-826-6991  
email: Aweiss@raklaw.Com

Irene Y Lee  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: ILEE@RAKLAW.COM

Marc A Fenster  
[COR LD NTC]

Ethostream Llc  
Counter Claimant

Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: MFENSTER@RAKLAW.COM

Brian G Gilpin  
[COR LD NTC]  
Godfrey and Kahn SC  
780 North Water Street  
Milwaukee , WI 53202  
USA  
414-273-3500  
fax: 414-273-5198  
<i>pro Hac Vice</ I>  
email: Bgilpin@gklaw.Com

David M Stein  
[COR LD NTC]  
Akin Gump Strauss Hauer and Feld LLP  
633 West Fifth Street Suite 5000  
Los Angeles , CA 90071  
USA  
213-254-1200  
fax: 213-229-1001  
email: Dstein@akingump.Com

James D Peterson  
[COR LD NTC]  
Godfrey and Kahn SC  
One East Main Street  
po Box 2719  
Madison , WI 53701-2719  
USA  
608-257-3911  
fax: 608-257-0609  
<i>pro Hac Vice</ I>  
email: Jpeterson@gklaw.Com

Linksmart Wireless Technology Llc  
Counter Defendant

Andrew David Weiss  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12th Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
fax: 310-826-6991  
email: Aweiss@raklaw.Com

Irene Y Lee  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: ILEE@RAKLAW.COM

Marc A Fenster  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor

T-Mobile USA Inc  
Counter Claimant

Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: MFENSTER@RAKLAW.COM

Adam P Romero  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
399 Park Avenue  
New York , NY 10022  
USA  
212-295-6422  
fax: 212-230-8888  
<i>pro Hac Vice</ I>  
email: Adam.Romero@wilmerhale.Com

David Bassett  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
399 Park Avenue  
New York , NY 10022  
USA  
212-230-8800  
fax: 212-230-8888  
<i>pro Hac Vice</ I>  
email: David.Bassett@wilmerhale.Com

Erin Greenfield Mehta  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
399 Park Avenue  
New York , NY 10022  
USA  
212-295-644  
fax: 213-230-8888  
<i>pro Hac Vice</ I>  
email: Erin.Mehta@wilmerhale.Com

Kate Saxton  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
60 State Street  
Boston , MA 02109  
USA  
617-526-6253  
fax: 617-526-5000  
<i>pro Hac Vice</ I>  
email: Kate.Saxton@wilmerhale.Com

Michael D Jay  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
350 South Grand Avenue Suite 2100  
Los Angeles , CA 90071  
USA  
213-443-5300  
fax: 213-443-5400  
email: Michael.Jay@wilmerhale.Com

Noah A Levine  
[COR LD NTC]  
Wilmer Cutler Pickering Hale & Dorr  
399 Park Avenue  
New York , NY 10022  
USA

212-230-8875  
fax: 212-230-8888  
<i>pro Hac Vice</ I>  
email: Noah.Levine@wilmerhale.Com

Sadaf R Abdullah  
[COR LD NTC]  
Wilmer Cutler Pickering Hale and Dorr LLP  
399 Park Avenue  
New York , NY 10022  
USA  
212-937-7247  
fax: 212-230-8888  
<i>pro Hac Vice</ I>  
email: Sadaf.Abdullah@wilmerhale.Com

Linksmart Wireless Technology Llc  
Counter Defendant

Andrew David Weiss  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12th Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
fax: 310-826-6991  
email: Aweiss@raklaw.Com

Irene Y Lee  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: ILEE@RAKLAW.COM

Marc A Fenster  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: MFENSTER@RAKLAW.COM

Marriott International Inc  
Counter Claimant

Brian M Koide  
[COR LD NTC]  
Crowell and Moring LLP  
1001 Pennsylvania Avenue NW  
Washington , DC 20004  
USA  
202-624-2931  
Fax: 949-263-8414  
<i>pro Hac Vice</ I>  
Email: BKOIDE@CROWELL.COM

Craig P Lytle  
[COR LD NTC]  
Crowell and Moring LLP  
1001 Pennsylvania Avenue Nw  
Washington , DC 20004  
USA  
202-624-2533  
fax: 202-628-5116

<i>pro Hac Vice</ I>  
email: Clytle@crowell.Com

Jeffrey Ahdoot  
[COR LD NTC]  
Crowell and Moring LLP  
1001 Pennsylvania Avenue Nw  
Washington , DC 20004  
USA  
202-624-2500  
fax: 202-628-5116  
<i>pro Hac Vice</ I>  
email: Jahdoot@crowell.Com

John L Cuddihy  
[COR LD NTC]  
Crowell and Moring LLP  
1001 Pennsylvania Avenue Nw  
Washington , DC 20004  
USA  
202-624-2500  
fax: 202-628-5116  
<i>pro Hac Vice</ I>  
email: Jcuddihy@crowell.Com

John S Gibson  
[COR LD NTC]  
Crowell and Moring LLP  
3 Park Plaza 20th Floor  
Irvine , CA 92614-8414  
USA  
949-263-8400  
fax: 949-263-8414  
email: Jgibson@crowell.Com

Linksmart Wireless Technology Llc  
Counter Defendant

Andrew David Weiss  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12th Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
fax: 310-826-6991  
email: Aweiss@raklaw.Com

Irene Y Lee  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: ILEE@RAKLAW.COM

Marc A Fenster  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: MFENSTER@RAKLAW.COM

Lodgenet Interactive Corp  
Counter Claimant

Douglas J Beteta  
[COR LD NTC]  
Morrison and Foerster LLP  
555 West 5TH Street Suite 3500  
Los Angeles , CA 90013-1024  
USA  
213-892-5200  
Fax: 213-892-5454  
Email: DBETETA@MOFO.COM

Mark E Ungerman  
[COR LD NTC]  
Morrison and Foerster LLP  
2000 Pennsylvania Avenue Nw  
suite 5500  
Washington , DC 20006-1888  
USA  
202-887-1535  
fax: 202-887-0763  
email: Mungerman@mofocom

Linksmart Wireless Technology Llc  
Counter Defendant

Andrew David Weiss  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12th Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
fax: 310-826-6991  
email: Aweiss@raklaw.com

Irene Y Lee  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: ILEE@RAKLAW.COM

Marc A Fenster  
[COR LD NTC]  
Russ August and Kabat  
12424 Wilshire Boulevard 12TH Floor  
Los Angeles , CA 90025  
USA  
310-826-7474  
Fax: 310-826-6991  
Email: MFENSTER@RAKLAW.COM

Date	#	Proceeding Text	Source
04/05/2012	1	COMPLAINT against Defendants Best Western International Inc, Choice Hotels International Inc, Ethostream LLC, Ibahn General Holdings Corp, Intercontinental Hotels Group Resources Inc, Lodgenet Interactive Corp, Marriott International Inc, Ramada Worldwide Inc, Six Continents Hotels Inc and T-Mobile USA Inc. Case assigned to Judge Josephine Staton Tucker for all further proceedings. Discovery referred to Magistrate Judge Arthur Nakazato.(Filing fee \$ 350 Paid). Jury Demanded. Filed by Plaintiff Linksmart Wireless Technology LLC.(lwag) (lwag). (Entered: 04/06/2012)	
04/05/2012	--	21 DAY Summons Issued re Complaint - (Discovery), Complaint - (Discovery), Complaint - (Discovery) 1 as to Defendants Best Western International Inc, Choice Hotels International Inc, Ethostream LLC, Ibahn General Holdings Corp, Intercontinental Hotels Group Resources Inc, Lodgenet Interactive Corp, Marriott International Inc, Ramada Worldwide Inc, Six Continents Hotels Inc and T-Mobile USA Inc. (lwag) (Entered: 04/06/2012)	

- 04/06/2012)
- 04/05/2012 2 CERTIFICATION and Notice of Interested Parties filed by Plaintiff Linksmart Wireless Technology LLC. (lwag) (lwag). (Entered: 04/06/2012)
- 04/05/2012 3 NOTICE of Related Case(s) filed by Plaintiff Linksmart Wireless Technology LLC. Related Case(s): 2:08-cv-00264-JRG-RSP; 2:09-cv-00026-DF-CE; 2:08-cv-00385-DF-CE and 2:08-cv-00304-DF-CE. (lwag) (lwag). (Entered: 04/06/2012)
- 04/05/2012 4 REPORT ON THE FILING OF AN ACTION Regarding a Patent or a Trademark (Initial Notification) filed by Linksmart Wireless Technology LLC. (lwag) (Entered: 04/06/2012)
- 04/05/2012 5 NOTICE TO PARTIES OF COURT-DIRECTED ADR PROGRAM filed.(lwag) (Entered: 04/06/2012)
- 04/09/2012 6 INITIAL STANDING ORDER for cases assigned to Judge Josephine Staton Tucker. (Guerrero, Terry) (Entered: 04/09/2012)
- 04/17/2012 7 PROOF OF SERVICE Executed by Plaintiff Linksmart Wireless Technology LLC, upon Defendant T-Mobile USA Inc served on 4/10/2012, answer due 5/1/2012. Service of the Summons and Complaint were executed upon Counsel Pursuant to Stipulation Dated 4/3/2012 attached to Complaint as Exhibit B in compliance with Federal Rules of Civil Procedure by service on a domestic corporation, unincorporated association, or public entity. Original Summons NOT returned. (Weiss, Andrew) (Entered: 04/17/2012)
- 04/17/2012 8 PROOF OF SERVICE Executed by Plaintiff Linksmart Wireless Technology LLC, upon Defendant Lodgenet Interactive Corp served on 4/10/2012, answer due 5/1/2012. Service of the Summons and Complaint were executed upon Counsel Pursuant to Stipulation Dated 4/3/2012 attached to Complaint as Exhibit B in compliance with Federal Rules of Civil Procedure by service on a domestic corporation, unincorporated association, or public entity. Original Summons NOT returned. (Weiss, Andrew) (Entered: 04/17/2012)
- 04/17/2012 9 PROOF OF SERVICE Executed by Plaintiff Linksmart Wireless Technology LLC, upon Defendant Ibahn General Holdings Corp served on 4/10/2012, answer due 5/1/2012. Service of the Summons and Complaint were executed upon Counsel Pursuant to Stipulation Dated 4/3/2012 attached to Complaint as Exhibit B in compliance with Federal Rules of Civil Procedure by service on a domestic corporation, unincorporated association, or public entity. Original Summons NOT returned. (Weiss, Andrew) (Entered: 04/17/2012)
- 04/17/2012 10 PROOF OF SERVICE Executed by Plaintiff Linksmart Wireless Technology LLC, upon Defendant Ethostream LLC served on 4/10/2012, answer due 5/1/2012. Service of the Summons and Complaint were executed upon Counsel Pursuant to Stipulation Dated 4/3/2012 attached to Complaint as Exhibit B in compliance with Federal Rules of Civil Procedure by method of service not specified. Original Summons NOT returned. (Weiss, Andrew) (Entered: 04/17/2012)
- 04/17/2012 11 PROOF OF SERVICE Executed by Plaintiff Linksmart Wireless Technology LLC, upon Defendant Ramada Worldwide Inc served on 4/10/2012, answer due 5/1/2012. Service of the Summons and Complaint were executed upon Counsel Pursuant to Stipulation Dated 4/3/2012 attached to Complaint as Exhibit B in compliance with Federal Rules of Civil Procedure by service on a domestic corporation, unincorporated association, or public entity. Original Summons NOT returned. (Weiss, Andrew) (Entered: 04/17/2012)
- 04/17/2012 12 PROOF OF SERVICE Executed by Plaintiff Linksmart Wireless Technology LLC, upon Defendant Marriott International Inc served on 4/10/2012, answer due 5/1/2012. Service of the Summons and Complaint were executed upon Counsel Pursuant to Stipulation Dated 4/3/2012 attached to Complaint as Exhibit B in compliance with Federal Rules of Civil Procedure by service on a domestic corporation, unincorporated association, or public entity. Original Summons NOT returned. (Weiss, Andrew) (Entered: 04/17/2012)
- 04/17/2012 13 PROOF OF SERVICE Executed by Plaintiff Linksmart Wireless Technology LLC, upon Defendant Six Continents Hotels Inc served on 4/10/2012, answer due 5/1/2012. Service of the Summons and Complaint were executed upon Counsel Pursuant to Stipulation Dated 4/3/2012 attached to Complaint as Exhibit B in compliance with Federal Rules of Civil Procedure by service on a domestic corporation, unincorporated association, or public entity. Original Summons NOT returned. (Weiss, Andrew) (Entered: 04/17/2012)
- 04/17/2012 14 PROOF OF SERVICE Executed by Plaintiff Linksmart Wireless Technology LLC, upon Defendant Intercontinental Hotels Group Resources Inc served on 4/10/2012, answer due 5/1/2012. Service of the Summons and Complaint were executed upon Counsel Pursuant to Stipulation Dated 4/3/2012 attached to Complaint as Exhibit B in compliance with Federal Rules of Civil Procedure by service on a domestic corporation,

- unincorporated association, or public entity. Original Summons NOT returned. (Weiss, Andrew) (Entered: 04/17/2012)
- 04/17/2012 15 PROOF OF SERVICE Executed by Plaintiff Linksmart Wireless Technology LLC, upon Defendant Choice Hotels International Inc served on 4/10/2012, answer due 5/1/2012. Service of the Summons and Complaint were executed upon Counsel Pursuant to Stipulation Dated 4/3/2012 attached to Complaint as Exhibit B in compliance with Federal Rules of Civil Procedure by service on a domestic corporation, unincorporated association, or public entity. Original Summons NOT returned. (Weiss, Andrew) (Entered: 04/17/2012)
- 04/17/2012 16 PROOF OF SERVICE Executed by Plaintiff Linksmart Wireless Technology LLC, upon Defendant Best Western International Inc served on 4/10/2012, answer due 5/1/2012. Service of the Summons and Complaint were executed upon Counsel Pursuant to Stipulation Dated 4/3/2012 attached to Complaint as Exhibit B in compliance with Federal Rules of Civil Procedure by service on a domestic corporation, unincorporated association, or public entity. Original Summons NOT returned. (Weiss, Andrew) (Entered: 04/17/2012)
- 04/30/2012 17 NOTICE OF MOTION AND MOTION for Extend Time to File Answer to 6/11/2012 re Complaint - (Discovery), Complaint - (Discovery), Complaint - (Discovery) 1 filed by Plaintiff Linksmart Wireless Technology LLC. Motion set for hearing on 6/4/2012 at 10:00 AM before Judge Josephine Staton Tucker. (Attachments: # 1 Proposed Order)(Weiss, Andrew) (Entered: 04/30/2012)
- 05/01/2012 18 MINUTES (IN CHAMBERS): ORDER by Judge Josephine Staton Tucker: STRIKING NOTICE AND CONSENT TO EXTEND TIME 17 : (See document for details.) The Court orders the motion stricken, and orders Plaintiff's counsel to review carefully the local rules and this Court's ISO. (rla) (Entered: 05/02/2012)
- 05/08/2012 19 STIPULATION for Extension of Time to File Answer to 6/11/2012 re Complaint - (Discovery), Complaint - (Discovery), Complaint - (Discovery) 1 filed by Plaintiff Linksmart Wireless Technology LLC. (Attachments: # 1 Proposed Order EXHIBIT A) (Weiss, Andrew) (Entered: 05/08/2012)
- 05/08/2012 20 APPLICATION for attorney David E. Rogers to Appear Pro Hac Vice(PHV Fee of \$325 receipt number 0973-10343977 paid.) filed by Defendant Best Western International Inc. (Attachments: # 1 Proposed Order)(Weldon, Elizabeth) (Entered: 05/08/2012)
- 05/09/2012 21 ORDER by Judge Josephine Staton Tucker: GRANTING Stipulation to Extend Time to Respond to Complaint 19 . The time for Defendants to answer to Plaintiff's Complaint for Patent Infringement Permanent Injunction and Damages shall be extended up to and including June 11, 2012. (rla) (Entered: 05/10/2012)
- 05/09/2012 23 ORDER by Judge Josephine Staton Tucker: granting 20 Application to Appear Pro Hac Vice by Attorney David E. Rogers on behalf of Defendant Best Western International, Inc., designating Elizabeth M. Weldon as local counsel. (lt) (Entered: 05/11/2012)
- 05/11/2012 22 APPLICATION for attorney Michael D. Broaddus to Appear Pro Hac Vice(PHV Fee of \$325 receipt number 0973-10359988 paid.) filed by defendant Ibahn General Holdings Corp. (Attachments: # 1 Proposed Order)(Kinsel, Grant) (Entered: 05/11/2012)
- 05/11/2012 24 APPLICATION for attorney Sid Leach to Appear Pro Hac Vice(PHV Fee of \$325 receipt number 0973-10363942 paid.) filed by Defendant Best Western International Inc. (Attachments: # 1 Proposed Order)(Weldon, Elizabeth) (Entered: 05/11/2012)
- 05/14/2012 25 APPLICATION for attorney Craig Lytle to Appear Pro Hac Vice. (PHV FEE PAID.) filed by defendant Marriott International Inc. Lodged order. (twdb) (Entered: 05/15/2012)
- 05/14/2012 26 APPLICATION for attorney Jeffrey Ahdoot to Appear Pro Hac Vice. (PHV FEE PAID.) filed by defendant Marriott International Inc. Lodged order. (twdb) (Entered: 05/15/2012)
- 05/14/2012 27 APPLICATION for attorney John Cuddihy to Appear Pro Hac Vice. (PHV FEE PAID.) filed by defendant Marriott International Inc. Lodged order. (twdb) (Entered: 05/15/2012)
- 05/17/2012 28 APPLICATION for attorney Kevin P. Anderson to Appear Pro Hac Vice. (PHV FEE PAID.) filed by defendant Choice Hotels International Inc. (nca) (Entered: 05/21/2012)
- 05/17/2012 29 APPLICATION for attorney Gregory R. Lyons to Appear Pro Hac Vice. (PHV FEE PAID.) filed by defendant Choice Hotels International Inc. (nca) (Entered: 05/21/2012)
- 05/24/2012 30 APPLICATION for attorney Brian M. Koide to Appear Pro Hac Vice. (PHV FEE PAID.) filed by defendant Marriott International Inc. Lodged order. (twdb) (Entered: 05/25/2012)
- 06/06/2012 31 ORDER by Judge Josephine Staton Tucker: granting 22 Application to Appear Pro Hac Vice by Attorney Michael D. Broaddus on behalf of iBAHN General Holding Corp,

- designating Grant E. Kinsel as local counsel. (It) (Entered: 06/07/2012)
- 06/06/2012 32 ORDER by Judge Josephine Staton Tucker: granting 24 Application to Appear Pro Hac Vice by Attorney Sid Leach on behalf of Defendant Best Western International, Inc., designating Elizabeth M. Weldon as local counsel. (It) (Entered: 06/07/2012)
- 06/06/2012 33 ORDER by Judge Josephine Staton Tucker: granting 25 Application to Appear Pro Hac Vice by Attorney Craig Lytle on behalf of Defendant Marriott International, Inc., designating John S. Gibson as local counsel. (It) (Entered: 06/07/2012)
- 06/06/2012 34 ORDER by Judge Josephine Staton Tucker: granting 27 Application to Appear Pro Hac Vice by Attorney John Cuddihay on behalf of Defendant Marriott International, Inc., designating John S. Gibson as local counsel. (It) (Entered: 06/07/2012)
- 06/06/2012 35 ORDER by Judge Josephine Staton Tucker: granting 29 Application to Appear Pro Hac Vice by Attorney Gregory R. Lyons on behalf of Defendant Choice Hotels International, Inc., designating George B. Newhouse, Jr. as local counsel. (It) (Entered: 06/07/2012)
- 06/06/2012 36 ORDER by Judge Josephine Staton Tucker: granting 26 Application to Appear Pro Hac Vice by Attorney Jeffrey Abbot on behalf of Defendant Marriott International, Inc., designating John S. Gibson as local counsel. (It) (Entered: 06/07/2012)
- 06/06/2012 37 ORDER by Judge Josephine Staton Tucker: granting 30 Application to Appear Pro Hac Vice by Attorney Brian Koide on behalf of Defendant Marriott International, Inc., designating John S. Gibson as local counsel. (It) (Entered: 06/07/2012)
- 06/06/2012 38 ORDER by Judge Josephine Staton Tucker: granting 28 Application to Appear Pro Hac Vice by Attorney Kevin P. Anderson on behalf of Defendant Choice Hotels International, Inc., designating George B. Newhouse, Jr. as local counsel. (It) (Entered: 06/07/2012)
- 06/11/2012 39 NOTICE of Manual Filing filed by Defendant Best Western International Inc of Answer, Defenses and Counterclaims. (Rogers, David) (Entered: 06/11/2012)
- 06/11/2012 40 NOTICE of Appearance filed by attorney David M Stein on behalf of Defendants Ethostream LLC, Ramada Worldwide Inc (Stein, David) (Entered: 06/11/2012)
- 06/11/2012 41 Certification and Notice of Interested Parties filed by Defendant Best Western International Inc, identifying Best Western International, Inc.. (Rogers, David) (Entered: 06/11/2012)
- 06/11/2012 42 ANSWER to Complaint - (Discovery), Complaint - (Discovery), Complaint - (Discovery) 1 filed by Defendant Ibahn General Holdings Corp.(Kinsel, Grant) (Entered: 06/11/2012)
- 06/11/2012 43 NOTICE of Manual Filing filed by Defendant T-Mobile USA Inc of Defendant T-Mobile USA, Inc.s Answer And Counterclaims; Defendant T-Mobile USA, Inc.s Corporate Disclosure Statement Pursuant To Federal Rules Of Civil Procedure 7.1 And Certification As To Interested Parties Pursuant To Local Rule 7.1-1; Proof Of Service. (Jay, Michael) (Entered: 06/11/2012)
- 06/11/2012 44 NOTICE of Manual Filing filed by Defendants Ethostream LLC, Ramada Worldwide Inc of Defendant Ramada Worldwide, Inc.'s Answer and Counterclaims; Defendant EthoStream, LLC's Answer and Counterclaims. (Stein, David) (Entered: 06/11/2012)
- 06/11/2012 45 ANSWER to Complaint - (Discovery), Complaint - (Discovery), Complaint - (Discovery) 1 with JURY DEMAND filed by Defendant Choice Hotels International Inc.(Newhouse, George) (Entered: 06/11/2012)
- 06/11/2012 46 CORPORATE DISCLOSURE STATEMENT filed by Defendant Choice Hotels International Inc (Newhouse, George) (Entered: 06/11/2012)
- 06/11/2012 47 Certificate and Notice of Interested Parties filed by Defendant Choice Hotels International Inc, (Newhouse, George) (Entered: 06/11/2012)
- 06/11/2012 48 NOTICE of Manual Filing filed by Defendant Marriott International Inc of Marriott International, Inc.'s Answer and Counterclaims to Linksmart Wireless Technology, LLC's Complaint. (Gibson, John) (Entered: 06/11/2012)
- 06/11/2012 49 NOTICE of Appearance filed by attorney John S Gibson on behalf of Defendant Marriott International Inc (Gibson, John) (Entered: 06/11/2012)
- 06/11/2012 50 Certification and Notice of Interested Parties filed by Defendant Marriott International Inc, identifying T.Rowe Price Associates, Inc.. (Gibson, John) (Entered: 06/11/2012)
- 06/11/2012 51 CORPORATE DISCLOSURE STATEMENT Pursuant to Fed. R. Civ. P. 7.1 filed by Defendant Marriott International Inc (Gibson, John) (Entered: 06/11/2012)
- 06/11/2012 52 Certificate of Interested Parties filed by Defendant Ibahn General Holdings Corp, (Kinsel,

- Grant) (Entered: 06/11/2012)
- 06/11/2012 53 STIPULATION Extending Time to Answer the complaint as to Lodgenet Interactive Corp answer now due 6/21/2012, filed by Plaintiff Linksmart Wireless Technology LLC. (Attachments: # 1 Proposed Order re Stipulation)(Weiss, Andrew) (Entered: 06/11/2012)
- 06/11/2012 54 CORPORATE DISCLOSURE STATEMENT filed by Defendant Ethostream LLC (Stein, David) (Entered: 06/11/2012)
- 06/11/2012 55 CORPORATE DISCLOSURE STATEMENT filed by Defendant Ramada Worldwide Inc (Stein, David) (Entered: 06/11/2012)
- 06/11/2012 56 Certification and Notice of Interested Parties filed by Defendant Ramada Worldwide Inc, (Stein, David) (Entered: 06/11/2012)
- 06/11/2012 57 Certification and Notice of Interested Parties filed by Defendant Ethostream LLC, (Stein, David) (Entered: 06/11/2012)
- 06/11/2012 58 ANSWER to Complaint - (Discovery) 1 and COUNTERCLAIM against Linksmart Wireless Technology LLC filed by defendant Best Western International Inc.(twdb) (Entered: 06/12/2012)
- 06/11/2012 59 PROOF OF SERVICE filed by defendants Intercontinental Hotels Group Resources Inc, Six Continents Hotels Inc, served on 06/11/2012. (db) (Entered: 06/13/2012)
- 06/11/2012 61 RULE 7.1 DISCLOSURE STATEMENT; filed by Defendants Intercontinental Hotels Group Resources Inc, Six Continents Hotels Inc (rla) (Entered: 06/13/2012)
- 06/11/2012 62 ANSWER to Complaint (Discovery) 1 , AND COUNTERCLAIM against Linksmart Wireless Technology LLC; filed by defendants Six Continents Hotels Inc, Intercontinental Hotels Group Resources Inc.(rla) (Entered: 06/13/2012)
- 06/11/2012 63 ANSWER to Complaint - (Discovery) 1 , and COUNTERCLAIM against Linksmart Wireless Technology LLC; filed by defendant Ramada Worldwide Inc.(rla) (Entered: 06/13/2012)
- 06/11/2012 64 ANSWER to Complaint - (Discovery) 1 , and COUNTERCLAIM against Linksmart Wireless Technology LLC; filed by defendant Ethostream LLC.(rla) Modified on 6/13/2012 (rla). (Entered: 06/13/2012)
- 06/11/2012 65 ANSWER to Complaint - (Discovery) 1 , and COUNTERCLAIM against Linksmart Wireless Technology LLC; filed by defendant T-Mobile USA Inc.(rla) (Entered: 06/13/2012)
- 06/11/2012 66 ANSWER to Complaint - (Discovery) 1 , and COUNTERCLAIM against Linksmart Wireless Technology LLC; filed by defendant Marriott International Inc.(rla) (Entered: 06/13/2012)
- 06/11/2012 67 DEMAND for Jury Trial; filed by defendant Ibahn General Holdings Corp.(rla) (Entered: 06/13/2012)
- 06/11/2012 68 CORPORATE DISCLOSURE STATMENT AND CERTIFICATION of Interested Parties; filed by defendant T-Mobile USA Inc, identifying Corporate Parent Deutsche Telekom AG, Corporate Parent T-Mobile Global Zwischenholding GmbH, Corporate Parent T-Mobile Global Holding GmbH, a German entity for T-Mobile USA Inc. (rla) (Entered: 06/13/2012)
- 06/11/2012 69 PROOF OF SERVICE of MANUALLY FILED DOCUMENTS filed by defendant/counterclaimant Marriott International Inc, ANSWER AND COUNTERCLAIMS served on 06/11/12. (rla) (Entered: 06/13/2012)
- 06/11/2012 70 PROOF OF SERVICE filed by defendant T-Mobile USA Inc, ANSWER AND COUNTERCLAIMS, AND CORPORATE DISCLOSURE STATEMENT AND CERTIFICATION AS TO INTERESTED PARTIES; served on 5/18/12. (rla) (Entered: 06/13/2012)
- 06/13/2012 60 ORDER granting Stipulation Extending Time to Respond to Complaint 53 by Judge Josephine Staton Tucker: The time for LodgeNet Interactive Corporation to answer Plaintiff's Complaint for Patent Infringement Permanent Injunction And Damages shall be extended up to and including June 21, 2012. (rla) (Entered: 06/13/2012)
- 06/14/2012 71 Defendant EthoStream, LLC's Demand For Trial by Jury re: Answer to Complaint (Discovery), Counterclaim 64 (Stein, David) (Entered: 06/14/2012)
- 06/14/2012 72 Defendant Ramada Worldwide, Inc.'s Demand For Trial by Jury re: Answer to Complaint (Discovery), Counterclaim 63 (Stein, David) (Entered: 06/14/2012)
- 06/21/2012 73 NOTICE of Manual Filing filed by Defendant Lodgenet Interactive Corp of Defendant Lodgenet Interactive Corp.'s Answer and Counterclaim to Complaint. (Beteta, Douglas)



- 07/02/2012 91 APPLICATION for attorney KATE SAXTON to Appear Pro Hac Vice(PHV Fee of \$325 receipt number 0973-10608931 paid.) filed by DEFENDANT T-Mobile USA Inc. (Attachments: # 1 Proposed Order ORDER ON APPLICATION OF NON-RESIDENT ATTORNEY TO APPEAR IN A SPECIFIC CASE)(Jay, Michael) (Entered: 07/02/2012)
- 07/05/2012 92 Linksmart's ANSWER to Answer to Complaint (Discovery), Counterclaim 64 filed by Plaintiff Linksmart Wireless Technology LLC.(Fenster, Marc) (Entered: 07/05/2012)
- 07/05/2012 93 Linksmart's ANSWER to Answer to Complaint (Discovery), Counterclaim 63 filed by Plaintiff Linksmart Wireless Technology LLC.(Fenster, Marc) (Entered: 07/05/2012)
- 07/05/2012 94 Linksmart's ANSWER to Answer to Complaint (Discovery), Counterclaim 58 filed by Plaintiff Linksmart Wireless Technology LLC.(Fenster, Marc) (Entered: 07/05/2012)
- 07/05/2012 95 Linksmart's ANSWER to Answer to Complaint (Discovery), Counterclaim 66 filed by Plaintiff Linksmart Wireless Technology LLC.(Fenster, Marc) (Entered: 07/05/2012)
- 07/05/2012 96 Linksmart's ANSWER to Answer to Complaint (Discovery), Counterclaim 65 filed by Plaintiff Linksmart Wireless Technology LLC.(Fenster, Marc) (Entered: 07/05/2012)
- 07/05/2012 97 ANSWER Linksmart filed by Plaintiff Linksmart Wireless Technology LLC.(Fenster, Marc) (Entered: 07/05/2012)
- 07/05/2012 98 ORDER by Judge Josephine Staton Tucker: granting 86 Application to Appear Pro Hac Vice by Attorney Erin Greenfield Mehta on behalf of Defendant T-Mobile, designating Michael D. Jay as local counsel. (It) (Entered: 07/06/2012)
- 07/05/2012 99 ORDER by Judge Josephine Staton Tucker: granting 87 Application to Appear Pro Hac Vice by Attorney Sadaf R. Abdullah on behalf of Defendant T-Mobile, designating Michael D. Jay as local counsel. (It) (Entered: 07/06/2012)
- 07/05/2012 100 ORDER by Judge Josephine Staton Tucker: granting 88 Application to Appear Pro Hac Vice by Attorney David B. Bassett on behalf of Defendant T-Mobile, designating Michael D. Jay as local counsel. (It) (Entered: 07/06/2012)
- 07/05/2012 101 ORDER by Judge Josephine Staton Tucker: granting 89 Application to Appear Pro Hac Vice by Attorney Adam Romero on behalf of Defendant T-Mobile, designating Michael D. Jay as local counsel. (It) (Entered: 07/06/2012)
- 07/05/2012 102 ORDER by Judge Josephine Staton Tucker: granting 90 Application to Appear Pro Hac Vice by Attorney Noah A. Levine on behalf of Defendant T-Mobile, designating Michael D. Jay as local counsel. (It) (Entered: 07/06/2012)
- 07/05/2012 103 ORDER by Judge Josephine Staton Tucker: granting 91 Application to Appear Pro Hac Vice by Attorney Kate Saxton on behalf of Defendant T-Mobile, designating Michael D. Jay as local counsel. (It) (Entered: 07/06/2012)

---

Copyright © 2012 LexisNexis CourtLink, Inc. All rights reserved.  
\*\*\* THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY \*\*\*

---

**US District Court Civil Docket**

**U.S. District - Texas Eastern  
(Marshall)**

**2:10cv277**

**Linksmart Wireless Technology Llc VS TJ Hospitality Ltd et al**

This case was retrieved from the court on Tuesday, July 10, 2012

---

<b>Date Filed: 07/29/2010</b>	<b>Class Code: CLOSED</b>
<b>Assigned To: Judge T John Ward</b>	<b>Closed: Yes</b>
<b>Referred To:</b>	<b>Statute: 15:1126</b>
<b>Nature of suit: Patent (830)</b>	<b>Jury Demand: Plaintiff</b>
<b>Cause: Patent Infringement</b>	<b>Demand Amount: \$0</b>
<b>Lead Docket: None</b>	<b>NOS Description: Patent</b>
<b>Other Docket: None</b>	
<b>Jurisdiction: Federal Question</b>	

**Litigants**

**Attorneys**

Linksmart Wireless Technology, Llc  
Plaintiff

Marc A Fenster  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
12TH Floor  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: Mfenster@raklaw.com

Tj Hospitality Ltd  
[Term: 11/30/2010]  
Defendant

Mmd Hotel Kilgore LP  
[Term: 11/30/2010]  
Defendant

Heritage Inn Number Xiv  
[Term: 11/30/2010]  
Defendant

Eight Pack Tyler LP  
[Term: 11/30/2010]  
Defendant

Heritage Inn Number X  
[Term: 11/30/2010]  
Defendant

B D & Sons Ltd  
[Term: 11/30/2010]  
Defendant





- 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 26 ORDER - granting 16 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant I-30 Hospitality LLC are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 27 ORDER - granting 17 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant Jyotika A. Patel are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 28 ORDER - granting 20 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant Meritax, LLC are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 29 ORDER - granting 14 Notice of Dismissal. All claims asserted by Plaintiff against Defendant Heritage Inn Number XIV are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 30 ORDER - granting 12 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant Heritage Inn Number X are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 31 ORDER - granting 13 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant Heritage Inn Number XII are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 32 ORDER - granting 15 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant Hwy 259 Lodging LLC are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 33 ORDER - granting 10 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant Carlex Hospitality LLC are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 34 ORDER - granting 11 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant Eight Pack Tyler LP are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 35 ORDER - granting 21 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant MMD Hotel Kilgore LP are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 36 ORDER - granting 18 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant Krishan Inc. are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Magistrate Judge Charles Everingham on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 37 ORDER - granting 22 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant NYR Property Corp. are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 38 ORDER - granting 23 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant Prus, LLC are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 39 ORDER - granting 24 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant TJ Hospitality Ltd. are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010. (ch, ) (Entered: 11/30/2010)
- 11/30/2010 40 ORDER - granting - 8 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant Amit C. Patel are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010.

- (ch, ) (Entered: 11/30/2010)
- 11/30/2010 41 ORDER - granting 9 Notice of Voluntary Dismissal. All claims asserted by Plaintiff against Defendant B D & Sons Ltd. are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010.  
(ch, ) (Entered: 11/30/2010)
- 11/30/2010 42 ORDER - granting 7 Notice of Dismissal. All claims asserted by Plaintiff against Defendant 281 Lodging Hotel Partners Inc. are hereby dismissed without prejudice. Each party will bear its own costs and attorneys fees. Signed by Judge T. John Ward on 11/30/2010.  
(ch, ) (Entered: 11/30/2010)

---

Copyright © 2012 LexisNexis CourtLink, Inc. All rights reserved.  
\*\*\* THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY \*\*\*

---

**US District Court Civil Docket****U.S. District - Texas Eastern  
(Marshall)****2:09cv26****Linksmart Wireless Technology Llc v. Six Continents Hotels Inc et al****This case was retrieved from the court on Tuesday, July 10, 2012**

---

<b>Date Filed: 01/21/2009</b>	<b>Class Code: CLOSED</b>
<b>Assigned To: Judge David Folsom</b>	<b>Closed: Yes</b>
<b>Referred To: Magistrate Judge Caroline Craven</b>	<b>Statute: 28:1338</b>
<b>Nature of suit: Patent (830)</b>	<b>Jury Demand: Defendant</b>
<b>Cause: Patent Infringement</b>	<b>Demand Amount: \$0</b>
<b>Lead Docket: None</b>	<b>NOS Description: Patent</b>
<b>Other Docket: 2:08-cv-00385-DF</b>	
<b>Jurisdiction: Federal Question</b>	

**Litigants**Linksmart Wireless Technology Llc  
Plaintiff**Attorneys**Marc A Fenster  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: MFENSTER@RAKLAW.COMAndrew W Spangler  
[COR LD NTC]  
Spangler & Fussell PC  
208 N Green St  
Suite 300  
Longview , TX 75601  
USA  
903-753-9300  
Fax: 903-553-0403  
Email: SPANGLER@SFIPFIRM.COMAndrew D Weiss  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: AWEISS@RAKLAW.COM

Six Continents Hotels Inc  
Defendant

John M Guaragna  
[COR LD NTC]  
Dla Piper US LLP -Austin  
401 Congress Ave  
Suite 2500  
Austin , TX 78701-3799  
USA  
512/ 457-7000  
Fax: 512/ 457-7001  
Email: JOHN.GUARAGNA@DLAPIPER.COM

Intercontinental Hotels Group Resources Inc  
Defendant

John M Guaragna  
[COR LD NTC]  
Dla Piper-US LLP -Austin  
401 Congress Ave  
Suite 2500  
Austin , TX 78701-3799  
USA  
512/ 457-7000  
Fax: 512/ 457-7001  
Email: JOHN.GUARAGNA@DLAPIPER.COM

Six Continents Hotels Inc  
Counter Claimant

John M Guaragna  
[COR LD NTC]  
Dla Piper US LLP -Austin  
401 Congress Ave  
Suite 2500  
Austin , TX 78701-3799  
USA  
512/ 457-7000  
Fax: 512/ 457-7001  
Email: JOHN.GUARAGNA@DLAPIPER.COM

Intercontinental Hotels Group Resources Inc  
Counter Claimant

John M Guaragna  
[COR LD NTC]  
Dla Piper US LLP -Austin  
401 Congress Ave  
Suite 2500  
Austin , TX 78701-3799  
USA  
512/ 457-7000  
Fax: 512/ 457-7001  
Email: JOHN.GUARAGNA@DLAPIPER.COM

Linksmart Wireless Technology Llc  
Counter Defendant

Marc A Fenster  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: MFENSTER@RAKLAW.COM

Andrew W Spangler  
[COR LD NTC]  
Spangler & Fussell PC  
208 N Green St  
Suite 300  
Longview , TX 75601  
USA  
903-753-9300

Fax: 903-553-0403  
Email: SPANGLER@SFIPFIRM.COM

Andrew D Weiss  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: AWEISS@RAKLAW.COM

Date	#	Proceeding Text	Source
01/21/2009	1	COMPLAINT against Six Continents Hotels Inc, Intercontinental Hotels Group Resources Inc ( Filing fee \$ 350 receipt number 0540000000001843024.), filed by Linksmart Wireless Technology LLC. (Attachments: # 1 Exhibit A, # 2 Civil Cover Sheet)(Fenster, Marc) (Entered: 01/21/2009)	
01/21/2009	2	Notice of Filing of Patent/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. Patent and Trademark Office. (Fenster, Marc) (Entered: 01/21/2009)	
01/21/2009	3	CORPORATE DISCLOSURE STATEMENT filed by Linksmart Wireless Technology LLC (Fenster, Marc) (Entered: 01/21/2009)	
01/21/2009	4	NOTICE by Linksmart Wireless Technology LLC of Related Cases (Fenster, Marc) (Entered: 01/21/2009)	
01/21/2009	5	E-GOV SEALED SUMMONS Issued as to Six Continents Hotels Inc, Intercontinental Hotels Group Resources Inc. (Attachments: # 1 summons InterContinental Hotels)(ehs, ) (Entered: 01/21/2009)	
01/21/2009	6	ORDER REFERRING CASE for Pretrial proceedings to Magistrate Judge Charles Everingham. Signed by Judge T. John Ward on 1/21/09. (ehs, ) (Entered: 01/21/2009)	
01/21/2009	7	Magistrate Consent Form Mailed to Linksmart Wireless Technology LLC (ehs, ) (Entered: 01/21/2009)	
01/22/2009	8	NOTICE of Attorney Appearance by Andrew D Weiss on behalf of Linksmart Wireless Technology LLC (Weiss, Andrew) (Entered: 01/22/2009)	
01/22/2009	9	NOTICE of Attorney Appearance by Andrew Wesley Spangler on behalf of Linksmart Wireless Technology LLC (Spangler, Andrew) (Entered: 01/22/2009)	
01/23/2009	10	Joint MOTION to Consolidate Cases by Linksmart Wireless Technology LLC. (Attachments: # 1 Text of Proposed Order)(Weiss, Andrew) (Entered: 01/23/2009)	
02/03/2009	11	ORDER REASSIGNING CASE. Case reassigned to Judge David Folsom for all further proceedings. Judge T. John Ward no longer assigned to case. Signed by Judge T. John Ward on 2/2/09. (ch, ) (Entered: 02/03/2009)	
02/06/2009	12	E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology LLC. Intercontinental Hotels Group Resources Inc served on 1/21/2009 to John Guaragna DLA Piper by CM RRR, answer due 2/10/2009. (ehs, ) (Entered: 02/06/2009)	
02/06/2009	13	E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology LLC. Six Continents Hotels Inc served on 1/21/2009 to John Guaragna, DLA Piper by CM RRR, answer due 2/10/2009. (ehs, ) (Entered: 02/06/2009)	
02/10/2009	14	ANSWER to 1 Complaint,, COUNTERCLAIM against Linksmart Wireless Technology LLC by Six Continents Hotels Inc, Intercontinental Hotels Group Resources Inc.(Guaragna, John) (Entered: 02/10/2009)	
02/10/2009	15	CORPORATE DISCLOSURE STATEMENT filed by Six Continents Hotels Inc, Intercontinental Hotels Group Resources Inc identifying Corporate Parent InterContinental Hotels Group PLC for Intercontinental Hotels Group Resources Inc, Six Continents Hotels Inc. (Guaragna, John) (Entered: 02/10/2009)	
02/27/2009	16	ANSWER to 14 Answer to Complaint, Counterclaim by Linksmart Wireless Technology LLC.(Weiss, Andrew) (Entered: 02/27/2009)	
04/22/2009	17	NOTICE of Change of Address by John M Guaragna (Guaragna, John) (Entered: 04/22/2009)	

- 04/22/2009)
- 05/01/2009 18 ORDER granting 10 Motion to Consolidate Cases. ORDERED that the above- captioned actions are consolidated for all purposes pursuant to Federal Rule of Civil Procedure 42 (a) and Local Rule CV-42(b) and (c).. Signed by Magistrate Judge Charles Everingham on 5/1/09. (ch, ) (Entered: 05/01/2009)
- 05/01/2009 -- NOTICE OF FILING DOCUMENTS IN CONSOLIDATED CASES re 18 Order on Motion to Consolidate Cases. ALL FUTURE FILINGS TO BE FILED IN LEAD CASE 2:08cv264 ONLY (ehs, ) (Entered: 09/03/2009)
- 05/04/2009 19 NOTICE of Hearing: Scheduling Conference set for 6/3/2009 10:00 AM in Mag Ctrm (Marshall) before Magistrate Judge Charles Everingham. (jml, ) (Entered: 05/04/2009)
- 05/06/2009 20 Notice of Scheduling Conference, Proposed Deadlines for Docket Control Order and Discovery Order. Scheduling Conference set for 6/3/2009 10:00 AM before Magistrate Judge Charles Everingham. The parties are directed to meet and confer in accordance with Fed. R. Civ. P. 26(f) no later than 5/27/09. Signed by Magistrate Judge Charles Everingham on 5/5/09. (ch, ) (Entered: 05/06/2009)
- 06/01/2009 21 REPORT of Rule 26(f) Planning Meeting. (Attachments: # 1 Exhibit A - Proposed Docket Control Order)(Weiss, Andrew) (Additional attachment(s) added on 6/1/2009: # 2 Revised Scheduling Order) (sm, ). (Entered: 06/01/2009)
- 06/03/2009 22 Minute Entry for proceedings held before Magistrate Judge Charles Everingham: Scheduling Conference held on 6/3/2009. (Court Reporter Susan Simmons, CSR.) (jml) (Entered: 06/04/2009)
- 07/06/2010 23 NOTICE OF FILING OF OFFICIAL TRANSCRIPT of CLAIM CONSTRUCTION HEARING held on 5/25/10 before Judge Chad Everingham. Court Reporter/Transcriber: Shelly Holmes, CSR, Telephone number: (903) 663-5083. (116 Pages) NOTICE RE REDACTION OF TRANSCRIPTS: The parties have seven (7) business days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.txed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER. Redaction Request due 7/30/2010. Redacted Transcript Deadline set for 8/9/2010. Release of Transcript Restriction set for 10/7/2010. (tja, ) (Entered: 07/06/2010)
- 07/19/2011 24 ORDER ADMINISTRATIVELY CLOSED. Signed by Judge David Folsom on 7/19/11. (mrm, ) (Entered: 07/19/2011)
- 02/06/2012 25 ORDER REFERRING CASE for pretrial purposes to Magistrate Judge Caroline Craven. Signed by Judge David Folsom on 2/6/12. (ehs, ) (Entered: 02/06/2012)

---

Copyright © 2012 LexisNexis CourtLink, Inc. All rights reserved.  
\*\*\* THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY \*\*\*

---

**US District Court Civil Docket**

**U.S. District - Texas Eastern  
(Marshall)**

**2:08cv385**

**Linksmart Wireless Technology, Llc v. Sbc Internet Services, Inc**

**This case was retrieved from the court on Tuesday, July 10, 2012**

---

<b>Date Filed: 10/09/2008</b>	<b>Class Code: CLOSED</b>
<b>Assigned To: Judge David Folsom</b>	<b>Closed: Yes</b>
<b>Referred To: Magistrate Judge Caroline Craven</b>	<b>Statute: 15:1126</b>
<b>Nature of suit: Patent (830)</b>	<b>Jury Demand: Both</b>
<b>Cause: Patent Infringement</b>	<b>Demand Amount: \$0</b>
<b>Lead Docket: None</b>	<b>NOS Description: Patent</b>
<b>Other Docket: 2:09-cv-00026-DF</b>	
<b>Jurisdiction: Federal Question</b>	

**Litigants**

**Attorneys**

Linksmart Wireless Technology, Llc  
Plaintiff

Marc A Fenster  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: MFENSTER@RAKLAW.COM

Andrew W Spangler  
[COR LD NTC]  
Spangler & Fussell PC  
208 N Green St  
Suite 300  
Longview , TX 75601  
USA  
903-753-9300  
Fax: 903-553-0403  
Email: SPANGLER@SFIPFIRM.COM

Andrew D Weiss  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: AWEISS@RAKLAW.COM

Sbc Internet Services, Inc Doing Business as At&T  
Internet Services  
Defendant

Richard Alan Sayles  
[COR LD NTC]  
Sayles Werbner  
1201 Elm Street  
4400 Renaissance Tower  
Dallas , TX 75270  
USA  
214/ 939-8700  
Fax: 12149398787  
Email: Dsayles@swtriallaw.com

David T Pritikin  
[COR LD NTC]  
Sidley Austin -Chicago Bank One Plaza  
One South Dearborn Ave  
Chicago , IL 60603  
USA  
312/ 853-7359  
Fax: 312/ 853-7036  
Email: DPRITIKIN@SIDLEY.COM

EVE L Henson  
[COR LD NTC]  
Sayles | Werbner  
1201 Elm Street  
4400 Renaissance Tower  
Dallas , TX 75270  
USA  
214/ 939-8700  
Fax: 12149398787  
Email: Ehenson@swtriallaw.com

Hugh A Abrams  
[COR LD NTC]  
Sidley Austin -Chicago Bank One Plaza  
One South Dearborn Ave  
Chicago , IL 60603  
USA  
312/ 853-7017  
Fax: 13128537036  
<i>pro Hac Vice</ I>  
Email: HABRAMS@SIDLEY.COM

Mark Daniel Strachan  
[COR LD NTC]  
Sayles Webner  
4400 Renaissance  
1201 Elm Street  
Dallas , TX 75270  
USA  
214-939-8707  
Fax: 214-939-8787  
Email: Mstrachan@swtriallaw.com

Rachel D Sher  
[COR LD NTC]  
Sidley Austin -Chicago  
One South Dearborn St  
Chicago , IL 60603  
USA  
312/ 853-7000  
Fax: 312/ 853-7036  
Email: RSHER@SIDLEY.COM

Richard T McCaulley , Jr  
[COR LD NTC]  
Sidley Austin -Chicago Bank One Plaza

One South Dearborn Ave  
Chicago , IL 60603  
USA  
312/ 853-7000  
Fax: 312/ 853-7036  
Email: RMCCAULLEY@SIDLEY.COM

Sbc Internet Services, Inc  
Counter Claimant

Richard Alan Sayles  
[COR LD NTC]  
Sayles Werbner  
1201 Elm Street  
4400 Renaissance Tower  
Dallas , TX 75270  
USA  
214/ 939-8700  
Fax: 12149398787  
Email: Dsayles@swtriallaw.com

David T Pritikin  
[COR LD NTC]  
Sidley Austin -Chicago Bank One Plaza  
One South Dearborn Ave  
Chicago , IL 60603  
USA  
312/ 853-7359  
Fax: 312/ 853-7036  
Email: DPRITIKIN@SIDLEY.COM

Rachel D Sher  
[COR LD NTC]  
Sidley Austin -Chicago  
One South Dearborn St  
Chicago , IL 60603  
USA  
312/ 853-7000  
Fax: 312/ 853-7036  
Email: RSHER@SIDLEY.COM

Richard T McCaulley , Jr  
[COR LD NTC]  
Sidley Austin -Chicago Bank One Plaza  
One South Dearborn Ave  
Chicago , IL 60603  
USA  
312/ 853-7000  
Fax: 312/ 853-7036  
Email: RMCCAULLEY@SIDLEY.COM

Linksmart Wireless Technology, Llc  
Counter Defendant

Marc A Fenster  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: MFENSTER@RAKLAW.COM

Andrew D Weiss  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025

USA  
 310/ 826-7474  
 Fax: 310/ 826-6991  
 Email: AWEISS@RAKLAW.COM

Date	#	Proceeding Text	Source
10/10/2008	1	COMPLAINT AND DEMAND FOR JURY TRIAL against SBC Internet Services, Inc. (Filing fee \$ 350 receipt number 0540000000001724676), filed by Linksmart Wireless Technology, LLC. (Attachments: # 1 Civil Cover Sheet)(ch, ) (Entered: 10/10/2008)	
10/10/2008	--	Case Assigned to Judge T. John Ward. (ch, ) (Entered: 10/10/2008)	
10/10/2008	2	Magistrate Consent Form Mailed to Linksmart Wireless Technology, LLC (ch, ) (Entered: 10/10/2008)	
10/10/2008	3	E-GOV SEALED SUMMONS Issued as to SBC Internet Services, Inc.. (ch, ) (Entered: 10/10/2008)	
10/10/2008	4	CORPORATE DISCLOSURE STATEMENT filed by Linksmart Wireless Technology, LLC (Fenster, Marc) (Entered: 10/10/2008)	
10/10/2008	5	NOTICE by Linksmart Wireless Technology, LLC of Related Cases (Fenster, Marc) (Entered: 10/10/2008)	
10/10/2008	6	Notice of Filing of Patent/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. Patent and Trademark Office. (Fenster, Marc) (Entered: 10/10/2008)	
10/23/2008	7	E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. SBC Internet Services, Inc. served on 10/14/2008, answer due 11/3/2008. (ehs, ) (Entered: 10/23/2008)	
11/03/2008	8	ANSWER to 1 Complaint, COUNTERCLAIM against Linksmart Wireless Technology, LLC by SBC Internet Services, Inc..(Sayles, Richard) (Entered: 11/03/2008)	
11/03/2008	9	CORPORATE DISCLOSURE STATEMENT filed by SBC Internet Services, Inc. identifying Corporate Parent AT&T Inc., Other Affiliate AT&T Mobility LLC, Other Affiliate AT&T Mobility Corporation, Other Affiliate SBC Long Distance, LLC, Other Affiliate SBC Alloy Holdings, Inc., Other Affiliate BLS Cingular Holdings, LLC, Other Affiliate BellSouth Mobile Data, Inc. for SBC Internet Services, Inc.. (Sayles, Richard) (Entered: 11/03/2008)	
11/03/2008	10	NOTICE of Attorney Appearance by Eve L Henson on behalf of SBC Internet Services, Inc. (Henson, Eve) (Entered: 11/03/2008)	
11/17/2008	11	APPLICATION to Appear Pro Hac Vice by Attorney Rachel D Sher for SBC Internet Services, Inc. (APPROVED) (FEE PAID) 2-1-4232. (ch, ) (Entered: 11/19/2008)	
11/17/2008	12	APPLICATION to Appear Pro Hac Vice by Attorney David T Pritikin for SBC Internet Services, Inc. (APPROVED)(FEE PAID) 2-1-4232. (ch, ) (Entered: 11/19/2008)	
11/17/2008	13	APPLICATION to Appear Pro Hac Vice by Attorney Richard T McCaulley, Jr for SBC Internet Services, Inc. (APPROVED)(FEE PAID) 2-1-4232. (ch, ) (Entered: 11/19/2008)	
01/14/2009	14	NOTICE of Attorney Appearance by Andrew Wesley Spangler on behalf of Linksmart Wireless Technology, LLC (Spangler, Andrew) (Entered: 01/14/2009)	
01/14/2009	15	NOTICE of Attorney Appearance by Andrew D Weiss on behalf of Linksmart Wireless Technology, LLC (Weiss, Andrew) (Entered: 01/14/2009)	
01/20/2009	16	Unopposed MOTION for Extension of Time to File Response/Reply to SBC's Counterclaims by Linksmart Wireless Technology, LLC. (Attachments: # 1 Text of Proposed Order) (Weiss, Andrew) (Entered: 01/20/2009)	
01/21/2009	17	ORDER granting 16 Motion for Extension of Time to File Response/Reply Responses due by 1/23/2009. Signed by Judge T. John Ward on 1/21/09. (ch, ) (Entered: 01/21/2009)	
01/21/2009	18	ANSWER to 8 Answer to Complaint, Counterclaim by Linksmart Wireless Technology, LLC. (Weiss, Andrew) (Entered: 01/21/2009)	
01/23/2009	19	Joint MOTION to Consolidate Cases by SBC Internet Services, Inc.. (Attachments: # 1 Text of Proposed Order)(Sayles, Richard) (Entered: 01/23/2009)	
02/03/2009	20	ORDER REASSIGNING CASE. Case reassigned to Judge David Folsom for all further proceedings. Judge T. John Ward no longer assigned to case. Signed by Judge T. John	

- Ward on 2/2/09. (ch, ) (Entered: 02/03/2009)
- 02/10/2009 21 ORDER REFERRING CASE to Magistrate Judge Charles Everingham for case management. Signed by Judge David Folsom on 2/10/09. (mrm, ) (Entered: 02/10/2009)
- 05/01/2009 22 ORDER granting 19 Motion to Consolidate Cases. ORDERED that the above- captioned actions are consolidated for all purposes pursuant to Federal Rule of Civil Procedure 42 (a) and Local Rule CV-42(b) and (c).. Signed by Magistrate Judge Charles Everingham on 5/1/09. (ch, ) (Entered: 05/01/2009)
- 05/01/2009 -- NOTICE OF FILING DOCUMENTS IN CONSOLIDATED CASES re 22 Order on Motion to Consolidate Cases. ALL FUTURE FILINGS TO BE FILED IN LEAD CASE 2:08cv264 ONLY (ehs, ) (Entered: 09/03/2009)
- 05/04/2009 23 NOTICE of Hearing: Scheduling Conference set for 6/3/2009 10:00 AM in Mag Ctrm (Marshall) before Magistrate Judge Charles Everingham. (jml) (Entered: 05/04/2009)
- 05/06/2009 24 Notice of Scheduling Conference, Proposed Deadlines Scheduling Conference set for 6/3/2009 10:00 AM before Magistrate Judge Charles Everingham. The parties are directed to meet and confer in accordance with Fed. R. Civ. P. 26(f) no later than 5/27/09. Signed by Magistrate Judge Charles Everingham on 5/5/09. (ch, ) (Entered: 05/06/2009)
- 05/06/2009 25 NOTICE of Attorney Appearance by Mark Daniel Strachan on behalf of SBC Internet Services, Inc. (Strachan, Mark) (Entered: 05/06/2009)
- 06/01/2009 26 REPORT of Rule 26(f) Planning Meeting. (Attachments: # 1 Exhibit A - Proposed Docket Control Order)(Weiss, Andrew) (Additional attachment(s) added on 6/1/2009: # 2 Revised Docket Control Order) (sm, ). (Entered: 06/01/2009)
- 06/03/2009 27 Minute Entry for proceedings held before Magistrate Judge Charles Everingham: Scheduling Conference held on 6/3/2009. (Court Reporter Susan Simmons, CSR.) (jml) (Entered: 06/04/2009)
- 08/14/2009 28 APPLICATION to Appear Pro Hac Vice by Attorney Hugh A Abrams for SBC Internet Services, Inc. (APPROVED FEE PAID) 2-1-4865. (ch, ) (Entered: 08/14/2009)
- 07/06/2010 29 NOTICE OF FILING OF OFFICIAL TRANSCRIPT of CLAIM CONSTRUCTION HEARING held on 5/25/10 before Judge Chad Everingham. Court Reporter/Transcriber: Shelly Holmes, CSR, Telephone number: (903) 663-5082. (116 Pages) NOTICE RE REDACTION OF TRANSCRIPTS: The parties have seven (7) business days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.txed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER. Redaction Request due 7/30/2010. Redacted Transcript Deadline set for 8/9/2010. Release of Transcript Restriction set for 10/7/2010. (tja, ) (Entered: 07/06/2010)
- 07/19/2011 30 ORDER ADMINISTRATIVELY CLOSED. Signed by Judge David Folsom on 7/19/11. (mrm, ) (Entered: 07/19/2011)
- 02/06/2012 31 ORDER REFERRING CASE for pretrial purposes to Magistrate Judge Caroline Craven. Signed by Judge David Folsom on 2/6/12. (ehs, ) (Entered: 02/06/2012)

---

Copyright © 2012 LexisNexis CourtLink, Inc. All rights reserved.  
\*\*\* THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY \*\*\*

---

**US District Court Civil Docket**

**U.S. District - Texas Eastern  
(Marshall)**

**2:08cv304**

**Linksmart Wireless Technology, Llc v. Cisco Systems, Inc et al**

**This case was retrieved from the court on Tuesday, July 10, 2012**

---

<b>Date Filed: 08/04/2008</b>	<b>Class Code: CLOSED</b>
<b>Assigned To: Judge David Folsom</b>	<b>Closed: Yes</b>
<b>Referred To: Magistrate Judge Caroline Craven</b>	<b>Statute: 35:271</b>
<b>Nature of suit: Patent (830)</b>	<b>Jury Demand: Plaintiff</b>
<b>Cause: Patent Infringement</b>	<b>Demand Amount: \$0</b>
<b>Lead Docket: None</b>	<b>NOS Description: Patent</b>
<b>Other Docket: None</b>	
<b>Jurisdiction: Federal Question</b>	

**Litigants**

**Attorneys**

Linksmart Wireless Technology, Llc  
Plaintiff

Marc A Fenster  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: MFENSTER@RAKLAW.COM

Andrew W Spangler  
[COR LD NTC]  
Spangler & Fussell PC  
208 N Green St  
Suite 300  
Longview , TX 75601  
USA  
903-753-9300  
Fax: 903-553-0403  
Email: SPANGLER@SFIPFIRM.COM

Andrew D Weiss  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: AWEISS@RAKLAW.COM

Cisco Systems, Inc  
Defendant

David J Beck  
[COR LD NTC]  
Beck Redden & Secrest  
1221 McKinney St, Suite 4500  
One Houston Center  
Houston , TX 77010-2020  
USA  
713/ 951-3700  
Fax: 17139513720  
Email: Dbeck@brsfirm.com

David B Bassett  
[COR LD NTC]  
Wilmer Cutler Pickering Hale & Dorr -New York  
399 Park Avenue  
New York , NY 10022  
USA  
212/ 230-8800  
Fax: 212/ 230-8888  
<i>pro Hac Vice</ I>  
Email: DAVID.BASSETT@WILMERHALE.COM

James P Barabas  
[COR LD NTC]  
Wilmer Cutler Pickering Hale & Dorr -New York  
399 Park Avenue  
New York , NY 10022  
USA  
212/ 230-8800  
Fax: 212/ 230-8888  
Email: JAMES.BARABAS@WILMERHALE.COM

Joyce Chen  
[COR LD NTC]  
Wilmer Cutler Pickering Hale & Dorr -New York  
399 Park Avenue  
New York , NY 10022  
USA  
212/ 230-8809  
Fax: 212/ 230-8888  
<i>pro Hac Vice</ I>  
Email: JOYCE.CHEN@WILMERHALE.COM

Michael Ernest Richardson  
[COR LD NTC]  
Beck Redden & Secrest -Houston  
1221 McKinney  
Suite 4500  
Houston , TX 77010-2010  
USA  
713/ 951-6284  
Fax: 17139513720  
Email: Mrichardson@brsfirm.com

Noah A Levine  
[COR LD NTC]  
Wilmer Cutler Pickering Hale & Dorr -New York  
399 Park Avenue  
New York , NY 10022  
USA  
212/ 230-8800  
Fax: 212/ 230-8888  
<i>pro Hac Vice</ I>  
Email: NOAH.LEVINE@WILMERHALE.COM

Peter M Dichiaro  
[COR LD NTC]

Wilmer Cutler Pickering Hale & Dorr -Boston  
60 State Street  
Boston , MA 02109  
USA  
617/ 526-6466  
Fax: 617/ 526-5000  
<i>pro Hac Vice</ I>  
Email: PETER.DICHIARA@WILMERHALE.COM

Robert David Daniel  
[COR LD NTC]  
Beck Redden & Secrest LLP  
One Houston Center  
1221 McKinney St, Suite 4500  
Houston , TX 77010-2020  
USA  
713/ 951-3700  
Fax: 17139513720  
Email: Bddaniel@brsfirm.com

William F Lee  
[COR LD NTC]  
Wilmer Cutler Pickering Hale & Dorr -Boston  
60 State Street  
Boston , MA 02109  
USA  
617-526-6556  
Fax: 617-526-5000  
<i>pro Hac Vice</ I>  
Email: WILLIAM.LEE@WILMERHALE.COM

Juniper Networks, Inc  
[Term: 09/03/2008]  
Defendant

Aruba Networks, Inc  
[Term: 09/03/2008]  
Defendant

Cisco Systems, Inc  
Counter Claimant

David J Beck  
[COR LD NTC]  
Beck Redden & Secrest  
1221 McKinney St, Suite 4500  
One Houston Center  
Houston , TX 77010-2020  
USA  
713/ 951-3700  
Fax: 17139513720  
Email: Dbeck@brsfirm.com

James P Barabas  
[COR LD NTC]  
Wilmer Cutler Pickering Hale & Dorr -New York  
399 Park Avenue  
New York , NY 10022  
USA  
212/ 230-8800  
Fax: 212/ 230-8888  
Email: JAMES.BARABAS@WILMERHALE.COM

Michael Ernest Richardson  
[COR LD NTC]  
Beck Redden & Secrest -Houston  
1221 McKinney  
Suite 4500  
Houston , TX 77010-2010

USA  
713/ 951-6284  
Fax: 17139513720  
Email: Mrichardson@brsfirm.com

Noah A Levine  
[COR LD NTC]  
Wilmer Cutler Pickering Hale & Dorr -New York  
399 Park Avenue  
New York , NY 10022  
USA  
212/ 230-8800  
Fax: 212/ 230-8888  
<i>pro Hac Vice</ I>  
Email: NOAH.LEVINE@WILMERHALE.COM

William F Lee  
[COR LD NTC]  
Wilmer Cutler Pickering Hale & Dorr -Boston  
60 State Street  
Boston , MA 02109  
USA  
617-526-6556  
Fax: 617-526-5000  
<i>pro Hac Vice</ I>  
Email: WILLIAM.LEE@WILMERHALE.COM

Linksmart Wireless Technology, Llc  
Counter Defendant

Marc A Fenster  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: MFENSTER@RAKLAW.COM

Andrew D Weiss  
[COR LD NTC]  
Russ August & Kabat  
12424 Wilshire Boulevard  
Suite 1200  
Los Angeles , CA 90025  
USA  
310/ 826-7474  
Fax: 310/ 826-6991  
Email: AWEISS@RAKLAW.COM

Cisco Systems, Inc  
Counter Defendant

David J Beck  
[COR LD NTC]  
Beck Redden & Secrest  
1221 McKinney St, Suite 4500  
One Houston Center  
Houston , TX 77010-2020  
USA  
713/ 951-3700  
Fax: 17139513720  
Email: Dbeck@brsfirm.com

Michael Ernest Richardson  
[COR LD NTC]  
Beck Redden & Secrest -Houston  
1221 McKinney  
Suite 4500

Houston , TX 77010-2010  
 USA  
 713/ 951-6284  
 Fax: 17139513720  
 Email: Mrichardson@brsfirm.com

Date	#	Proceeding Text	Source
08/04/2008	1	COMPLAINT and Demand for Jury Trial against Cisco Systems, Inc., Juniper Networks, Inc., Aruba Networks, Inc. ( Filing fee \$ 350 receipt number 0540000000001643001.), filed by Linksmart Wireless Technology, LLC. (Attachments: # 1 Exhibit A to Complaint, # 2 Civil Cover Sheet)(Fenster, Marc) (Entered: 08/04/2008)	
08/04/2008	2	Notice of Filing of Patent/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. Patent and Trademark Office. (Fenster, Marc) (Entered: 08/04/2008)	
08/04/2008	3	CORPORATE DISCLOSURE STATEMENT filed by Linksmart Wireless Technology, LLC (Fenster, Marc) (Entered: 08/04/2008)	
08/04/2008	4	NOTICE by Linksmart Wireless Technology, LLC of Related Case (Fenster, Marc) (Entered: 08/04/2008)	
08/04/2008	--	Case Assigned to Judge David Folsom. (ch, ) (Entered: 08/05/2008)	
08/05/2008	5	STANDING ORDER REFERRING CASE - to Magistrate Judge Charles Everingham. Signed by Judge David Folsom on 8/5/08. (ch, ) (Entered: 08/05/2008)	
08/05/2008	6	Magistrate Consent Form Mailed to Linksmart Wireless Technology, LLC (ch, ) (Entered: 08/05/2008)	
08/05/2008	--	E-GOV SEALED SUMMONS Issued as to Cisco Systems, Inc., Juniper Networks, Inc., Aruba Networks, Inc.. (ch, ) (Entered: 08/05/2008)	
08/07/2008	--	E-GOV SEALED SUMMONS REISSUED as to Cisco Systems, Inc., Juniper Networks, Inc., Aruba Networks, Inc., attorney didn't receive the ones issued on 8/5/08. (ch, ) (Entered: 08/07/2008)	
09/02/2008	7	NOTICE by Linksmart Wireless Technology, LLC of Dismissal Without Prejudice as to Defs Juniper Networks, Inc. and Aruba Networks, Inc. ONLY (Fenster, Marc) (Additional attachment(s) added on 9/3/2008: # 1 Text of Proposed Order) (sm, ). (Entered: 09/02/2008)	
09/03/2008	8	ORDER GRANTING PLAINTIFFS REQUEST FOR DISMISSAL WITHOUT PREJUDICE; re 7 Notice (Other) filed by Linksmart Wireless Technology, LLC, Motions terminated.; Aruba Networks, Inc. and Juniper Networks, Inc. terminated.. Signed by Judge David Folsom on 9/3/08. (mrm, ) (Entered: 09/03/2008)	
10/30/2008	9	E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Cisco Systems, Inc. served on 10/22/2008, answer due 11/12/2008. (ch, ) (Entered: 10/30/2008)	
11/06/2008	10	Cisco Systems, Inc.'s Answer and Counterclaims ANSWER to 1 Complaint,, COUNTERCLAIM against Linksmart Wireless Technology, LLC, Cisco Systems, Inc. by Cisco Systems, Inc..(Beck, David) (Entered: 11/06/2008)	
11/06/2008	11	CORPORATE DISCLOSURE STATEMENT filed by Cisco Systems, Inc. (Beck, David) (Entered: 11/06/2008)	
11/17/2008	12	APPLICATION to Appear Pro Hac Vice by Attorney William F Lee for Cisco Systems, Inc. (APPROVED)(FEE PAID) 2-1-4231. (ch, ) (Entered: 11/19/2008)	
11/17/2008	13	APPLICATION to Appear Pro Hac Vice by Attorney James P Barabas for Cisco Systems, Inc. (APPROVED)(FEE PAID) 2-1-4244. (ch, ) (Entered: 11/19/2008)	
11/17/2008	14	APPLICATION to Appear Pro Hac Vice by Attorney Noah A Levine for Cisco Systems, Inc. (APPROVED)(FEE PAID) 2-1-4244. (ch, ) (Entered: 11/20/2008)	
11/26/2008	16	APPLICATION to Appear Pro Hac Vice by Attorney David B Bassett for Cisco Systems, Inc. (APPROVED)(FEE PAID) 2-1-4277. (ch, ) (Entered: 12/02/2008)	
12/01/2008	15	Linksmart's ANSWER to 10 Answer to Complaint, Counterclaim of Cisco Systems, Inc. by Linksmart Wireless Technology, LLC.(Fenster, Marc) (Entered: 12/01/2008)	
01/13/2009	17	NOTICE of Attorney Appearance by Andrew Wesley Spangler on behalf of Linksmart Wireless Technology, LLC (Spangler, Andrew) (Entered: 01/13/2009)	

- 01/14/2009 18 NOTICE of Attorney Appearance by Andrew D Weiss on behalf of Linksmart Wireless Technology, LLC (Weiss, Andrew) (Entered: 01/14/2009)
- 01/21/2009 19 NOTICE of Hearing: Scheduling Conference set for 2/17/2009 02:30 PM in Mag Ctrm (Marshall) before Magistrate Judge Charles Everingham. (jml, ) (Entered: 01/21/2009)
- 01/23/2009 20 Joint MOTION to Consolidate Cases by Cisco Systems, Inc.. (Attachments: # 1 Text of Proposed Order)(Beck, David) (Entered: 01/23/2009)
- 01/26/2009 21 Notice of Scheduling Conference, Proposed Deadlines for Docket Control Order and Discovery Order. Scheduling Conference set for 2/17/2009 02:30 PM before Magistrate Judge Charles Everingham.. Signed by Magistrate Judge Charles Everingham on 1/26/09. (ch, ) (Entered: 01/26/2009)
- 01/29/2009 22 NOTICE of Attorney Appearance by Michael Ernest Richardson on behalf of Cisco Systems, Inc. (Richardson, Michael) (Entered: 01/29/2009)
- 02/10/2009 23 NOTICE of Hearing: Scheduling Conference set for 2/17/2009, 02:30 PM, in Mag Ctrm (Marshall) before Magistrate Judge Charles Everingham is CANCELLED.(delat) (Entered: 02/10/2009)
- 02/13/2009 24 APPLICATION to Appear Pro Hac Vice by Attorney Peter M Dichiara for Cisco Systems, Inc. (APPROVED FEE PAID) 2-1-4494. (ch, ) (Entered: 02/13/2009)
- 05/01/2009 25 ORDER granting 20 Motion to Consolidate Cases. ORDERED that the above- captioned actions are consolidated for all purposes pursuant to Federal Rule of Civil Procedure 42 (a) and Local Rule CV-42(b) and (c).. Signed by Magistrate Judge Charles Everingham on 5/1/09. (ch, ) (Entered: 05/01/2009)
- 05/01/2009 -- NOTICE OF FILING DOCUMENTS IN CONSOLIDATED CASES re 25 Order GRANTING Motion to Consolidate Cases. ALL FUTURE FILING ARE TO BE FILED IN THE LEAD CASE ONLY 2:08cv264 (ehs, ) (Entered: 09/02/2009)
- 05/04/2009 26 NOTICE of Hearing: Scheduling Conference set for 6/3/2009 10:00 AM in Mag Ctrm (Marshall) before Magistrate Judge Charles Everingham. (jml) (Entered: 05/04/2009)
- 05/06/2009 27 Notice of Scheduling Conference, Proposed Deadlines for Docket Control Order, and Discovery Order. Scheduling Conference set for 6/3/2009 10:00 AM before Magistrate Judge Charles Everingham. The parties are directed to meet and confer in accordance with the Fed. R. Civ. P. 26(f) no later than 5/27/09. Signed by Magistrate Judge Charles Everingham on 5/5/09. (ch, ) (Entered: 05/06/2009)
- 06/01/2009 28 REPORT of Rule 26(f) Planning Meeting. (Attachments: # 1 Exhibit A - Proposed Docket Control Order)(Weiss, Andrew) (Additional attachment(s) added on 6/1/2009: # 2 Revised Scheduling Order) (sm, ). (Entered: 06/01/2009)
- 06/03/2009 29 Minute Entry for proceedings held before Magistrate Judge Charles Everingham: Scheduling Conference held on 6/3/2009. (Court Reporter Susan Simmons, CSR.) (jml) (Entered: 06/04/2009)
- 07/10/2009 30 APPLICATION to Appear Pro Hac Vice by Attorney Joyce Chen for Cisco Systems, Inc. (APPROVED FEE PAID) 2-1-4798. (ch, ) (Entered: 07/10/2009)
- 08/19/2009 31 NOTICE of Attorney Appearance by Robert David Daniel on behalf of Cisco Systems, Inc. (Daniel, Robert) (Entered: 08/19/2009)
- 07/06/2010 32 NOTICE OF FILING OF OFFICIAL TRANSCRIPT OF CLAIM CONSTRUCTION HEARING held on 5/25/10 before Judge Chad Everingham. Court Reporter/Transcriber: Shelly Holmes, CSR, Telephone number: (903) 663-5082. (116 Pages) NOTICE RE REDACTION OF TRANSCRIPTS: The parties have seven (7) business days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.txed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER. Redaction Request due 7/30/2010. Redacted Transcript Deadline set for 8/9/2010. Release of Transcript Restriction set for 10/7/2010. (tja, ) (Entered: 07/06/2010)
- 07/19/2011 33 ORDER ADMINISTRATIVELY CLOSED. Signed by Judge David Folsom on 7/19/11. (mrm, ) (Entered: 07/19/2011)
- 02/06/2012 34 ORDER REFERRING CASE for pretrial purposes to Magistrate Judge Caroline Craven. Signed by Judge David Folsom on 2/6/12. (ehs, ) (Entered: 02/06/2012)

Copyright © 2012 LexisNexis CourtLink, Inc. All rights reserved.  
\*\*\* THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY \*\*\*

---

**US District Court Civil Docket**

**U.S. District - Texas Eastern  
(Marshall)**

**2:08cv264**

**Linksmart Wireless Technology, Llc v. T-Mobile USA, Inc et al**

This case was retrieved from the court on Tuesday, July 10, 2012

---

<b>Date Filed:</b> 07/01/2008	<b>Class Code:</b> CLOSED
<b>Assigned To:</b>	<b>Closed:</b> Yes
<b>Referred To:</b>	<b>Statute:</b> 15:1126
<b>Nature of suit:</b> Patent (830)	<b>Jury Demand:</b> Both
<b>Cause:</b> Patent Infringement	<b>Demand Amount:</b> \$0
<b>Lead Docket:</b> None	<b>NOS Description:</b> Patent
<b>Other Docket:</b> None	
<b>Jurisdiction:</b> Federal Question	

<b>Date</b>	<b>#</b>	<b>Proceeding Text</b>	<b>Source</b>
07/01/2008	1	COMPLAINT against all defendants ( Filing fee \$ 350 receipt number 0540000000001601022.), filed by Linksmart Wireless Technology, LLC.(Fenster, Marc) (Additional attachment(s) added on 7/2/2008: # 1 Civil Cover Sheet) (mpv, ). (Entered: 07/01/2008)	
07/01/2008	2	***FILED IN ERROR; PLEASE IGNORE*** NOTICE of Disclosure by Linksmart Wireless Technology, LLC (Fenster, Marc) Modified on 7/2/2008 (mpv, ). (Entered: 07/01/2008)	
07/01/2008	3	Notice of Filing of Patent/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. Patent and Trademark Office. (Fenster, Marc) (Entered: 07/01/2008)	
07/01/2008	4	***FILED IN ERROR; PLEASE IGNORE*** Additional Attachments to Main Document: 1 Complaint.. (Fenster, Marc) Modified on 7/2/2008 (mpv, ). (Entered: 07/01/2008)	
07/02/2008	--	E-GOV SEALED SUMMONS Issued as to NetNearU Corp., Pronto Networks, Inc., Aptilo Networks, Inc., FreeFi Networks, Inc., Meraki, Inc., Second Rule LLC, Mail Boxes Etc., Inc., McDonalds Corp., Barnes & Noble Booksellers, Inc., Ramada Worldwide, Inc., Marriott International, Inc., InterContinental Hotels Group PLC, Choice Hotels International Inc., Best Western International, Inc., T-Mobile USA, Inc., Wayport, Inc., AT&T, Inc., AT&T Mobility, LLC, LodgeNet Interactive Corporation, iBAHN General Holdings Corp., EthoStream, LLC, Hot Point Wireless, Inc.. (ch, ) (Entered: 07/02/2008)	
07/02/2008	--	***FILED IN ERROR. Document # 4, Additional attachments to main document. PLEASE IGNORE. Civil Cover Sheet now attached as an attachment to #1 Complaint by clerk*** (mpv, ) (Entered: 07/02/2008)	
07/02/2008	--	NOTICE of Deficiency regarding #2 the NOTICE of Disclosure submitted Docketed incorrectly, attorney to refile as Corporate Disclosure Statement. Correction should be made by one business day (mpv, ) (Entered: 07/02/2008)	
07/02/2008	--	Case Assigned to Judge T. John Ward. (ch, ) (Entered: 07/02/2008)	
07/02/2008	5	ORDER REFERRING CASE to Magistrate Judge Charles Everingham. Signed by Judge T. John Ward on 7/2/08. (ch, ) (Entered: 07/02/2008)	
07/02/2008	6	Magistrate Consent Form Mailed to Linksmart Wireless Technology, LLC (ch, ) (Entered: 07/02/2008)	
07/02/2008	7	CORPORATE DISCLOSURE STATEMENT filed by Linksmart Wireless Technology, LLC	

- (Fenster, Marc) (Entered: 07/02/2008)
- 07/09/2008 8 APPLICATION to Appear Pro Hac Vice by Attorney Larry C Russ for Linksmart Wireless Technology, LLC. (FEE PAID) 2-1-3936 (ehs, ) (Entered: 07/09/2008)
- 07/09/2008 9 APPLICATION to Appear Pro Hac Vice by Attorney Stanley H Thompson, Jr for Linksmart Wireless Technology, LLC. (FEE PAID) 2-1-3936 (ehs, ) (Entered: 07/09/2008)
- 07/09/2008 10 APPLICATION to Appear Pro Hac Vice by Attorney Stephen M Lobbin for Linksmart Wireless Technology, LLC. (FEE PAID) 2-1-3936 (ehs, ) (Entered: 07/09/2008)
- 07/18/2008 11 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Ramada Worldwide, Inc. served on 7/10/2008, answer due 7/30/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 12 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. AT&T Mobility, LLC served on 7/10/2008, answer due 7/30/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 13 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Barnes & Noble Booksellers, Inc. served on 7/11/2008, answer due 7/31/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 14 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Best Western International, Inc. served on 7/10/2008, answer due 7/30/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 15 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Choice Hotels International Inc. served on 7/14/2008, answer due 8/4/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 16 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. EthoStream, LLC served on 7/14/2008, answer due 8/4/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 17 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. iBAHN General Holdings Corp. served on 7/10/2008, answer due 7/30/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 18 NOTICE of Attorney Appearance by David M Stein on behalf of Ramada Worldwide, Inc. (Stein, David) (Entered: 07/18/2008)
- 07/18/2008 19 NOTICE of Attorney Appearance by Fay E Morisseau on behalf of Ramada Worldwide, Inc. (Morisseau, Fay) (Entered: 07/18/2008)
- 07/18/2008 20 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. InterContinental Hotels Group PLC served on 7/11/2008, answer due 7/31/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 21 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. LodgeNet Interactive Corporation served on 7/11/2008, answer due 7/31/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 22 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. McDonalds Corp. served on 7/11/2008, answer due 7/31/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 23 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Mail Boxes Etc., Inc. served on 7/10/2008, answer due 7/30/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 24 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Marriott International, Inc. served on 7/11/2008, answer due 7/31/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 25 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Second Rule LLC served on 7/10/2008, answer due 7/30/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 26 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. T-Mobile USA, Inc. served on 7/10/2008, answer due 7/30/2008. (ehs, ) (Entered: 07/18/2008)
- 07/18/2008 27 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Wayport, Inc. served on 7/10/2008, answer due 7/30/2008. (ehs, ) (Entered: 07/18/2008)

- 07/22/2008 28 NOTICE of Attorney Appearance by J Thad Heartfield on behalf of Ramada Worldwide, Inc. (Heartfield, J) (Entered: 07/22/2008)
- 07/24/2008 29 Defendant's Unopposed First Application for Extension of Time to Answer Complaint re Ramada Worldwide, Inc..( Heartfield, J) (Entered: 07/24/2008)
- 07/24/2008 30 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Pronto Networks, Inc. served on 7/11/2008, answer due 7/31/2008. (ch, ) (Entered: 07/24/2008)
- 07/24/2008 31 E-GOV SEALED SUMMONS Returned Executed by Linksmart Wireless Technology, LLC. Aptilo Networks, Inc. served on 7/15/2008, answer due 8/4/2008. (ch, ) (Entered: 07/24/2008)

---

Copyright © 2012 LexisNexis CourtLink, Inc. All rights reserved.  
\*\*\* THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY \*\*\*

# Patent Assignment Abstract of Title

## Total Assignments: 2

Application #: 09295966

Filing Dt: 04/21/1999

Patent #: 6779118

Issue Dt: 08/17/2004

PCT #: NONE

Publication #: NONE

Pub Dt:

Inventors: KOICHIRO IKUDOME, MOON TAI YEUNG

Title: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

## Assignment: 1

Reel/Frame: 010062 / 0040

Received: 07/06/1999

Recorded: 06/29/1999

Mailed: 09/01/1999

Pages: 3

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignors: IKUDOME, KOICHIRO

Exec Dt: 06/15/1999

YEUNG, MOON TAI

Exec Dt: 06/15/1999

Assignee: AURIC WEB SYSTEMS

3452 EAST FOOTHILL BOULEVARD, SUITE 300  
PASADENA, CALIFORNIA 91107

Correspondent: CHRISTIE, PARKER & HALE, LLP

WESLEY W. MONROE

P.O. BOX 7068

PASADENA, CA 91109-7068

## Assignment: 2

Reel/Frame: 021185 / 0416

Received: 07/02/2008

Recorded: 07/02/2008

Mailed: 07/02/2008

Pages: 12

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignor: AURIQ SYSTEMS, INC.

Exec Dt: 06/25/2008

Assignee: LINKSMART WIRELESS TECHNOLOGY, LLC

3452 E. FOOTHILL BLVD.

SUITE 320

PASADENA, CALIFORNIA 91107

Correspondent: CLARK D. GROSS

12424 WILSHIRE BOULEVARD, STE. 1200

LOS ANGELES, CA 90025

Search Results as of: 07/03/2012 11:25 AM

If you have any comments or questions concerning the data displayed, contact PRD / Assignments at 571-272-3350. v.2.2.1  
Web interface last modified: Jan 26, 2012

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

(Also referred to as FORM PTO-1465)

**REQUEST FOR *EX PARTE* REEXAMINATION TRANSMITTAL FORM**

Address to:

**Mail Stop *Ex Parte* Reexam  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450**

Attorney Docket No.: MIPIKU.002REDate: June 28, 2012

1.  This is a request for *ex parte* reexamination pursuant to 37 CFR 1.510 of patent number 6,779,118 issued August 17, 2004. The request is made by:  
 patent owner.  third party requester.
2.  The name and address of the person requesting reexamination is:  
Donald D. Min  
1717 Pennsylvania Ave, Suite 900  
Washington, DC 20006
3.  a. A check in the amount of \$\_\_\_\_\_ is enclosed to cover the reexamination fee, 37 CFR 1.20(c)(1);  
 b. The Director is hereby authorized to charge the fee as set forth in 37 CFR 1.20(c)(1) to Deposit Account No. \_\_\_\_\_; **or**  
 c. Payment by credit card. Form PTO-2038 is attached.
4.  Any refund should be made by  check or  credit to Deposit Account No. 50-5067 37 CFR 1.26(c). If payment is made by credit card, refund must be to credit card account.
5.  A copy of the patent to be reexamined having a double column format on one side of a separate paper is enclosed. 37 CFR 1.510(b)(4)
6.  CD-ROM or CD-R in duplicate, Computer Program (Appendix) or large table  
 Landscape Table on CD
7.  Nucleotide and/or Amino Acid Sequence Submission  
*If applicable, items a. – c. are required.*  
a.  Computer Readable Form (CRF)  
b. Specification Sequence Listing on:  
i.  CD-ROM (2 copies) or CD-R (2 copies); **or**  
ii.  paper  
c.  Statements verifying identity of above copies
8.  A copy of any disclaimer, certificate of correction or reexamination certificate issued in the patent is included.
9.  Reexamination of claim(s) 2-7, 9-14, 16-24, 26-90 is requested.
10.  A copy of every patent or printed publication relied upon is submitted herewith including a listing thereof on Form PTO/SB/08, PTO-1449, or equivalent.
11.  An English language translation of all necessary and pertinent non-English language patents and/or printed publications is included.

[Page 1 of 2]

This collection of information is required by 37 CFR 1.510. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

**SEND TO: Mail Stop *Ex Parte* Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

12.  The attached detailed request includes at least the following items:

- a. A statement identifying each substantial new question of patentability based on prior patents and printed publications. 37 CFR 1.510(b)(1)
- b. An identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited art to every claim for which reexamination is requested. 37 CFR 1.510(b)(2).

13.  A proposed amendment is included (only where the patent owner is the requester). 37 CFR 1.510(e)14.  a. It is certified that a copy of this request (if filed by other than the patent owner) has been served in its entirety on the patent owner as provided in 37 CFR 1.33(c).

The name and address of the party served and the date of service are:

Hershkovitz & Associates, LLC2845 Duke StreetAlexandria, VA 22314

Date of Service: \_\_\_\_\_; or

- b. A duplicate copy is enclosed because service on patent owner was not possible. An explanation of the efforts made to serve patent owner **is attached**. See MPEP 2220.

15. Correspondence Address: Direct all communications about the reexamination to:

 The address associated with Customer Number:

90934

OR

 Firm or  
Individual Name \_\_\_\_\_

Address

City

State

Zip

Country

Telephone

Email

16.  The patent is currently the subject of the following concurrent proceeding(s):

- a. Copending reissue Application No. \_\_\_\_\_
- b. Copending reexamination Control No. \_\_\_\_\_
- c. Copending Interference No. \_\_\_\_\_
- d. Copending litigation styled:  
Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc.,  
No. 8:1-cv-00522-JST-AN

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**/Donald D. Min/

Authorized Signature

Donald D. Min

Typed/Printed Name

June 28, 2012

Date

47796

Registration No.

 For Patent Owner Requester For Third Party Requester

## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

REEXAMINATION REQUEST

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Patentees	: Koichiro Ikudome et al.
Pat. No.	: 6,779,118
Issued	: August 17, 2004
For	: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Art Unit	: 3992
Examiner	: Sam Rimell

**REQUEST FOR EX PARTE REEXAMINATION**

Mail Stop Ex Parte Reexam  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

Don Min (“Requestor”) respectfully submits the following request for *ex parte* reexamination of U.S. Patent No. 6,779,118 (filed Apr. 21, 1999) to Ikudome et al. (“the ’118 Patent”). Pursuant to 35 U.S.C. § 302 and 37 C.F.R. § 1.510(b), Requestor provides the following statement identifying each substantial new question of patentability raised in this request, identifying the claims for which reexamination is requested, and explaining in detail the pertinency and manner of applying the cited art to the claims for which reexamination is requested.

## TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	THE '118 PATENT TO BE REEXAMINED .....	3
	A.    The Original Examination.....	3
	B.    The Prior Reexamination.....	4
	C.    Related Examinations.....	7
III.	THE PRIOR ART RAISES SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY .....	7
	A.    Legal Standards for a Substantial New Question of Patentability.....	7
	B.    Willens and ChoiceNet Raise Substantial New Questions of Patentability.....	9
IV.	SUMMARY OF THE PRIOR ART REFERENCES .....	10
	A.    U.S. Patent No. 5,889,958 to Willens.....	10
	B.    The ChoiceNet™ Administrator's Guide.....	12
	C.    U.S. Patent No. 6,233,686 to Zenchelsky et al.....	14
	D.    U.S. Patent No. 6,088,451 to He et al.....	14
	E.    The Patent Owner's Admissions.....	15
	F.    The Board Declared That Redirection Is an Obvious Extension of Blocking .....	15
V.	THE CLAIMS OF THE '118 PATENT ARE OBVIOUS OVER WILLENS IN VIEW OF ZENCHELSKY AND THE PATENT OWNER'S ADMISSIONS, RAISING SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY .....	16
	A.    Claims 2-7, 28, and 30-31 Are Obvious over Willens in view of Zenchelsky and the Patent Owner's Admissions.....	16
	1. <i>Overview of Obviousness</i> .....	16
	2. <i>Detailed Explanation of Obviousness</i> .....	19
	3. <i>The Combination of Willens, Zenchelsky, and the Patent Owner's                 Admissions Renders the Common Elements of Claims 2-7, 28, and                 30-31 Obvious</i> .....	24
	4. <i>Claim 2</i> .....	25
	5. <i>Claim 3</i> .....	26
	6. <i>Claim 4</i> .....	26
	7. <i>Claim 5</i> .....	27
	8. <i>Claim 6</i> .....	27
	9. <i>Claim 7</i> .....	28

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

10.	<i>Claim 28</i> .....	28
11.	<i>Claim 30</i> .....	29
12.	<i>Claim 31</i> .....	30
B.	Claims 9-14, 32, and 34-35 Are Obvious over Willens in view of Zenchelsky and the Patent Owner’s Admissions.....	30
1.	<i>Detailed Explanation of Obviousness</i> .....	30
2.	<i>The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders the Common Elements of Claims 9-14, 32, and 34-35 Obvious</i> .....	34
3.	<i>Claim 9</i> .....	35
4.	<i>Claim 10</i> .....	36
5.	<i>Claim 11</i> .....	37
6.	<i>Claim 12</i> .....	37
7.	<i>Claim 13</i> .....	38
8.	<i>Claim 14</i> .....	38
9.	<i>Claim 32</i> .....	39
10.	<i>Claim 34</i> .....	40
11.	<i>Claim 35</i> .....	40
C.	Claims 16-24, 36, and 38-39 Are Obvious over Willens in view of Zenchelsky and the Patent Owner’s Admissions.....	41
1.	<i>Detailed Explanation of Obviousness</i> .....	41
2.	<i>The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders the Common Elements of Claims 16-24, 36, and 38-39 Obvious</i> .....	43
3.	<i>Claim 16</i> .....	44
4.	<i>Claim 17</i> .....	45
5.	<i>Claim 18</i> .....	46
6.	<i>Claim 19</i> .....	46
7.	<i>Claim 20</i> .....	47
8.	<i>Claim 21</i> .....	48
9.	<i>Claim 22</i> .....	48
10.	<i>Claim 23</i> .....	49
11.	<i>Claim 24</i> .....	50
12.	<i>Claim 36</i> .....	50

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

13.	<i>Claim 38</i> .....	51
14.	<i>Claim 39</i> .....	51
D.	Claims 26-27, 40, and 42-43 Are Obvious over Willens in view of Zenchelsky and the Patent Owner’s Admissions.....	52
1.	<i>Detailed Explanation of Obviousness</i> .....	52
2.	<i>The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders the Common Elements of Claims 26-27, 40, and 42-43 Obvious</i> .....	55
3.	<i>Claim 26</i> .....	56
4.	<i>Claim 27</i> .....	57
5.	<i>Claim 40</i> .....	58
6.	<i>Claim 42</i> .....	58
7.	<i>Claim 43</i> .....	59
E.	Claim 44 Is Obvious over Willens in View of Zenchelsky and the Patent Owner’s Admissions .....	59
1.	<i>Overview of Obviousness</i> .....	59
2.	<i>Detailed Explanation of Obviousness</i> .....	60
3.	<i>The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 44 Obvious</i> .....	63
F.	Claim 56 Is Obvious over Willens in view of Zenchelsky and the Patent Owner’s Admissions .....	64
1.	<i>Detailed Explanation of Obviousness</i> .....	64
2.	<i>The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 56 Obvious</i> .....	68
G.	Claim 68 Is Obvious over Willens in view of Zenchelsky and the Patent Owner’s Admissions .....	69
1.	<i>Detailed Explanation of Obviousness</i> .....	69
2.	<i>The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 68 Obvious</i> .....	72
H.	Claim 83 Is Obvious over Willens in View of Zenchelsky and the Patent Owner’s Admissions .....	73
1.	<i>Detailed Explanation of Obviousness</i> .....	73
2.	<i>The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 83 Obvious</i> .....	76

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

I.	Claims 45-51, 53-55, 57-63, 65-67, 69-78, 80-82, 84-86, and 88-90 are Obvious over Willens in View of Zenchelsky and the Patent Owner's Admissions .....	78
1.	<i>Claim 45</i> .....	78
2.	<i>Claim 46</i> .....	78
3.	<i>Claim 47</i> .....	79
4.	<i>Claim 48</i> .....	79
5.	<i>Claim 49</i> .....	80
6.	<i>Claim 50</i> .....	80
7.	<i>Claim 51</i> .....	81
8.	<i>Claim 53</i> .....	81
9.	<i>Claim 54</i> .....	82
10.	<i>Claim 55</i> .....	82
11.	<i>Claim 57</i> .....	83
12.	<i>Claim 58</i> .....	83
13.	<i>Claim 59</i> .....	84
14.	<i>Claim 60</i> .....	84
15.	<i>Claim 61</i> .....	85
16.	<i>Claim 62</i> .....	85
17.	<i>Claim 63</i> .....	86
18.	<i>Claim 65</i> .....	86
19.	<i>Claim 66</i> .....	87
20.	<i>Claim 67</i> .....	88
21.	<i>Claim 69</i> .....	88
22.	<i>Claim 70</i> .....	89
23.	<i>Claim 71</i> .....	90
24.	<i>Claim 72</i> .....	90
25.	<i>Claim 73</i> .....	91
26.	<i>Claim 74</i> .....	92
27.	<i>Claim 75</i> .....	92
28.	<i>Claim 76</i> .....	93
29.	<i>Claim 77</i> .....	94
30.	<i>Claim 78</i> .....	94

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

31.	<i>Claim 80</i> .....	95
32.	<i>Claim 81</i> .....	96
33.	<i>Claim 82</i> .....	96
34.	<i>Claim 84</i> .....	97
35.	<i>Claim 85</i> .....	97
36.	<i>Claim 86</i> .....	98
37.	<i>Claim 88</i> .....	99
38.	<i>Claim 89</i> .....	99
39.	<i>Claim 90</i> .....	100
VI.	CLAIMS 29, 33, 37, 41, 52, 64, 79, AND 87 ARE OBVIOUS OVER WILLENS IN VIEW OF HE, ZENCHELSKY, AND THE PATENT OWNER’S ADMISSIONS.....	101
A.	Claims 29, 33, 52, and 64.....	101
B.	Claims 37, 41, 79, and 87.....	102
VII.	THE CLAIMS OF THE ’118 PATENT ARE OBVIOUS OVER CHOICENET IN VIEW OF ZENCHELSKY AND THE PATENT OWNER’S ADMISSIONS, RAISING SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY .....	104
A.	Claims 2-7, 28, and 30-31 Are Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s Admissions.....	104
1.	<i>Overview of Obviousness</i> .....	104
2.	<i>Detailed Explanation of Obviousness</i> .....	106
3.	<i>The Combination of ChoiceNet, Zenchelsky, and the Patent Owner’s Admissions Renders the Common Elements of Claims 2-7 and 28-31 Obvious</i> .....	110
4.	<i>Claim 2</i> .....	111
5.	<i>Claim 3</i> .....	112
6.	<i>Claim 4</i> .....	112
7.	<i>Claim 5</i> .....	113
8.	<i>Claim 6</i> .....	113
9.	<i>Claim 7</i> .....	114
10.	<i>Claim 28</i> .....	114
11.	<i>Claim 30</i> .....	115
12.	<i>Claim 31</i> .....	115
B.	Claims 9-14, 32, and 34-35 Are Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s Admissions.....	116

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

1.	<i>Detailed Explanation of Obviousness</i> .....	116
2.	<i>The Combination of ChoiceNet, Zenchelsky, and the Patent Owner's Admissions Renders the Common Elements of Claims 9-14 and 32-35 Obvious</i> .....	119
3.	<i>Claim 9</i> .....	120
4.	<i>Claim 10</i> .....	121
5.	<i>Claim 11</i> .....	122
6.	<i>Claim 12</i> .....	122
7.	<i>Claim 13</i> .....	123
8.	<i>Claim 14</i> .....	123
9.	<i>Claim 32</i> .....	124
10.	<i>Claim 34</i> .....	125
11.	<i>Claim 35</i> .....	125
C.	Claims 16-24, 36, and 38-39 Are Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's Admissions.....	126
1.	<i>Detailed Explanation of Obviousness</i> .....	126
2.	<i>The Combination of ChoiceNet, Zenchelsky, and the Patent Owner's Admissions Renders the Common Elements of Claims 16-24 and 36-39 Obvious</i> .....	128
3.	<i>Claim 16</i> .....	129
4.	<i>Claim 17</i> .....	130
5.	<i>Claim 18</i> .....	130
6.	<i>Claim 19</i> .....	131
7.	<i>Claim 20</i> .....	132
8.	<i>Claim 21</i> .....	133
9.	<i>Claim 22</i> .....	133
10.	<i>Claim 23</i> .....	134
11.	<i>Claim 24</i> .....	134
12.	<i>Claim 36</i> .....	135
13.	<i>Claim 38</i> .....	136
14.	<i>Claim 39</i> .....	136
D.	Claims 26-27, 40, and 42-43 Are Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's Admissions.....	137
1.	<i>Detailed Explanation of Obviousness</i> .....	137

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

2.	<i>The Combination of ChoiceNet, Zenchelsky, and the Patent Owner's Admissions Renders the Common Elements of Claims 26-27 and 40-43 Obvious.....</i>	140
3.	<i>Claim 26.....</i>	141
4.	<i>Claim 27.....</i>	142
5.	<i>Claim 40.....</i>	142
6.	<i>Claim 42.....</i>	143
7.	<i>Claim 43.....</i>	144
E.	Claim 44 Is Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's Admissions .....	144
1.	<i>Overview of Obviousness.....</i>	144
2.	<i>Detailed Explanation of Obviousness .....</i>	145
3.	<i>The Combination of ChoiceNet, Zenchelsky, and the Patent Owner's Admissions Renders Claim 44 Obvious.....</i>	147
F.	Claim 56 Is Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's Admissions .....	148
1.	<i>Detailed Explanation of Obviousness .....</i>	148
2.	<i>The Combination of ChoiceNet, Zenchelsky, and the Patent Owner's Admissions Renders Claim 56 Obvious.....</i>	151
G.	Claim 68 Is Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's Admissions .....	153
1.	<i>Detailed Explanation of Obviousness .....</i>	153
2.	<i>The Combination of ChoiceNet, Zenchelsky, and the Patent Owner's Admissions Renders Claim 68 Obvious.....</i>	155
H.	Claim 83 Is Obvious over ChoiceNet in View of Zenchelsky and the Patent Owner's Admissions .....	156
1.	<i>Detailed Explanation of Obviousness .....</i>	156
2.	<i>The Combination of ChoiceNet, Zenchelsky, and the Patent Owner's Admissions Renders Claim 83 Obvious.....</i>	159
I.	Claims 45-51, 53-55, 57-63, 65-67, 69-78, 80-82, 84-86, and 88-90 are Obvious over ChoiceNet in View of Zenchelsky and the Patent Owner's Admissions .....	160
1.	<i>Claim 45.....</i>	160
2.	<i>Claim 46.....</i>	161
3.	<i>Claim 47.....</i>	161
4.	<i>Claim 48.....</i>	162

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

5.	<i>Claim 49</i> .....	162
6.	<i>Claim 50</i> .....	163
7.	<i>Claim 51</i> .....	163
8.	<i>Claim 53</i> .....	164
9.	<i>Claim 54</i> .....	165
10.	<i>Claim 55</i> .....	165
11.	<i>Claim 57</i> .....	166
12.	<i>Claim 58</i> .....	166
13.	<i>Claim 59</i> .....	167
14.	<i>Claim 60</i> .....	167
15.	<i>Claim 61</i> .....	168
16.	<i>Claim 62</i> .....	168
17.	<i>Claim 63</i> .....	169
18.	<i>Claim 65</i> .....	169
19.	<i>Claim 66</i> .....	170
20.	<i>Claim 67</i> .....	170
21.	<i>Claim 69</i> .....	171
22.	<i>Claim 70</i> .....	172
23.	<i>Claim 71</i> .....	173
24.	<i>Claim 72</i> .....	173
25.	<i>Claim 73</i> .....	174
26.	<i>Claim 74</i> .....	175
27.	<i>Claim 75</i> .....	175
28.	<i>Claim 76</i> .....	176
29.	<i>Claim 77</i> .....	177
30.	<i>Claim 78</i> .....	177
31.	<i>Claim 80</i> .....	178
32.	<i>Claim 81</i> .....	179
33.	<i>Claim 82</i> .....	179
34.	<i>Claim 84</i> .....	180
35.	<i>Claim 85</i> .....	180
36.	<i>Claim 86</i> .....	181

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

37.	<i>Claim 88</i> .....	182
38.	<i>Claim 89</i> .....	182
39.	<i>Claim 90</i> .....	183
VIII.	CLAIMS 29, 33, 37, 41, 52, 64, 79, AND 87 ARE OBVIOUS OVER CHOICENET IN VIEW OF HE, ZENCHELSKY, AND THE PATENT OWNER'S ADMISSIONS .....	184
A.	Claims 29, 33, 52, and 64.....	184
B.	Claims 37, 41, 79, and 87.....	185
IX.	CONCLUSION.....	186
X.	CERTIFICATE OF SERVICE .....	188
XI.	APPENDIX: CLAIM CHARTS.....	189

**TABLE OF EXHIBITS**

U.S. PATENT NO.: 6,779,118 (“THE ’118 PATENT”) ..... A  
U.S. PATENT NO.: 5,889,958 (“WILLENS”) ..... B  
THE CHOICENET™ ADMINISTRATOR’S GUIDE, JANUARY 1997 (“CHOICENET”) ..... C  
U.S. PATENT NO.: 6,233,686 (“ZENCHELSKY”) ..... D  
EX PARTE LINKSMART WIRELESS TECHNOLOGY, LLC, NO. 2011-009566 (B.P.A.I. AUG.  
23, 2011) ..... E  
U.S. PATENT NO.: 6,088,451 (“HE”) ..... F

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

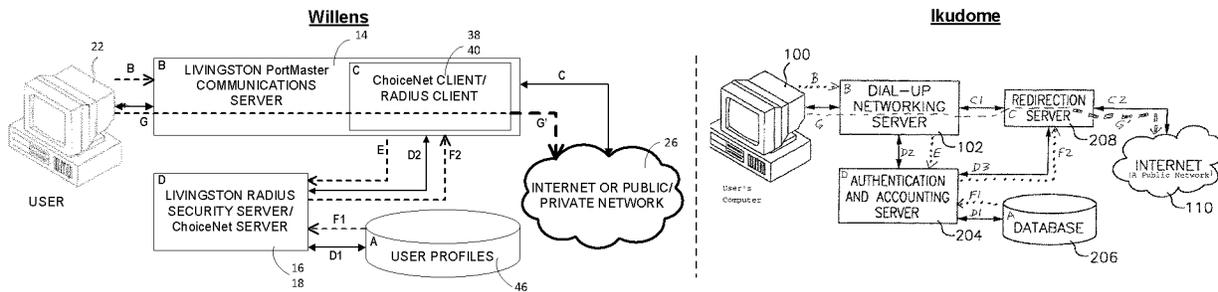
**I. INTRODUCTION**

Requestor respectfully submits this request for reexamination of **Claims 2-7, 9-14, 16-24, and 26-90** of U.S. Patent No. 6,779,118 (filed Apr. 21, 1999) to Ikudome et al. (“the ’118 Patent”), a copy of which is attached as Exhibit A. As explained in detail below, Claims 2-7, 9-14, 16-24, 26-27, 29-32, 34-36, 38-40, 42-51, 53-63, 65-78, 80-87, and 89-90 are rendered obvious by **U.S. Patent No. 5,889,958 (filed Dec. 20, 1996) to Willens (“Willens”) in view of U.S. Patent No. 6,233,686 to Zenchelsky et al. (“Zenchelsky”) and the Patent Owner’s admissions in the ’118 Patent.** Claims 29, 33, 37, 41, 52, 64, 79, and 87 are rendered obvious by Willens in view of Zenchelsky and the Patent Owner’s admissions, and further in view of U.S. Patent No. 6,088,451 to He et al. (“He”). In addition, Claims 2-7, 9-14, 16-24, 26-27, 29-32, 34-36, 38-40, 42-51, 53-63, 65-78, 80-87, and 89-90 are rendered obvious by ***ChoiceNet™ Administrator’s Guide (Jan. 1997) (“ChoiceNet”) in view of Zenchelsky and the Patent Owner’s admissions in the ’118 Patent.*** Claims 29, 33, 37, 41, 52, 64, 79, and 87 are rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions, and further in view of He.

The ’118 patent was reexamined in a prior proceeding, No. 90/009,301 (the “Prior Reexamination”), filed December 17, 2008. The Reexamination Certificate in the Prior Reexamination, No. 8926, was issued on March 27, 2012. As a result of the Prior Reexamination, claims 2-7, 9-14, 16-24, and 26-90 were determined to be patentable. Requestor requests reexamination of these claims.

As a summary of the argument presented in detail in this request, Willens teaches a system used to control access to the Internet or public network, as depicted in the left-hand figure in Diagram 1 below. The ’118 Patent claims a system for controlling access to the Internet, as depicted in the right-hand figure below (which is a diagram submitted by the Patent Owner in an after-final Office Action response in the Prior Reexamination). The few differences that exist between the two systems would have been obvious at the time of the invention in view of the Patent Owner’s admissions of the state of the prior art and Zenchelsky.

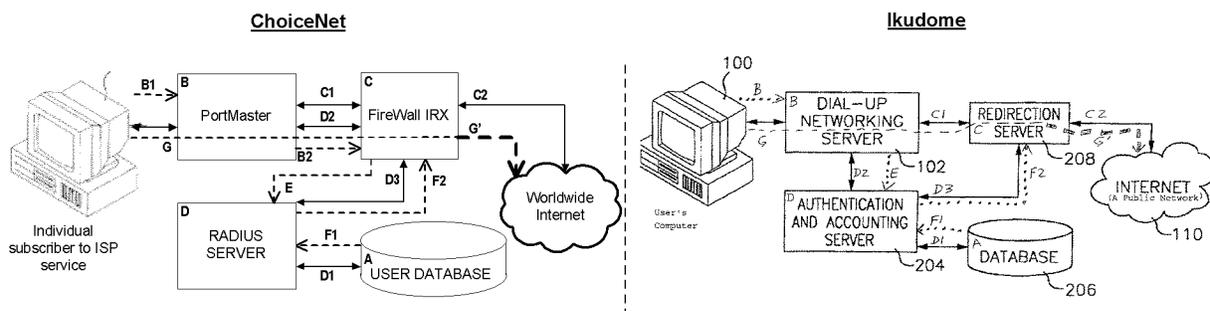
**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**



**Diagram 1 – The system in Willens (left) compared to the system claimed in the '118 Patent (right). Full versions of these figures are on pages 16 and 17.**

Willens teaches a server that permits or denies user access requests based on filter rules, but may not teach a server that additionally performs redirection. However, in view of the Patent Owner's admissions, the Board of Patent Appeals and Interferences (the "Board") declared that redirection is an obvious extension of blocking. Furthermore, Willens may not teach assigning a temporary network address to a user computer associated with a user ID. However, the Patent Owner's admissions, as demonstrated by Zenchelsky, teaches this limitation.

In addition, ChoiceNet teaches a system for controlling access to the Internet, which was cited by an examiner in a pending continuation application as anticipating a system similar to the one claimed in the '118 Patent. To illustrate, ChoiceNet teaches the system depicted in the left-hand figure below in Diagram 2. The right-hand figure again is the figure submitted by the Patent Owner in the Prior Reexamination. The few differences that exist between the two systems would have been obvious at the time of the invention in view of the Patent Owner's admissions of the state of the prior art and Zenchelsky.



**Diagram 2 – The system in ChoiceNet (left) compared to the system claimed in the '118 Patent (right). Full versions of these figures are on pages 16 and 105.**

ChoiceNet teaches a server that permits or denies user access requests based on filter rules, but may not teach a server that additionally performs redirection. However, in view of the Patent Owner's admissions, the Board declared that redirection is an obvious extension of

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

blocking. Furthermore, ChoiceNet may not teach assigning a temporary network address to a user computer associated with a user ID. However, the Patent Owner's admissions, as demonstrated by Zenchelsky, teaches this limitation.

During the Prior Reexamination, the Patent Owner canceled independent Claims 1, 8, 15, and 25 and added corresponding independent claims 44, 56, 68, and 83 to "clarify the 'between' location of the redirection server," where "between" corresponds to "the redirection server 208 [being] located *between* the user's computer 100 and the network." U.S. Patent App. No. 90/009,301 Response and Proposed Amendment, at 3, 24 (October 24, 2012) (emphasis original). Both Willens and ChoiceNet teach a network topology having a redirection server located between a user computer and a public network, as shown in Diagrams 1 and 2. Furthermore, the additional limitations set forth in dependent claims in the '118 Patent would have been obvious over either Willens or ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

The proposed combination of references presents a substantial new question of patentability that warrants *ex parte* reexamination. Willens and ChoiceNet were never specifically analyzed in view of the claims during the Prior Reexamination, but rather only mentioned in an Information Disclosure Statement. Moreover, a substantial new question of patentability of the '118 Patent is raised because the decision of the Board in the Prior Reexamination introduced a new interpretation of the prior art based on the Patent Owner's admissions, casting references like Willens and ChoiceNet in a new light. Specifically, in view of the Patent Owner's admissions, the Board stated that "redirection is an obvious extension of the use of a control to block the user." *Ex parte Linksmart Wireless Tech.*, No. 2011-009566, at 9 (B.P.A.I. Aug. 23, 2011). This finding by the Board opened the door to new grounds for obviousness based on references directed to systems that control access to a network by blocking. Thus, according to the Board's finding in view of the Patent Owner's admissions, it would have been obvious to one having skill in the art at the time of the invention to modify controls that block the user, as in the Willens and ChoiceNet systems, to redirect the user.

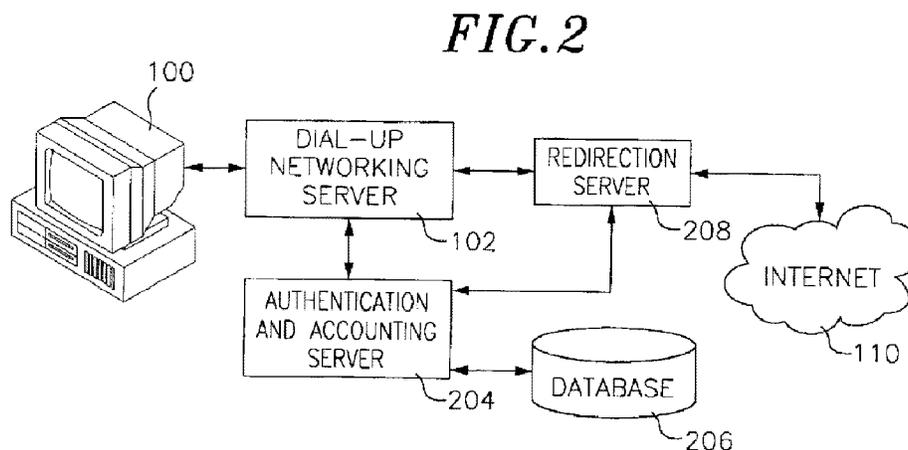
**II. THE '118 PATENT TO BE REEXAMINED**

**A. The Original Examination**

The '118 Patent was filed May 1999, and it claims priority to a provisional application filed May 1998. The patent generally discloses a computer system that connects dial-up network

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

user computers to the Internet. The main components of the system are a dial-up networking server (102) that is used to “establish a communications link with the user’s PC”; an authentication server (204) to “authenticate user ID [sic] and permit, or deny, access to the network”; a database with rule sets “unique for each user ID”; and a redirection server (208) that is “programed [sic] to implement the rule set.” *Col. 3 ll. 61-62; col. 4 ll. 7-8, 41, 61.*<sup>1</sup> “Rule sets may contain data about a type of service which may or may not be accessed, a location which may or may not be accessed, how long to keep the rule set active, under what conditions the rule set should be removed, when and how to modify the rule set during a session, and the like.” *Col. 4 ll. 42-47.* These system components are depicted in Figure 2 of the patent, reproduced in Diagram 3 below.



**Diagram 3 - The system claimed in the '118 Patent**

**B. The Prior Reexamination**

During the Prior Reexamination, the Board found independent Claims 1, 8, 15, and 25 to be obvious. *Linksmart Wireless Tech.*, No. 2011-009566, at 10. Subsequent to the Board’s decision, the Patent Owner canceled Claims 1, 8, 15, and 25 and added corresponding independent Claims 44, 56, 68, and 83 and dependent claims. The Patent Owner explained that “a new set of claims is provided (48-94) [44-90 after claim renumbering] which corresponds to the claim set that was appealed, and which *further clarifies the location of the redirection server.*” Response and Proposed Amendment, at 3 (emphasis added). Specifically, the Patent Owner stated that the independent claims have “additional terms to clarify the ‘between’ location of the redirection server.” *Id.* Furthermore, the Patent Owner explained that “[t]hese clarifications were discussed with the Examiners...and the Examiner stated that such

<sup>1</sup> Unless otherwise specified, column and line numbers are citations to the patent being discussed.

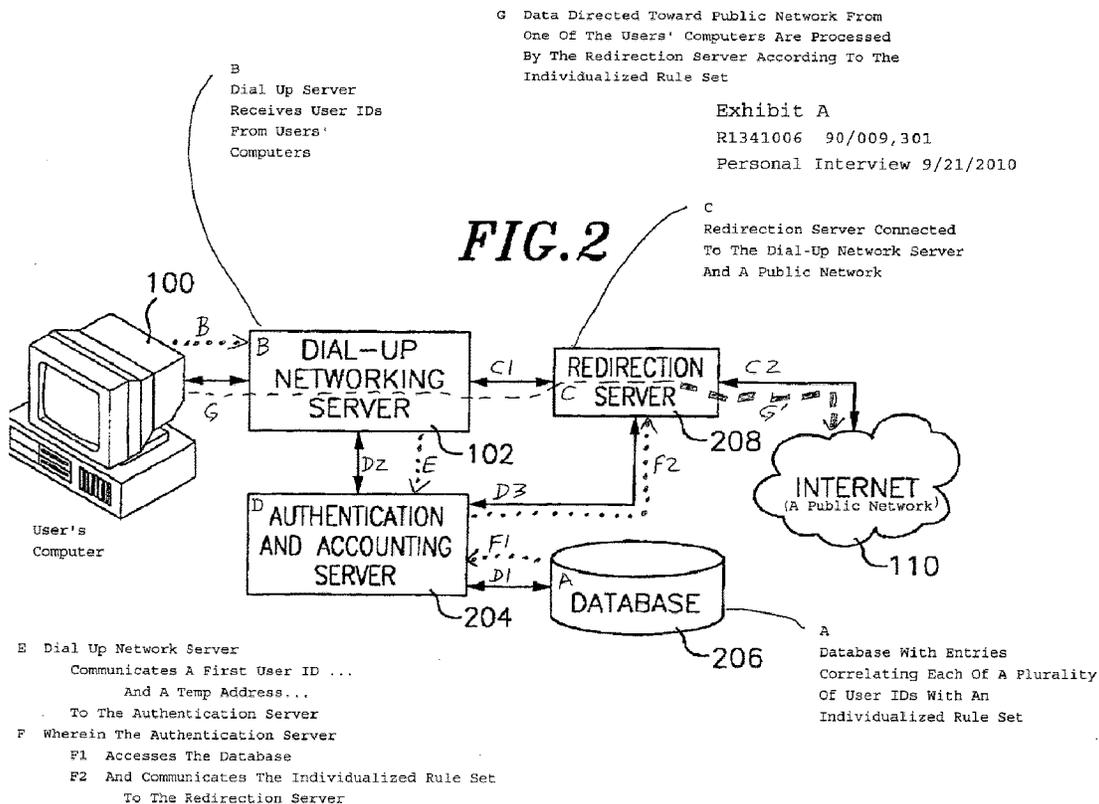
**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

clarifications would overcome the applied art and make these claims patentable.” *Id.* Finally, the Patent Owner declared that “new dependent claims 45-54, 57-66, 69-81, and 84-89...generally correspond respectively, to dependent claims 2-7, 28-31, 9-14, 32-35, 16-24, 36-39, 26-27, and 40-43.” *Id.* (all numbers adjusted according to the numbering of the claims as issued).

As a result, the '118 Patent includes 86 claims which are the subject of this request. These claims may be categorized into 2 groups based on subject matter. Claims 2-7, 9-14, and 44-67 pertain to controlling access to the Internet based on rule sets. Claims 16-24, 26-43, and 68-90 relate to modification of the rule sets. Claim 44 is representative of the first group, while Claim 68 is representative of the second. Claim 44 is identical to canceled Claim 1 in the '118 Patent except for a change in one word, rather than “a redirection server connected to the dial-up network server and a public network” as in Claim 1 (emphasis added), Claim 44 states “a redirection server connected between the dial-up network server and a public network” (emphasis added). Similarly, Claim 68 is identical to canceled Claim 15 but for a similar change to indicate that the redirection server is *between* the dial-up network server and the public network.

Regarding Claim 1, the Patent Owner submitted the following explanatory diagram as Appendix A to an After-Final Response filed October 4, 2010 in the Prior Reexamination.

Patent No.: 6,779,118  
Request for *Ex Parte* Reexamination



**Diagram 4 - Annotated figure of the claimed system in the '118 Patent**

In the After-Final Response, the Patent Owner explained how Claim 1 is depicted in the above annotated figure. The key elements of that explanation are as follows:

- The user computer connects to the Dial-up Networking Server (arrow B, ref. 100 to 102)
- The Dial-up Networking Server sends a user ID and network address to the Authentication Server (arrow E, ref. 102 to 204)
- The Authentication Server locates a corresponding rule set in the Database and sends that rule set, along with the network address, to the Redirection Server (arrows F1 and F2, ref. 206 to 204 and 204 to 208)
- Data from the user computer and directed toward the public network is processed by the Redirection Server, according to the rule set (arrow G, ref. 100 through 102 and 208 to 110)

Claim 68 relates primarily to the redirection server, and in particular the ability to allow modifications to rule sets on the redirection server. Generally, the claims require the following elements:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

- A redirection server is programmed with a user's rule set
- The redirection server allows automated modification of the rule set
- The modification is based on time, data transmitted to/from the user, and/or a location the user accesses

**C. Related Examinations**

U.S. Patent Application No. 11/645,924, Publication No. 20070294417 (filed Dec. 26, 2006) is a pending continuation of the '118 Patent. During prosecution of the application, the examiner stated in a non-final rejection dated March 1, 2011, that ChoiceNet anticipated claims to a redirection server having similar functionality as the claims presented in this request. In an amendment dated August 8, 2011, Applicant amended the claims to get around ChoiceNet. In light of this amendment, the examiner vacated the rejection based on ChoiceNet in a final rejection dated October 20, 2011, stating the rejection was moot "in view of the changed scope of the amended claims." U.S. Patent App. No. 11/645,924 Final Rejection, at 2 (October 20, 2011).

Further details on the '118 Patent, its file history, and litigation related to the patent are summarized in the Request for Ex Parte Reexamination filed by Jerry Turner Sewell on December 17, 2008, in the Prior Reexamination.

**III. THE PRIOR ART RAISES SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY**

**A. Legal Standards for a Substantial New Question of Patentability**

As 35 U.S.C. § 303(a) provides, "[w]ithin three months following the filing of a request for reexamination under the provisions of section 302 of this title, the Director will determine whether a substantial new question of patentability affecting any claim of the patent concerned is raised by the request, with or without consideration of other patents or printed publications." Furthermore, 35 U.S.C. § 304 states that "[i]f, in a determination made under the provisions of subsection 303(a) of this title, the Director finds that a substantial new question of patentability affecting any claim of a patent is raised, the determination will include an order for reexamination of the patent for resolution of the question."

The Manual of Patent Examining Procedure (M.P.E.P.) provides that:

A prior art patent or printed publication raises a substantial question of patentability where there is a substantial likelihood that a reasonable examiner

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

would consider the prior art patent or printed publication important in deciding whether or not the claim is patentable. If the prior art patents and/or publications would be considered important, then the examiner should find “a substantial new question of patentability” unless the same question of patentability has already been decided as to the claim in a final holding of invalidity by the Federal court system or by the Office in a previous examination.

M.P.E.P., § 2242, at 2200-57 (8th ed. Rev. 8, July 2010). Although 35 U.S.C. § 303(a) calls for a “substantial new question of patentability,” a prior art reference is eligible to raise a substantial new question of patentability even if it was previously cited or considered during examination or litigation of the patent.

Amended in 2002, 35 U.S.C. § 303(a) now provides, in pertinent part, that “[t]he existence of a substantial new question of patentability is not precluded by the fact that a patent or printed publication was previously cited by or to the Office or considered by the Office.” The Federal Circuit recently explained that, “to decide whether a reference that was previously considered by the PTO creates a substantial new question of patentability, the PTO should evaluate the context in which the reference was previously considered and the scope of the prior consideration and determine whether the reference is now being considered for a substantially different purpose.” *In re Swanson*, No. 2007-1534 (Reexamination No. 90/006,785) at 21, 540 F.3d 1368, 1380 (Fed. Cir. Sep. 4, 2008). For a reference previously submitted in an information disclosure statement, the scope of the prior consideration depends on the explanation of the patent owner regarding the “content and relevance” of the reference:

Where patents, publications, and other such items of information are submitted by a party (patent owner or requester) in compliance with the requirements of the rules, *the requisite degree of consideration to be given to such information will be normally limited by the degree to which the party filing the information citation has explained the content and relevance of the information.* The initials of the examiner placed adjacent to the citations on the form PTO/SB/08A and 08B or its equivalent, without an indication to the contrary in the record, do not signify that the information has been considered by the examiner any further than to the extent noted above.

M.P.E.P., § 2256, at 2200-87 (emphasis added).

Moreover, in a reexamination ordered on or after November 2, 2002, the examiner may base a rejection exclusively on a reference cited or considered in a previous examination:

For a reexamination that was ordered on or after November 2, 2002 . . . , reliance solely on old art (as the basis for a rejection) does not necessarily preclude the existence of a substantial new question of patentability (SNQ) that is based

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

exclusively on that old art. Determinations on whether a SNQ exists in such an instance shall be based upon a fact-specific inquiry done on a case-by-case basis. For example, a SNQ may be based solely on old art where the old art is being presented/viewed in a new light, or in a different way, as compared with its use in the earlier concluded examination(s), in view of a material new argument or interpretation presented in the request.

M.P.E.P., § 2258.01, at 2200-98.

**B. Willens and ChoiceNet Raise Substantial New Questions of Patentability**

Willens and ChoiceNet raise substantial new questions of patentability even though they were submitted in Information Disclosure Statements in the Prior Reexamination. This is so because (1) the references are presented in a new light, in view of the Board decision in the Prior Reexamination, and (2) references cited without explanation during a reexamination are ordinarily not considered by the examiner.

Both Willens and ChoiceNet are prior art to the '118 Patent. U.S. Patent No. 5,889,958 to Willens was filed December 20, 1996, so it is prior art under 35 U.S.C. § 102(e). The *ChoiceNet™ Administrator's Guide* was published January 1997, so it is prior art under 35 U.S.C. § 102(b).

As stated above, a substantial new question of patentability may be based on art that has been cited or considered during prosecution where it is “being presented/viewed in a new light,” as compared with the earlier examination, “in view of a material new argument or interpretation presented in the request.” M.P.E.P., § 2258.01, at 2200-98. The PTO should evaluate the context and scope of the prior consideration to see if it is being applied for a substantially different purpose. *See In re Swanson*, No. 2007-1534 at 21, 540 F.3d at 1380. For a reference submitted in an information disclosure statement, the scope of prior consideration depends on the patent owner’s explanation of the “content and relevance” of the reference. M.P.E.P., § 2256, at 2200-87.

The Examiner did not have the benefit of the Board’s decision when analyzing Willens and ChoiceNet. In view of the Patent Owner’s admissions, the Board declared that redirection “would have been an obvious extension of blocking” at the time of the invention. *Ex parte Linksmart Wireless Tech.*, No. 2011-009566, at 9-10 (B.P.A.I. Aug. 23, 2011). The Board’s decision casts all prior art references in a new light because the Board stated that redirection is obvious and in the prior art, as admitted by the Patent Owner. This new interpretation opened the door to new references and new interpretations of old art that did not teach redirection but

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

from which redirection could be derived. Hence, the Board's decision implies that it would have been obvious to one having skill in the art at the time of the invention to modify the systems in Willens and ChoiceNet to perform redirection.

Furthermore, as explained above, a reference cited in an information disclosure statement during a reexamination proceeding is given consideration "normally limited by the degree to which the party filing the information citation has explained the content and relevance of the information." M.P.E.P., § 2256. Here, Willens and ChoiceNet were submitted during the Prior Reexamination in Information Disclosure Statements dated November 16, 2009 and October 15, 2010, respectively. The Patent Owner explained neither the content nor the relevance of the references in conjunction with the information disclosure statements except to state that ChoiceNet was referenced in invalidity contentions served by defendants in related litigation.<sup>2</sup> See U.S. Patent App. No. 90/009,301 Transmittal Letters dated November 16, 2009 and October 15, 2010. Following the M.P.E.P., the examiner would accordingly have given Willens and ChoiceNet no consideration, because the party filing the citations failed to explain the content and relevance of Willens and ChoiceNet.

Thus, Willens and ChoiceNet are being presented in a new light because of the material new interpretation provided by the Board in the Prior Reexamination. Because of this new interpretation and a lack of explanation of the content and relevance of Willens and ChoiceNet, the application of these references is substantially different in both context and scope from their prior consideration. Moreover, as explained in more detail below, Willens and ChoiceNet disclose all or almost all of the limitations of each of Claims 2-7, 9-14, 16-24 and 26-90 of the '118 Patent in light of the Board's interpretation of the state of the prior art. As such, Requestor respectfully submits that Willens and ChoiceNet raise a substantial new question of patentability with respect to these claims.

**IV. SUMMARY OF THE PRIOR ART REFERENCES**

**A. U.S. Patent No. 5,889,958 to Willens**

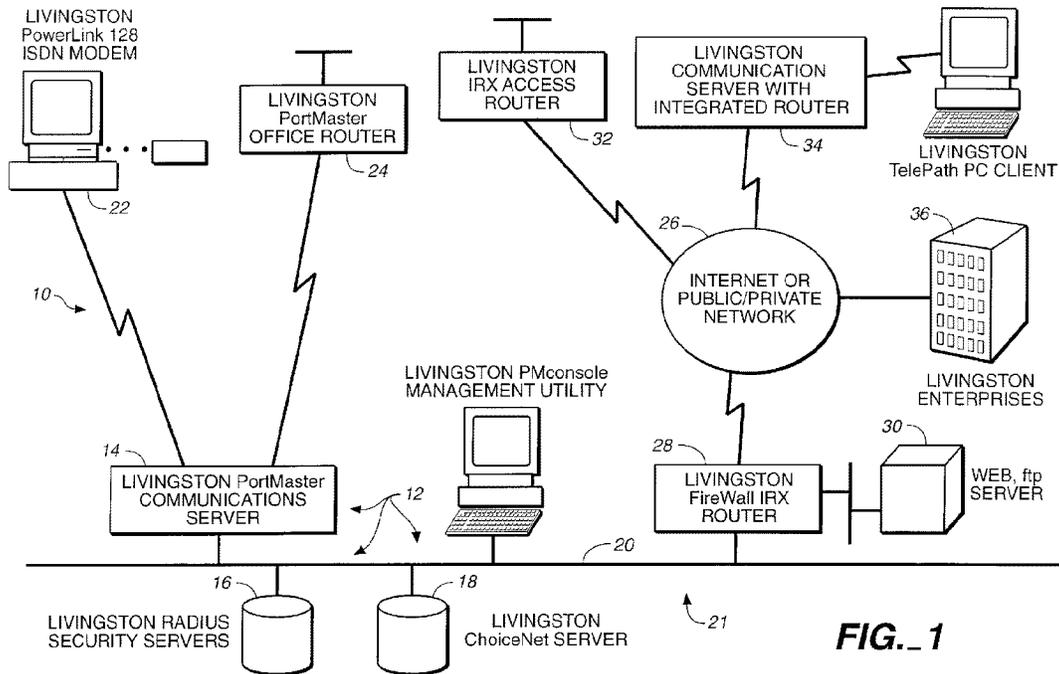
The system taught in Willens is generally an Internet access system incorporating an access control system, an authorization and accounting system, and a communications server.

---

<sup>2</sup> The related litigation referenced was *Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc., et al.*, U.S. District Court, Eastern District of Texas, Marshall Division, 2:08-cv-00254-DF-CE, 2:08-cv-00304-DF-CE, 2:08-cv-00385-DF-CD, 2:09-cv-00026-DF-CE.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

One embodiment of Willens is directed to a system to permit or deny access to data directed toward the Internet, as shown in figure 1 of Willens (Diagram 5).



**Diagram 5 - Block diagram of an Internet access system employing network access controls according to the invention in Willens**

A user 22 can gain access to the Internet or public network 26 by establishing a connection with communications server 14. *See col. 3 l. 53 to col. 4 l. 12.* Alternatively, a user can establish a connection with the communications server 14 through a router, such as the office router 24. *See col. 4 ll. 24-25.* The communications server 14 communicates with RADIUS server 16 through RADIUS client 45 to authenticate a user attempting to access the network 26, as shown in Figure 3 of Willens (Diagram 6 below). *See col. 5 ll. 9-18.* The communications server 14 communicates with ChoiceNet server 18 through ChoiceNet client 44 to control access to data directed to and from the network 26. *See col. 5 ll. 12-37.*

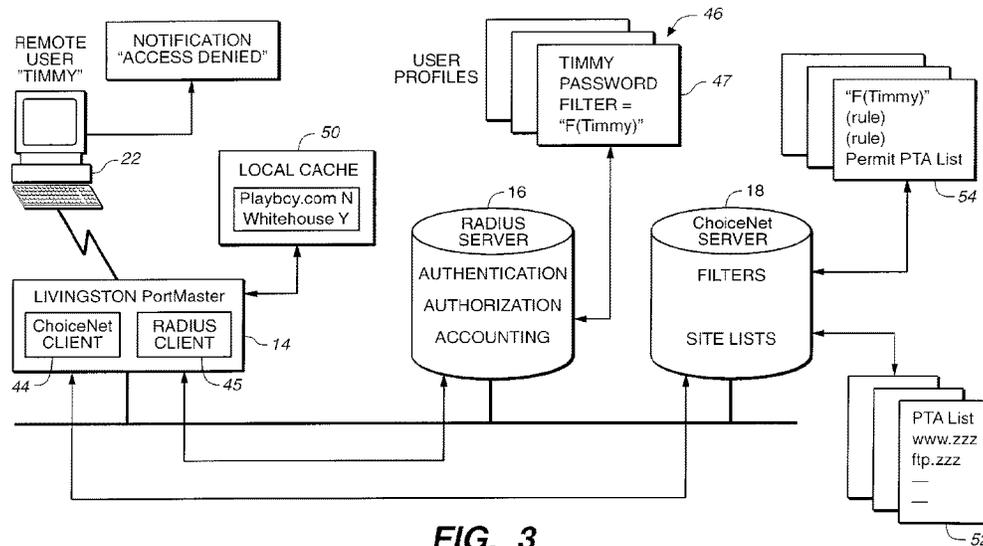


FIG. 3

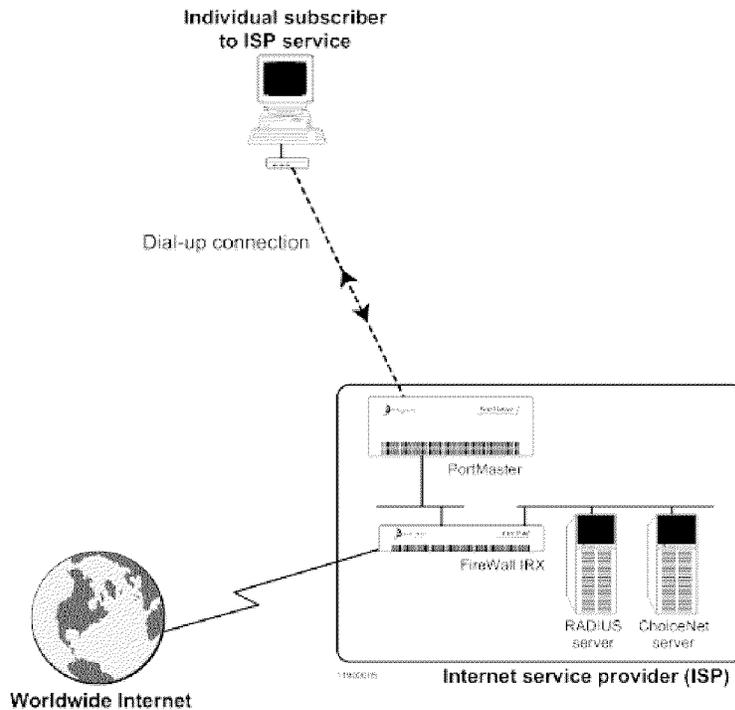
Diagram 6 - Authentication, authorization, and access systems according to the invention in Willens

As shown in figure 3 from Willens, Diagram 6 above, the RADIUS server 16 accesses stored user profiles 46, which contain filters for particular users. *See col. 5 ll. 9-18*. Once a user 22 logs in through the RADIUS server 16, the RADIUS server returns the user profile associated with the remote user 22. *See Id.* The ChoiceNet client 44 controls data directed to the network based on the identified filter(s) returned by the RADIUS server, using its local cache 50 and filter rules 54 retrieved from the ChoiceNet server 18. *See col. 5 ll. 12-37*.

**B. The ChoiceNet™ Administrator's Guide**

The system taught in ChoiceNet is generally “a client/server packet-filtering application” that “provides a mechanism to filter network traffic on dial-up remote access.” *ChoiceNet™ Administrator's Guide* 1-1 (Jan. 1997). One embodiment of the system taught in ChoiceNet is directed to a system configured to establish and control access to the Worldwide Internet, as shown in figure 5-10 of ChoiceNet and reproduced here as Diagram 7.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

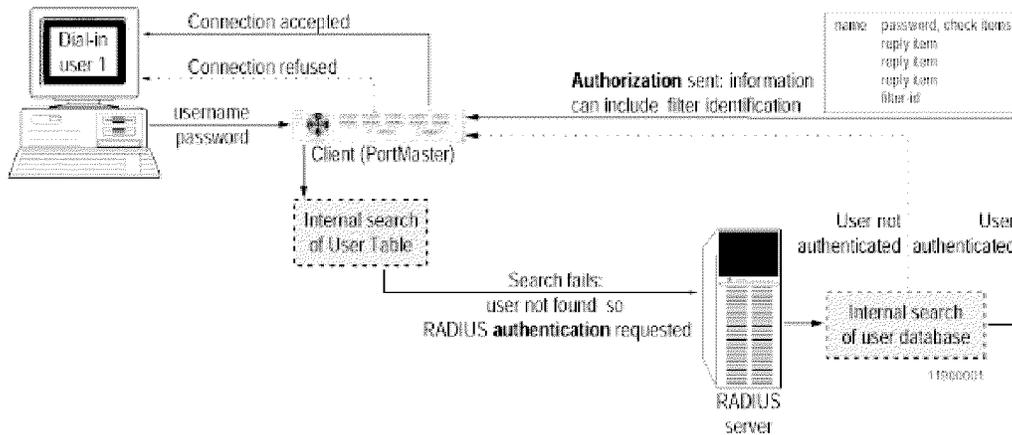


**Diagram 7 – Embodiment of an Internet access and control system according to ChoiceNet**

A user establishes a dial-up connection to a PortMaster client. *See id.* fig. 5-10. The PortMaster client is connected to a FireWall IRX Router. *See id.* The FireWall IRX connects to a RADIUS server and a ChoiceNet server, and is connected to the Worldwide Internet. *See id.*

As shown in figure 1-2 in ChoiceNet, reproduced here as Diagram 8, a user establishes a connection by authorizing their username and password through a PortMaster client and/or a RADIUS server. *See id.* at 1-6. As part of the interaction between the PortMaster and the RADIUS server, a filter-Id can be returned to a ChoiceNet client running on the FireWall IRX. *See id.* at 1-1, 1-6. If the filter-Id is in the ChoiceNet client's local cache, it applies the rules associated with that filter. *See id.* at 1-6. If not, the ChoiceNet client requests the rules from the ChoiceNet server. *See id.* at 1-7; fig. 1-3. When a user requests access to a site on the Internet, the ChoiceNet client permits or denies access based on the rules in the filter. *See id.* at 1-7; fig. 1-4. The FireWall IRX in figure 5-10 can run a ChoiceNet client. *See id.* at 1-1.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**



**Diagram 8 - ChoiceNet's authorization and access system**

**C. U.S. Patent No. 6,233,686 to Zenchelsky et al.**

U.S. Pat. No. 6,233,686 to Zenchelsky et al. (“Zenchelsky”) was filed on January 17, 1997, so it qualifies as prior art at least under 35 U.S.C. § 102(e). Zenchelsky discloses a firewall with a filter that blocks and allows traffic between peers, or users, and a public network on a user-specific basis based in part on a temporary network address.

In the system of Zenchelsky, “[t]o obtain connectivity to the Internet, for example, a user must commonly obtain a temporary IP address from a host with a pool of such addresses. Such a temporary address is retained by the user only for the duration of a single session of connectivity with the Internet.” *Col. 1 ll. 29-35*. The system in Zenchelsky filters access to the Internet based in part on temporary IP addresses where “a user is assigned a temporary IP address by an Internet Service Provider (ISP) Point of Presence (POP) 33 from a pool of such address kept by the POP 33 for this purpose.” *Col. 3 ll. 23-26*.

**D. U.S. Patent No. 6,088,451 to He et al.**

U.S. Pat. No. 6,088,451 to He et al. (“He”) was filed on June 28, 1996, so it qualifies as prior art at least under 35 U.S.C. § 102(e). The system taught in He is generally an authentication system that enables users to gain access to online services such as server computers and printers.

He discloses “a network security architecture to provide protection to user access to the resources and information in network elements.” *Col. 33 ll. 8-10*. In one embodiment, the system in He allows or denies access based on duration of a timed session. *See col. 28 ll. 26-41*. He states “[a] session length is typically defined as the period between log-ons for a user element coupled to the network 106, or for dial-up sessions delimited by the dial-up communication

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

protocol software.” *Col. 28 ll. 26-29*. The administrator of the system in He can limit the “time that the user element and selected network can communicate with each other.” *Col. 28 ll. 31-33*. Furthermore, He states that “if the length of time that is allowed for the log-on session is exceeded, all the tickets [granting access to network elements] that have been issued to the user will also become invalid and therefore be destroyed.” *Col. 28 ll. 36-38*.

**E. The Patent Owner’s Admissions**

The Patent Owner admitted in the background section of the ’118 Patent that “[t]he redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using HTTP (hypertext transfer protocol)).” *Col. 1 ll. 38-40*. In the appeal of the Examiner’s rejection to the Board of Patent Appeals and Interferences, the Board approved the Examiner’s use of this admission to conclude “that those in the art were familiar with redirection (and how to do it).” *Linksmart Wireless*, No. 2011-009566, at 9.

Furthermore, the Patent Owner described dial-up networking servers and authentication and accounting servers and their functionality in “prior art systems” as part the background section in the ’118 Patent. *Col. 1 l. 16; see col. 1 ll. 21-24, 28-37; fig. 1*. The Patent Owner stated that “[i]n prior art systems...[t]he dial-up networking server...passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user.” *Col. 1 ll. 21-24*. The Patent Owner further stated that the authentication and accounting server verifies the end user’s user ID and password by checking them against user IDs and passwords stored in a database, and upon verification “the end user would be identified by the temporarily assigned IP address” throughout the duration of the session. *Col. 1 ll. 28-37*.

**F. The Board Declared That Redirection Is an Obvious Extension of Blocking**

In view of the Patent Owner’s admissions, the Board stated that “redirection is an obvious extension of the use of a control to block the user” and “redirection would have been an obvious extension of blocking.” *Linksmart Wireless*, No. 2011-009566, at 9, 10. Furthermore, the Board stated that “blocking a website based on [‘some combination of time, data transmitted to or from the user, or location the user accesses’] would have been obvious.” *Id.* at 9-10 (quoting the ’118 Patent, Claim 15). As an example, the Board stated that “blocking a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Based on this reasoning, the Board entered a rejection of Ikudome’s claims, stating “[s]ince redirection

would have been an obvious extension of blocking, it follows that the combination of He and Zenchelsky in view of Ikudome's admission would have made redirection based on the same bases obvious as well." *Linksmart Wireless*, No. 2011-009566, at 10.

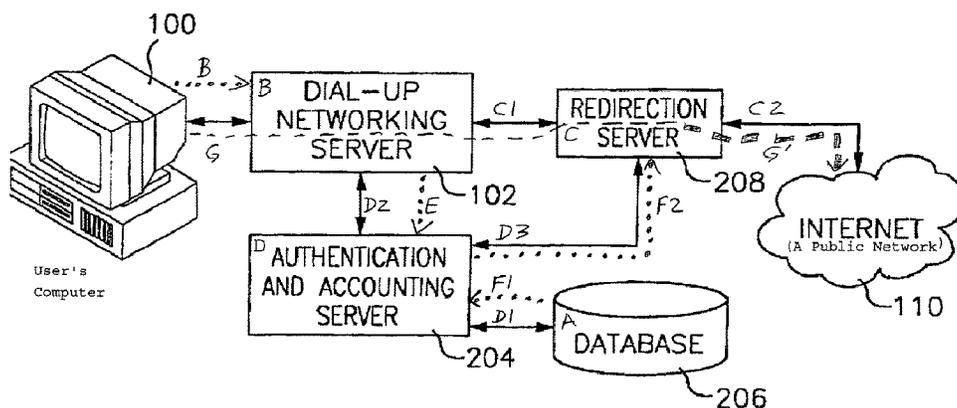
**V. THE CLAIMS OF THE '118 PATENT ARE OBVIOUS OVER WILLENS IN VIEW OF ZENCHELSKY AND THE PATENT OWNER'S ADMISSIONS, RAISING SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY**

With the above understanding of the prior art references, the following argument is presented to show that the claims of the '118 Patent are obvious under 35 U.S.C. § 103. The Appendix features claim charts showing that each limitation of the claims in this request is present in Willens when combined with Zenchelsky and the Patent Owner's admissions in the '118 Patent. Thus, Requestor has raised a substantial new question of patentability.

**A. Claims 2-7, 28, and 30-31 Are Obvious over Willens in view of Zenchelsky and the Patent Owner's Admissions**

**1. Overview of Obviousness**

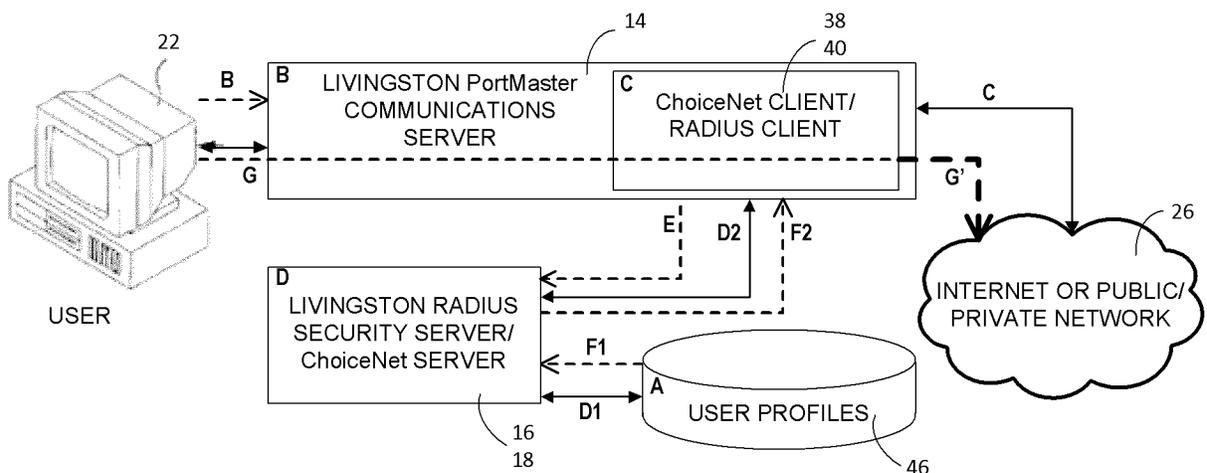
Claims 2-7, 28, and 30-31 are rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions in the Background section of the '118 Patent. Claims 2-7, 28, and 30-31 are dependent on canceled Claim 1, thus each of the claims share common elements corresponding to canceled Claim 1. Reproduced below is the Patent Owner's annotated figure 2, identifying the common elements of Claims 2-7, 28, and 30-31 (with explanatory text removed for clarity):



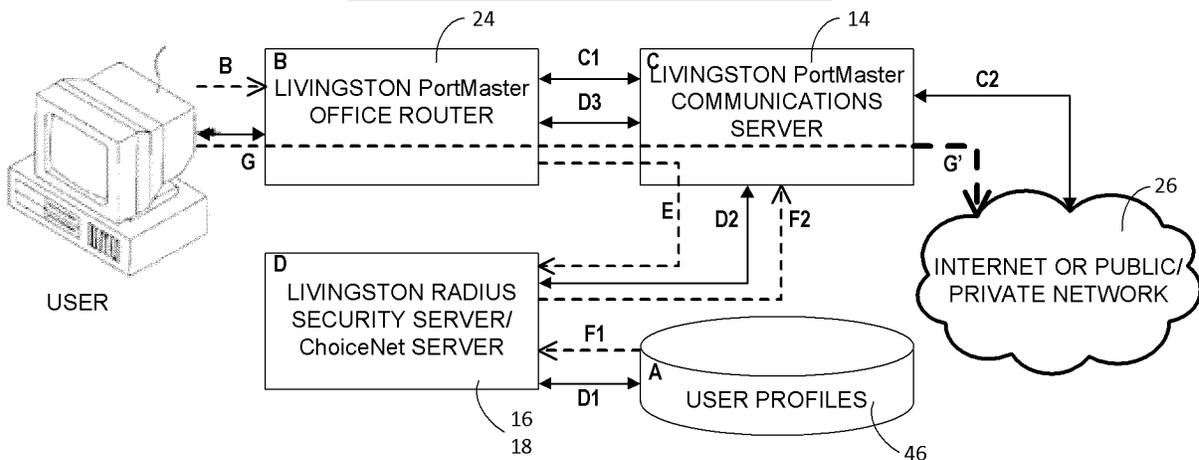
**Diagram 9 - Patent Owner's annotated Figure 2**

Diagram 10 depicts the elements taught in Willens, arranged in the form of the above Diagram 9, to demonstrate the correspondences between the claim elements and elements of the prior art reference:

**A First Embodiment of Willens**



**A Second Embodiment of Willens**



**Diagram 10 – Two embodiments of systems as taught by Willens**

Note that the solid arrows in Diagram 9 and Diagram 10 represent connections between the various components, which are all taught by Willens. The procedural signal flows are shown in dotted arrows, also taught by Willens.

Figures 1 and 3 in Willens (Diagram 11 and Diagram 12) illustrate the system as taught by Willens.

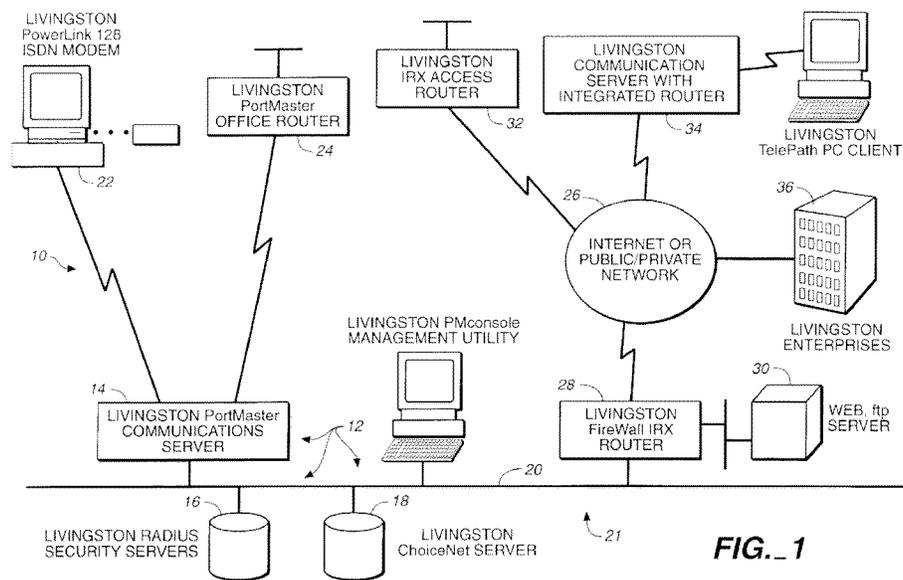


Diagram 11 – Figure 1 from Willens showing the network topology

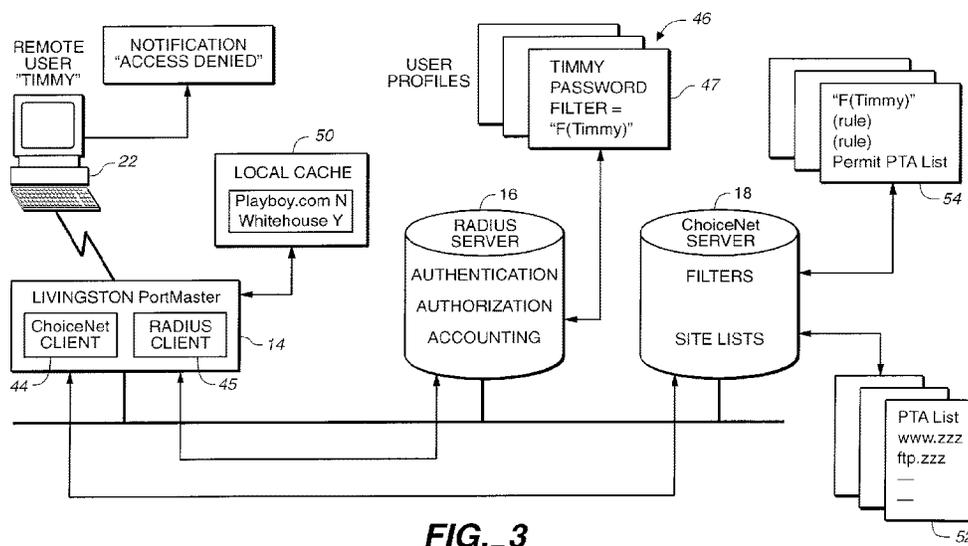
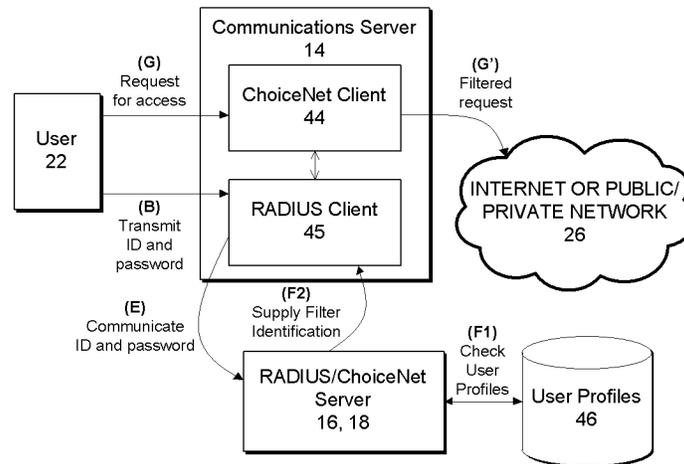


Diagram 12 – Figure 3 from Willens showing a detailed block diagram of the remote access control subsystem. For comparison, Requestor has prepared a schematic diagram, in Diagram 13, arranging the elements in Willens as illustrated in figures 1 and 3 to show that Diagram 10 in fact corresponds to elements of Willens. The letters of the steps correspond to the Patent Owner’s diagram and the solid arrows show the flow of information through the system.



Schematic Diagram of Willens

**Diagram 13 - A schematic representation of the system in Willens**

The user 22 transmits user information and a password to the communications server 14 (B). *Col. 5 ll. 9-12.* The RADIUS client 45 running on the communications server 14 communicates this information to the RADIUS server 16 (E). *Id.* The RADIUS server 16 authorizes the user 22 through the use of a database of user profiles 46 (F1). *Id.* The RADIUS server 16 supplies a filter identification to the ChoiceNet client 44 through the RADIUS client 45 (F2). *Col. 5 ll. 12-18.* The filter identification corresponds to filter rules found in the ChoiceNet client 44 or retrieved from the ChoiceNet server 18. *Col. 5 ll. 18-24.* The user 22 requests access to a network location and the ChoiceNet client 44 on the communications server 14 processes that request (G). *Col. 5 l. 60-64.* The communications server 14, through the ChoiceNet client 44, applies the filter rules and either permits or denies the requested access. (G'). *Col. 5 l. 64 to col. 6 l. 9.*

In the Prior Reexamination, the Board found Claim 1 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. Each of Claims 2-7, 28, and 30-31 add limitations to Claim 1 which, as described in more detail below, would have been obvious in view of Willens and the prior art at the time of invention, as admitted by the Patent Owner and demonstrated by Zenchelsky.

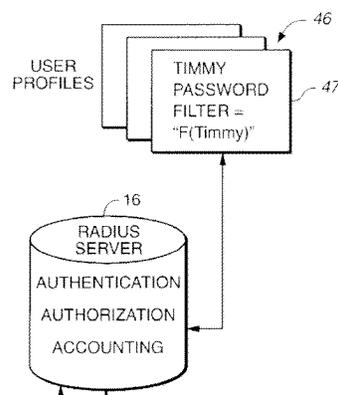
## **2. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of Willens in relation to canceled Claim 1 which forms the common elements of Claims 2-7, 28, and 30-31. Each limitation has been identified using letters (a) through (g) for ease of description and for later reference. The Appendix features claim charts of Claims 2-7, 28, and 30-31 which shows that each limitation of

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Claims 2-7, 28, and 30-31 is present in Willens when combined with Zenchelsky and the Patent Owner's admissions in the '118 Patent. In relation to the common elements of Claims 2-7, 28, and 30-31, Willens teaches or renders obvious a system comprising:

**(a) a database with entries correlating each of a plurality of user IDs with an individualized rule set:** Willens teaches "the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46." *Col. 5 ll.* 10-11. Diagram 14, included below, is taken from figure 3 in Willens and illustrates the elements from Willens that correspond to the elements in the limitation above.



**Diagram 14 – Database entries and rule sets from Willens**

The user profiles 46 stored on the RADIUS server 16 in Willens correspond to the entries in the database in the above recited limitation. In Willens, user profiles 46 are associated with a user and identify filters 47 for each user which corresponds to the above recited limitation that the database entries correlate user IDs with an individualized rule set. *See col. 5 ll.* 16-18; fig. 3. As described in the '118 Patent, the individualized rule set in the limitation includes "personalized filtering and redirection information for the particular user ID." *Col. 3 ll.* 3-4. In Willens, the filters 47 are used "for determining if a request by a user for access to a desired site in the system should be permitted." *Col. 1 ll.* 12-16. Thus, the filters 47 in the user profiles 46 from Willens correspond to the individualized rule set in the limitation above.

**(b) a dial-up network server that receives user IDs from users' computers:** Willens teaches that "users are connected to the network by dial-up connections 22 through the communications server 14 or via a local area network (LAN) router 24, also through the communications server 14." *Col. 3 ll.* 60-64. In one embodiment, the local area network router 24 in Willens corresponds to the dial-up network server in the limitation. *See fig. 1.* The dial-up

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

network server in the '118 Patent “is used to establish a communication link with the user’s PC.” *Col. 3 ll. 60-63*. Figure 1 in Willens (reproduced above in Diagram 11) shows that the local area network router 24 is used to establish a communication link between a user’s computer and the communications server 14. Furthermore, in a recent opinion construing the claims at issue in the '118 Patent, the District Court “construe[d] ‘dial-up network server’ to mean ‘a server that is used to establish a communications link with the user’s PC.’” *Linksmart Wireless Tech. v. T-Mobile USA, Inc.*, Mem. Op. and Order, No. 2:08-CV-264-DF-CE, at 13 (E.D. Tex. June 30, 2010). Thus, the local area network router 24 of Willens corresponds to the dial-up network server in the limitation because it provides the same functionality.

Alternatively, the communications server 14 can correspond to the dial-up network server in the limitation above. The communications server 14 is used to establish a network connection with the user 22. *See col. 3 ll. 60-64, fig. 1*. Following the same reasoning presented above, the communications server 14 corresponds to the dial-up network server because it connects a user to the network and is thus within the broadest possible meaning of dial-up network server.

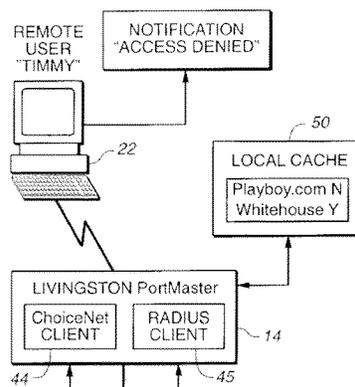
As illustrated in figure 3 from Willens (reproduced above in Diagram 12), when users log in to the communications server 14, their information is authenticated by the RADIUS server 16 which receives user IDs. *See col. 5 ll. 10-16*. In one example in Willens, “an ISP can allow users who log in with a predetermined name, such as VIPguest, access using the system and process of this invention.” *Col. 6 ll. 6-8*. Thus, in Willens the local area network router 24 and/or the communications server 14 (corresponding to the dial-up network server) receives user IDs from users’ computers to pass to the RADIUS server 16 for authentication.

***(c) a redirection server connected to the dial-up network server and a public network:*** According to figure 1 from Willens (Diagram 11 above), the communications server 14 is connected to and sits between the local area network router 24 and the Internet or public network 26. As described in relation to limitation (b), the communications server 14 in Willens corresponds to the redirection server in the limitation. In another embodiment disclosed in Willens, the communications server 14 acts as both the dial-up server (see above) and the redirection server through the ChoiceNet Client 44 running on the communications server 14. *See col. 3 ll. 60-64, col. 5 ll. 18-37*.

The communications server 14 of Willens falls within the broadest reasonable interpretation of “redirection server” as used in the claim. The redirection server in the '118

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Patent “programs the rule set and IP address so as to control (filter, block, redirect, and the like) the user’s data as a function of the rule set.” *Col. 6 ll. 1-3*. In Willens, access to the public network is “implemented with a communications server 14” which can include the ChoiceNet client software 44 (illustrated in Diagram 15 below). *Col. 3 ll. 56-57; see fig. 3*. “In practice, the client software and permit-based filtering technology is integrated in the communications operating system software that runs on the server or routers.” *Col. 5 ll. 34-37*. The communications server 14 can be configured to apply the filters associated with a particular user, to permit or deny access to data according to the filters.



**Diagram 15 - Willens' communication server 14 is a redirection server**

Therefore, Willens teaches or renders obvious a redirection server (communications server 14) connected to the dial-up network server (communications server 14 or local area network router 24) and a public network.

**(d) an authentication accounting server connected to the database, the dial-up network server and the redirection server:** Willens teaches that “[t]he access control subsystem 12 is implemented with a communications server 14, one or more Remote Authentication Dial In User Service (RADIUS) servers 16, and a remote access server 18, all connected to a network backbone 20.” *Col. 3 ll. 56-60*. In figure 3 from Willens, Diagram 12 above, the RADIUS Server 16 provides authentication, authorization, and accounting functionality. Thus, the RADIUS Server 16 in Willens corresponds to the authentication accounting server in the limitation above. In figure 1 from Willens, Diagram 11 above, the RADIUS Server 16 is connected to the communications server 14 which is connected to the local area network router 24. As described above, the RADIUS server 16 accesses user information stored on the server. Thus, Willens discloses an authentication accounting server (the RADIUS Server 16) connected to the database (stored user information on the server), the dial-up network server (the local area

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

network 24 or the communications server 14), and the redirection server (the communications server 14).

*(e) wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server:* Willens teaches that “[t]he source and destination addresses in the header packet are used to identify the user, allowing selection of the appropriate user filter, and to identify the site for which the user desires access.” *Col. 6 ll. 35-38*. In addition, Willens teaches that “[i]f multiple users are associated with a particular address node, then login information is used to determine which user filter should be applied for access requests.” *Col. 6 ll. 52-55*. These teachings demonstrate that users are associated with a particular network address else the communication and capabilities described by Willens would not be possible. Furthermore, “[w]hen user 22 logs in through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46.” *Col. 5 ll. 9-12*. Combining these teachings demonstrates that the communication between the components of the system utilizes network addresses and these network addresses are associated with a user ID. Thus, Willens teaches that the dial-up network server (the local area network 24 or the communications server 14) communicates a user ID and network address to the authentication accounting server (the RADIUS server 16).

*(f) wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server:* Willens teaches: “The user profiles 46 also identify a filter ‘F(Timmy)’ in his user profile 46. After checking user 22’s authorization, the RADIUS server 16 supplies the filter identification through the RADIUS client 45 software along with the verification acknowledgment for the user 22 for use by client software 44 for controlling access by the user 22 to Internet sites.” *Col. 5 ll. 12-18*. Willens also teaches that communication among the components in the network occurs via transmitting IP packets, which contain source and destination network addresses. *See Col. 6 ll. 10-15, 44-46*. The network addresses in the IP packet headers can be used “for the purposes of identifying user filters.” *Col. 6 ll. 44-49*. Thus, the RADIUS server 16 (corresponding to the authentication accounting server) accesses the database where the user profiles 46 are stored and communicates the filter information (corresponding to the individualized rule set) to the client software 44 on

the communications server 14 (corresponding to the redirection server). As described above, the filter information is associated with a user and a network address. Therefore, each element of the limitation recited above is taught by Willens.

*(g) wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set:* Willens teaches that “[i]n response to the user 22 request for access...the server 14 applies the filter ‘F(Timmy)’ 54 as a mask to the site list in the local cache to determine if the request will be granted.” *Col. 5 ll.* 60-64. In addition, Willens teaches that “[b]ased on the result [of searching a list of sites in the filter], the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 6 ll.* 4-7. Furthermore, Willens teaches that “[i]n practice, the client software and permit-based filtering technology is integrated in the communications operating system software that runs on the server or routers.” *Col. 5 ll.* 34-37. Thus, data directed toward the public network, such as attempts to access websites, is processed by the client software 44 on the communications server 14 (corresponding to the redirection server) according to the rules in the filters (corresponding to the individualized rule set).

**3. The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders the Common Elements of Claims 2-7, 28, and 30-31 Obvious**

Willens may not teach the following two elements of Claims 2-7, 28, and 30-31:

1. A redirection server that performs redirection as well as blocking; and
2. A dial-up network server that communicates a first user ID for one of the users’ computers and a temporarily assigned network address for the first user ID to the authentication and accounting server.

However, these differences between Willens and the common elements of Claims 2-7, 28, and 30-31 would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner’s admissions of prior art.

In regard to the first of the noted limitations, the Board has determined that it would have been obvious at the time of the invention to modify the communications server 14 of Willens to perform redirection as well as blocking. The Board stated that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Because the communications server 14 of Willens

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

can be configured as a control to block the user, it would have been obvious to alter the communication server to redirect the user as well. Thus the communications server 14 has the same functionality as the redirection server of the limitation recited above. As Diagram 15 illustrates, the client software 44 running on the communications server 14 acts to control user 22's access to the public network. Thus, the communication server in Willens corresponds to the redirection server in the limitation.

In regard to the second of the noted limitations, to the extent the examiner does not find that Willens teaches that "the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server," Willens combined with Zenchelsky and the Patent Owner admitted prior art does.

In the '118 Patent, the Patent Owner admits that in "prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server 104." *Col. 1 ll. 21-24*. Thus, by the Patent Owner's admission, this limitation was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found:

It would have been obvious to one of ordinary skill in the art to modify He et al [U.S. Patent No. 6,088,451]; so to provide temporary IP address to a user node and additionally encode communications packets with source and destination addresses as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.

Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and communicating using IP addresses and that this teaching was within the prior art as admitted by the Patent Owner in the background section of the '118 Patent.

**4. Claim 2**

In addition to common elements (a) through (g) described above, Claim 2 contains the following limitation:

*wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set:* Willens teaches that "the access control system and process is implemented using an extension of the Internet

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or drop packets to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax.” *Col. 6 ll. 10-17*. In addition, “[a]ll communications initiated by the user to sites that are on the permit list are allowed, while access to all other sites is denied by default.” *Col. 4 ll. 26-35; see also col. 5 l. 58–col. 6 l. 9* (describing the process of permitting or denying access to a user based on filter rules). Thus, Willens teaches a redirection server that provides control over a plurality of data to and from the user’s computer, *e.g.* either routing or denying IP packets, based on filter rules.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 2 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**5. Claim 3**

In addition to common elements (a) through (g) described above, Claim 3 contains the following limitation:

*wherein the redirection server further blocks the data to and from the users’ computers as a function of the individualized rule set:* Willens teaches that “[i]n response to the user 22 request for access...the server 14 applies the filter ‘F(Timmy)’...to determine if the request will be granted.... Based on the result, the server 14 either permits or denies access.... In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site.” *Col. 5 l. 58–col. 6 l. 9*. As explained above, the server 14 in Willens corresponds to the redirection server in the ’118 Patent. The server 14 in Willens blocks data to and from the users’ computers as a function of the filter “F(Timmy).” The filter and associated rules correspond to the individualized rule set, as described above. Therefore, Willens teaches a redirection server that blocks data to and from a user’s computer based on an individualized rule set.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 3 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**6. Claim 4**

In addition to common elements (a) through (g) described above, Claim 4 contains the following limitation:

*wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set:* Willens teaches that “[i]n response to the user 22 request for access...the server 14 applies the filter ‘F(Timmy)’...to determine if the request will be granted.... Based on the result, the server 14 either permits or denies access.” *Col. 5 l. 58–col. 6 l. 6*. As explained above, the server 14 in Willens corresponds to the redirection server in the ’118 Patent. The server 14 in Willens permits data to and from the users’ computers as a function of the filter “F(Timmy).” The filter and associated rules correspond to the individualized rule set, as described above. Therefore, Willens teaches a redirection server that allows data to and from a user’s computer based on an individualized rule set.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 4 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**7. Claim 5**

In addition to common elements (a) through (g) described above, Claim 5 contains the following limitation:

*wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set:* Willens teaches that a redirection server checks access requests against stored rules and “[b]ased on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 6 ll. 5-7*. As discussed in Section IV.F., the Board declared that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user” and “redirection would have been an obvious extension of blocking.” *Linksmart Wireless*, No. 2011-009566, at 9, 10. Based on the statement by the Board, it would have been obvious in view of the Patent Owner’s admissions to modify the communications server in Willens to redirect data to and from a user’s computer as a function of filter rules.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 5 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**8. Claim 6**

In addition to common elements (a) through (g) described above, Claim 6 contains the following limitation:

*wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set:* Requestor respectfully

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

submits that, given its broadest reasonable interpretation, Claim 6 encompasses at least a redirection server that redirects some data to one destination based on one rule, another destination based on another rule, and so on. As taught in Willens, filters contain one or more filter rules comprising an instruction to permit or deny access for each site listed. *See col. 5 ll. 11-12, 27-34, 60-66.* A user can request access to a site and the redirection server can check the filter rules stored locally and on a remote server, and “[b]ased on the result, the server 14 either permits or denies access.” *Col. 6 ll. 5-6.* Thus, Willens teaches a system that permits or denies access to multiple destinations. As discussed in Section IV.F., the Board stated that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the communications server of Willens to perform redirection to multiple destinations.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 6 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**9. Claim 7**

In addition to common elements (a) through (g) described above, Claim 7 contains the following limitation:

***wherein the database entries for a plurality of the plurality of users’ IDs are correlated with a common individualized rule set:*** Willens teaches that the access control system can have common rules for groups of users. For example, “[w]hen a game subscriber logs in, a user filter can be used to permit access to a game server, while allowing the ISP to deny access to non-subscribers.” *Col. 7 ll. 3-6.* Game subscribers can have a common rule set allowing access to the same game server. *See id.* Filters are stored in the RADIUS server 16 database and associate a filter with a user. *See col. 5 ll. 12-13.* Thus, Willens teaches that a plurality of user IDs can be associated with a common rule set, *e.g.*, the game subscriber filter rules.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 7 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**10. Claim 28**

In addition to common elements (a) through (g) described above, Claim 28 contains the following limitation:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service:* The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11.* Furthermore, the '118 Patent declares that “[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header.” *Col. 2 ll. 11-13.* Willens teaches “[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]” *Col. 6 ll. 16-22.* Thus, Willens teaches filter rules that block and allow based on IP services because they detect protocols and ports such as http traffic. *See id.* In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, “redirection is not limited to WWW traffic, and the concept is valid for all IP services.” *Col. 1 ll. 41-42; see Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the server in Willens to filter based on IP service.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 28 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**11. Claim 30**

In addition to common elements (a) through (g) described above, Claim 30 contains the following limitation:

*wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address:* The '118 Patent gives examples of “request type” as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36.* Therefore, the broadest reasonable interpretation of request type includes http requests. Willens teaches filters that are “an explicit set of rules based on either permit or deny syntax” and “[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]” *Col. 6 ll. 15-22.* Furthermore, “[t]he server 14 uses such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security.” *Col. 6 ll. 44-47.* Thus, Willens teaches filter rules that allow access based on a destination address and “request type,” such as http requests.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 30 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**12. Claim 31**

In addition to common elements (a) through (g) described above, Claim 31 contains the following limitation:

*wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address:* Claim 31 contains nearly identical language to Claim 30 described above, except that Claim 31 is directed to “redirecting the data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. Willens teaches permitting or denying access based on a request type and an attempted destination address, as discussed above in Section V.A.11. In the prior reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in Willens to redirect data based on a request type and destination address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 31 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**B. Claims 9-14, 32, and 34-35 Are Obvious over Willens in view of Zenchelsky and the Patent Owner’s Admissions**

**1. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of Willens in relation to canceled Claim 8 which forms the common elements of Claims 9-14, 32, and 34-35. In the Prior Reexamination, the Board found Claim 8 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. Each of Claims 9-14, 32, and 34-35 add limitations to Claim 8. As described in more detail below, these limitations would have been obvious in view of Willens and the prior art at the time of invention, as admitted by the Patent Owner and demonstrated by Zenchelsky.

The common elements of Claims 9-14, 32, and 34-35 are analogous to the common elements of Claims 2-7, 28, and 30-31, and so the common elements of Claims 9-14, 32, and 34-35 are rendered obvious by Willens in view of Zenchelsky and the Patent Owner’s admissions for analogous reasons as discussed above with respect to the common elements of Claims 2-7, 28, and 30-31 in Section V.A. In relation to the common elements of Claims 9-14, 32, and 34-35, Willens teaches or renders obvious a system comprising:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*a database with entries correlating each of a plurality of user IDs with an individualized rule set:* This language is identical to the language in the limitation identified as (a) above in Section V.A. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches “the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46.” *Col. 5 ll.* 10-11. Willens also teaches filters 47 associated with the user profiles, where the filters 47 are used “for determining if a request by a user for access to a desired site in the system should be permitted.” *Col. 1 ll.* 12-16. The user profiles 46 and filters 47 stored on the RADIUS server 16 in Willens correspond to the entries in the database which correlate user IDs with an individualized rule set. *See fig. 3.* Thus, Willens teaches a database with entries correlating user IDs with an individualized rule set.

*a dial-up network server that receives user IDs from users’ computers:* This language is identical to the language in the limitation identified as (b) above in Section V.A. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that “users are connected to the network by dial-up connections 22 through the communications server 14 or via a local area network (LAN) router 24, also through the communications server 14.” *Col. 3 ll.* 60-64. The local area network router 24 or the communications server 14 can act as the dial-up network server. *See col. 3 ll.* 60-64; *fig. 1.* As illustrated in figure 3 from Willens (reproduced above in Diagram 12), when users log in to the communications server 14, their information is authenticated by the RADIUS server 16 which therefore receives user IDs. *See col. 5 ll.* 10-18. Thus, in Willens the local area network router 24 and/or the communications server 14 receives user IDs from users’ computers. *See col. 5 ll.* 10-18; *fig. 3.*

*a redirection server connected to the dial-up network server and a public network:* This language is identical to the language in the limitation identified as (c) above in Section V.A. Thus, according to the discussion above in those sections and for analogous reasons, this limitation is taught by Willens.

According to figure 1 from Willens (Diagram 11 above), the communications server 14 is connected to and sits between the local area network router 24 and the Internet or public network 26. The communications server 14 in Willens corresponds to the redirection server in the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

limitation above because it applies the filters that block or allow network traffic. *See col. 3 ll. 56-67; col. 5 ll. 34-47; fig. 3.* The communications server 14 is connected to, and sits between, the router 24 and the public network 26, thus teaching each element of the recited limitation.

The communications server 14 of Willens falls within the broadest reasonable interpretation of “redirection server” as used in the claim. The redirection server in the ’118 Patent “programs the rule set and IP address so as to control (filter, block, redirect, and the like) the user’s data as a function of the rule set.” *Col. 6 ll. 1-3.* In Willens, access to the public network is “implemented with a communications server 14” which can include the ChoiceNet client software 44 (illustrated in Diagram 15). *Col. 3 ll. 56-57; see fig. 3.* “In practice, the client software and permit-based filtering technology is integrated in the communications operating system software that runs on the server or routers.” *Col. 5 ll. 34-37.* The communications server 14 can be configured to apply the filters associated with a particular user, to permit or deny access to data according to the filters.

In another embodiment, the communications server 14 acts as both the dial-up server (see above) and the redirection server through the ChoiceNet Client 44. *See col. 3 ll. 60-64; col. 5 ll. 18-37.* In this embodiment, traffic directed to the public network passes through the communications server 14 where it is processed by the ChoiceNet Client software 44 before continuing to the public network, if it is not blocked. Thus, the functionality of the communications server 14 when it acts as both the redirection server and the dial-up network server is the same as having the redirection server sit between the dial-up network server and the public network, as well as having it connect to both.

Therefore, Willens teaches a redirection server (the communications server 14) connected to the dial-up network server (the local area network router 24 or the communications server 14) and a public network (the Internet 26).

***an authentication accounting server connected to the database, the dial-up network server and the redirection server.*** This language is identical to the language in the limitation identified as (d) above in Section V.A. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that “[t]he access control subsystem 12 is implemented with a communications server 14, one or more Remote Authentication Dial In User Service (RADIUS) servers 16, and a remote access server 18, all connected to a network backbone 20.” *Col. 3 ll.*

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

56-60. The RADIUS Server 16 in Willens provides authentication, authorization, and accounting functionality. *See* fig. 1. Thus, the RADIUS Server 16 in Willens corresponds to the authentication accounting server in the limitation above. The RADIUS Server 16 is connected to the communications server 14 which is connected to the local area network router 24. *See id.* As described above, the RADIUS server 16 accesses user information stored on the server. Thus, Willens teaches an authentication accounting server (the RADIUS Server 16) connected to the database (stored user information on the server), the dial-up network server (the local area network 24 or the communications server 14), and the redirection server (the communications server 14).

*a method comprising the steps of: communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server:* This language is identical to the language in the limitation identified as (e) above in Section V.A. except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that communication occurs using packets that contain addresses that are associated with particular users. *See col. 6 ll. 35-38; col. 6 ll. 52-55.* Furthermore, users are authorized through communication with the RADIUS server 16. *See col. 5 ll. 9-12.* Combining these teachings demonstrates that the communication between the components of the system in Willens utilizes network addresses and these network addresses are associated with user IDs. Thus, Willens teaches that the dial-up network server (the local area network 24 or the communications server 14) communicates a user ID and network address to the authentication accounting server (the RADIUS server 16).

*communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server:* This language is identical to the language in the limitation identified as (f) above in Section V.A. except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Willens teaches: “The user profiles 46 also identify a filter ‘F(Timmy)’ in his user profile 46. After checking user 22’s authorization, the RADIUS server 16 supplies the filter identification through the RADIUS client 45 software along with the verification acknowledgment for the user 22 for use by client software 44 for controlling access by the user 22 to Internet sites.” *Col. 5 ll. 12-18*. Willens also teaches that communication among the components in the network occurs via transmitting IP packets, which contain source and destination network addresses. *See Col. 6 ll. 10-15, 44-46*. Thus, Willens teaches an authentication accounting server (the RADIUS server 16) that accesses a database and communicates the individualized rule set (the filter information 46 and 47) to the redirection server (the communications server 14) where the user ID is associated with a network address.

*processing data directed toward the public network from the one of the users’ computers according to the individualized rule set*: This language is identical to the language in the limitation identified as (g) above in Section V.A. except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that “[i]n response to the user 22 request for access...the server 14 applies the filter ‘F(Timmy)’ 54 as a mask to the site list in the local cache to determine if the request will be granted.” *Col. 5 ll. 60-64*. In addition, Willens teaches that “[b]ased on the result [of searching a list of sites in the filter], the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 6 ll. 4-7*. Thus, data directed toward the public network is processed by the communications server 14 (corresponding to the redirection server) according to the rules in the filters (corresponding to the individualized rule set).

**2. The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders the Common Elements of Claims 9-14, 32, and 34-35 Obvious**

Willens may not teach the following two elements of Claims 9-14, 32, and 34-35:

1. A redirection server that performs redirection as well as blocking; and
2. A dial-up network server that communicates a first user ID for one of the users’ computers and a temporarily assigned network address for the first user ID to the authentication and accounting server.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

For reasons analogous to those described in Section V.A.3., these differences between Willens and the common elements of Claims 9-14, 32, and 34-35 would have been obvious modifications to one of ordinary skill in the art at the time of the invention, in view of Zenchelsky and the Patent Owner's admissions of prior art.

In regard to the first of the noted limitations, the Board has determined that it would have been obvious in view of the Patent Owner's admissions to modify the communications server 14 of Willens to perform redirection as well as blocking by stating "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Thus, it would have been obvious to modify the communications server 14 of Willens to perform redirection in addition to blocking.

In regard to the second of the noted limitations, to the extent the examiner does not find that Willens teaches that "the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server," Willens combined with Zenchelsky and the Patent Owner's admissions does.

In the '118 Patent, the Patent Owner admits that in "prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server 104." *Col. 1 ll. 21-24*. Thus, by the Patent Owner's admission, this limitation was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and communicating using IP addresses and that this teaching was within the prior art as admitted by the Patent Owner in the Background section of the '118 Patent.

**3. Claim 9**

In addition to the common elements described above, Claim 9 contains the following limitation:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.* Claim 9 is analogous to Claim 2, and for reasons analogous to those described in Section V.A.4., Claim 9 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

Willens teaches that "the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or drop packets to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax." *Col. 6 ll. 10-17.* In addition, "[a]ll communications initiated by the user to sites that are on the permit list are allowed, while access to all other sites is denied by default." *Col. 4 ll. 26-35; see also col. 5 l. 58-col. 6 l. 9* (describing the process of permitting or denying access to a user based on filter rules). Thus, Willens teaches a redirection server that provides control over a plurality of data to and from the user's computer, *e.g.* either routing or denying IP packets, based on filter rules.

Therefore, Requestor respectfully submits that Claim 9 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**4. Claim 10**

In addition to the common elements described above, Claim 10 contains the following limitation:

*further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.* Claim 10 is analogous to Claim 3, and for reasons analogous to those described in Section V.A.5., Claim 10 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

Willens teaches that "[i]n response to the user 22 request for access...the server 14 applies the filter 'F(Timmy)'...to determine if the request will be granted.... Based on the result, the server 14 either permits or denies access.... In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site." *Col. 5 l. 58-col. 6 l. 9.* As explained above, the server 14 in Willens corresponds to the redirection server in the '118 Patent. The server 14 in Willens blocks data to and from the users' computers as a function of the filter "F(Timmy)." The filter and associated rules correspond to the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

individualized rule set, as described above. Therefore, Willens teaches a redirection server that blocks data to and from a user's computer based on an individualized rule set.

Therefore, Requestor respectfully submits that Claim 10 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**5. Claim 11**

In addition to the common elements described above, Claim 11 contains the following limitation:

*further including the step of allowing the data to and from the users' computers as a function of the individualized rule set:* Claim 11 is analogous to Claim 4, and for reasons analogous to those described in Section V.A.6., Claim 11 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

Willens teaches that "[i]n response to the user 22 request for access...the server 14 applies the filter 'F(Timmy)'...to determine if the request will be granted.... Based on the result, the server 14 either permits or denies access." *Col. 5 l. 58–col. 6 l. 6*. As explained above, the server 14 in Willens corresponds to the redirection server in the '118 Patent. The server 14 in Willens permits data to and from the users' computers as a function of the filter "F(Timmy)." The filter and associated rules correspond to the individualized rule set, as described above. Therefore, Willens teaches a redirection server that allows data to and from a user's computer based on an individualized rule set.

Therefore, Requestor respectfully submits that Claim 11 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**6. Claim 12**

In addition to the common elements described above, Claim 12 contains the following limitation:

*further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set:* Claim 12 is analogous to Claim 5, and for reasons analogous to those described in Section V.A.7., Claim 12 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

Willens teaches that a redirection server checks access requests against stored rules and "[b]ased on the result, the server 14 either permits or denies access and updates it's [sic] local cache 50." *Col. 6 ll. 5-7*. As discussed in Section IV.F., the Board declared that, in view of the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user" and "redirection would have been an obvious extension of blocking." *Linksmart Wireless*, No. 2011-009566, at 9, 10. Based on the statement by the Board, it would have been obvious in view of the Patent Owner's admissions to modify the communications server in Willens to redirect data to and from a user's computer as a function of filter rules.

Therefore, Requestor respectfully submits that Claim 12 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**7. Claim 13**

In addition to the common elements described above, Claim 13 contains the following limitation:

*further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.* Claim 13 is analogous to Claim 6, and for reasons analogous to those described in Section V.A.8., Claim 13 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

Requestor respectfully submits that, given its broadest reasonable interpretation, Claim 13 encompasses at least a redirection server that redirects some data to one destination based on one rule, another destination based on another rule, and so on. As taught in Willens, filters contain one or more filter rules comprising an instruction to permit or deny access for each site listed. *See col. 5 ll. 11-12, 27-34, 60-66.* A user can request access to a site and the redirection server can check the filter rules stored locally and on a remote server, and "[b]ased on the result, the server 14 either permits or denies access." *Col. 6 ll. 5-6.* Thus, Willens teaches a system that permits or denies access to multiple destinations. As discussed in Section IV.F., the Board stated that, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the communications server of Willens to perform redirection to multiple destinations.

Therefore, Requestor respectfully submits that Claim 13 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**8. Claim 14**

In addition to the common elements described above, Claim 14 contains the following limitation:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set:* Claim 14 is analogous to Claim 7, and for reasons analogous to those described in Section V.A.9., Claim 14 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

Willens teaches that the access control system can have common rules for groups of users. For example, "[w]hen a game subscriber logs in, a user filter can be used to permit access to a game server, while allowing the ISP to deny access to non-subscribers." *Col. 7 ll. 3-6*. Game subscribers can have a common rule set allowing access to the same game server. *See id.* Filters are stored in the RADIUS server 16 database and associate a filter with a user. *See col. 5 ll. 12-13*. Thus, Willens teaches that a plurality of user IDs can be associated with a common rule set, *e.g.*, the game subscriber filter rules.

Therefore, Requestor respectfully submits that Claim 14 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**9. Claim 32**

In addition to the common elements described above, Claim 32 contains the following limitation:

*wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service:* Claim 32 is analogous to Claim 28, and for reasons analogous to those described in Section V.A.10., Claim 32 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11*. Furthermore, the '118 Patent declares that "[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header." *Col. 2 ll. 11-13*. Willens teaches "[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]." *Col. 6 ll. 16-22*. Thus, Willens teaches filter rules that block and allow based on IP services because they detect protocols and ports such as http traffic. *See id.* In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, "redirection is not limited to WWW traffic, and the concept is valid for all IP services." *Col. 1 ll. 41-42; see*

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the server in Willens to filter based on IP service.

Therefore, Requestor respectfully submits that Claim 32 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**10. Claim 34**

In addition to the common elements described above, Claim 34 contains the following limitation:

*wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address:* Claim 34 is analogous to Claim 30, and for reasons analogous to those described in Section V.A.11., Claim 34 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

The '118 Patent gives examples of "request type" as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36.* Therefore, the broadest reasonable interpretation of request type includes http requests. Willens teaches filters that are "an explicit set of rules based on either permit or deny syntax" and "[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]" *Col. 6 ll. 15-22.* Furthermore, "[t]he server 14 uses such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security." *Col. 6 ll. 44-47.* Thus, Willens teaches filter rules that allow access based on a destination address and "request type," such as http requests.

Therefore, Requestor respectfully submits that Claim 34 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**11. Claim 35**

In addition to the common elements described above, Claim 35 contains the following limitation:

*wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address:* Claim 35 is analogous to Claim 31, and for reasons analogous to those described in Section V.A.12., Claim 35 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Furthermore, Claim 35 is identical to Claim 34 described above, except that Claim 35 is directed to “redirecting the data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. Willens teaches permitting or denying access based on a request type and an attempted destination address, as discussed above in Sections V.A.11. and V.B.10. In the prior reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in Willens to redirect data based on a request type and destination address.

Therefore, Requestor respectfully submits that Claim 35 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**C. Claims 16-24, 36, and 38-39 Are Obvious over Willens in view of Zenchelsky and the Patent Owner’s Admissions**

**1. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of Willens in relation to canceled Claim 15 which forms the common elements of Claims 16-24, 36, and 38-39. Each limitation has been identified using letters (a) through (d) for ease of description and for later reference. In the Prior Reexamination, the Board found Claim 15 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. Each of Claims 16-24, 36, and 38-39 add limitations to Claim 15. As described in more detail below, these limitations would have been obvious in view of Willens and the prior art at the time of invention, as admitted by the Patent Owner and demonstrated by Zenchelsky. In relation to the common elements of Claims 16-24, 36, and 38-39, Willens teaches or renders obvious a system comprising:

***(a) a redirection server programmed with a user’s rule set correlated to a temporarily assigned network address:*** Willens teaches that “the RADIUS server 16 supplies the filter identification through the RADIUS client 45 software along with the verification acknowledgement for the user 22 for use by client software 44.” *Col. 5 ll.* 10-18. Additionally, “the client software 44 and permit-based filtering technology is integrated in the communications operating system software that runs on the server 14 or routers 24, 32, or 34.” *Col. 5 ll.* 34-47. Thus, the client software 44 integrated into the communications server 14 is programmed with filter rules based on the filter identification sent from the RADIUS server 16. Therefore, Willens teaches a redirection server programmed with a user’s rule set.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Willens teaches that “[t]he source and destination addresses in the header packet are used to identify the user, allowing selection of the appropriate user filter, and to identify the site for which the user desires access.” *Col. 6 ll. 35-38*. In addition, Willens teaches that “[i]f multiple users are associated with a particular address node, then login information is used to determine which user filter should be applied for access requests.” *Col. 6 ll. 52-55*. These teachings demonstrate that users’ rule sets are correlated with a particular network address; else the communication and capabilities described by Willens would not be possible.

***(b) wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network:*** Willens teaches:

“the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or drop packets to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. The firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]”

*Col. 6 ll. 10-20*. The communications server 14 of Willens contains a plurality of functions to control data passing between the user and a public network, i.e., the server 14 can permit or deny access requests or route or drop network packets passing between source and destination addresses. *See id*. The decision to permit or deny access is based on rules contained in filters. *See id; col. 6 ll. 5-9*. Thus, Willens teaches or renders obvious each element in the above limitation.

***(c) wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address:*** Willens teaches “[t]he server software also automatically maintains the permit list by downloading updated versions of the list over the Internet and compiling the list for use by the client software [44]. As a result of this self maintenance [sic] capability, the [remote access control] server 18 requires minimal administrative attention.” *Col. 5 ll. 41-46*. “[C]ontinuously updated versions of the permit list that reside on the server 18” can be provided. *Col. 5 ll. 55-57*. Furthermore, Willens teaches that “said network access server automatically maintains and compiles said list of permitted sites” and filters stored in local cache are “automatically updated based on said access determination.” *Col. 7 ll. 65-67; col. 8 ll. 39-42*. Thus, Willens teaches that at least a

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

portion of the filter rules implemented in the client software 44 can be updated through an automated process. As described above, Willens teaches that the rule set is correlated to a network address. *See col. 6 ll. 35-38, 52-55.*

*(d) wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses:* Willens teaches “controlling access by a user to sites based on the nature of their content.” *Col. 6 ll. 66-67.* Willens also teaches that a rule set can be modified based on a location the user accesses. *See col. 5 l. 64-col. 6 l. 7.* Thus, Willens teaches a communications server 14 (the redirection server) configured to allow automated modification of a rule set stored in its local cache as a function of data transmitted to or from the user or location the user accesses. Furthermore, the Board stated that “blocking a website based on these bases [time, data, or location] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Therefore, Willens teaches or renders obvious the above limitation.

**2. The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders the Common Elements of Claims 16-24, 36, and 38-39 Obvious**

Willens may not teach the following two elements of Claims 16-24, 36, and 38-39:

1. A redirection server that performs redirection as well as blocking; and
2. A user’s rule set correlated to a temporarily assigned network address.

However, these differences between Willens and the claims would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner’s admissions of prior art.

In regard to the first of the noted limitations, the Board has determined that, in view of the Patent Owner’s admissions, it would have been obvious to modify the communications server 14 of Willens to perform redirection as well as blocking by stating “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

009566, at 9. Thus, it would have been obvious to modify the communications server 14 of Willens to perform redirection in addition to blocking.

In regard to the second of the noted limitations, to the extent the examiner does not find that Willens teaches “a user’s rule set correlated to a temporarily assigned network address,” Willens combined with Zenchelsky and the Patent Owner’s admissions does.

In the ’118 Patent, the Patent Owner admits that in “prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP’s authentication and accounting server 104.” *Col. 1 ll. 21-24*. Additionally, the Patent Owner admits that “the end user would be identified by the temporarily assigned IP address.” *Col. 1 ll. 35-37*. Thus, by the Patent Owner’s admission, identifying a user with a temporarily assigned IP address was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and identifying a user with the temporary IP address and that this teaching was within the prior art as admitted by the Patent Owner in the background section of the ’118 Patent. Thus, Willens, in view of Zenchelsky and the Patent Owner’s Admissions, renders obvious a user’s rule set correlated to a temporarily assigned network address.

**3. Claim 16**

In addition to common elements (a) through (d) described above, Claim 16 contains the following limitation:

***wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time:*** Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of “modification” of a portion of a rule set because updating a rule set can change or modify a rule.

As taught in Willens, the access control system 12 (which includes the communication server 14) “provides for a central, server based permit list that can be easily updated on a daily or hourly basis.” *Col. 4 ll. 40-45*. Willens also teaches a “list of permitted sites being

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

automatically maintained by periodically downloading updated versions of said list over the Internet.” *Col. 10 ll. 60-62*. Thus, Willens teaches a communications server 14 (corresponding to the redirection server) that can update rules as a function of time. Furthermore, the Board stated that “blocking a website based on these bases [as a function of time, data sent or received, or location accessed] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, the Board stated it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Based on the statements by the Board, it would have been obvious to modify the server in Willens to be configured to allow portions of rule sets to be modified as a function of time.

Therefore, in view of the discussion above, Requestor respectfully submits that Claims 16 and 19 are obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**4. Claim 17**

In addition to common elements (a) through (d) described above, Claim 17 contains the following limitation:

***wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user:*** Similar to Claim 16 above, Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of “modification” of a portion of a rule set because updating a rule set can change or modify a rule. Willens teaches that filter rules and site lists can be updated at various times. *See col. 4 ll. 40-45; col. 10 ll. 60-62*. As taught in Willens, the communications server 14 can be configured to “control[] access by a user to sites based on the nature of their content.” *Col. 6 ll. 66-67*. Thus, Willens teaches a redirection server responsive to data transmitted to or from the user. Moreover, as stated above regarding Claim 16, the Board declared that modifying rule sets based on data transmitted to or from the user would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the server in Willens to allow modification of rules as a function of data the user sends or receives.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 17 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**5. Claim 18**

In addition to common elements (a) through (d) described above, Claim 18 contains the following limitation:

*wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses:* Similar to Claim 16, Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of “modification” of a portion of a rule set because updating a rule set can change or modify a rule. Willens teaches that filter rules and site lists can be updated at various times. *See col. 4 ll. 40-45; col. 10 ll. 60-62.* As taught in Willens, a redirection server can perform a rule look-up when a user attempts to access a particular location. “This look-up contains the list name ‘PTA List’ and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 5 l. 64–col. 6 l. 7.* As described, the rule set stored in the local cache 50 on the communications server 14 is modified, including possibly removing or reinstating rules, based on the location a user tries to access. *See id.* Moreover, as stated above regarding Claim 16, the Board declared that modifying rule sets based on the location or locations the user accesses would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the server in Willens to allow modification of rules as a function of locations the user attempts to access.

Therefore, in view of the discussion above, Requestor respectfully submits that Claims 18 and 21 are obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**6. Claim 19**

In addition to common elements (a) through (d) described above, Claim 19 contains the following limitation:

*wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time:* The difference between Claim 16 and Claim 19 is that the limitation in Claim 16 states a portion of the rule set can be modified as a function of time and the limitation in Claim 19 states a portion of the rule set can be removed or reinstated as a function of time. Thus, the difference between Claims 16 and 19 is a change from “modification” to “removal or reinstatement.” Requestor respectfully submits that updating a

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

portion of a rule set falls within the broadest reasonable interpretation of “removal or reinstatement” of a portion of a rule set because updating a rule set can remove or reinstate a rule.

As taught in Willens, the access control system 12 (which includes the communication server 14) “provides for a central, server based permit list that can be easily updated on a daily or hourly basis.” *Col. 4 ll. 40-45*. Willens also teaches a “list of permitted sites being automatically maintained by periodically downloading updated versions of said list over the Internet.” *Col. 10 ll. 60-62*. Thus, Willens teaches a communications server 14 (corresponding to the redirection server) that can update rules as a function of time. Furthermore, the Board stated that “blocking a website based on these bases [as a function of time, data sent or received, or location accessed] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, the Board stated it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Based on the statements by the Board, it would have been obvious to modify the server in Willens to be configured to allow portions of rule sets to be removed or reinstated as a function of time.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 19 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**7. Claim 20**

In addition to common elements (a) through (d) described above, Claim 20 contains the following limitation:

***wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user:*** Similar to Claims 16 and 19 above, the difference between Claims 17 and 20 is the change of the word “modification” to the words “removal or reinstatement.” Willens teaches that filter rules and site lists can be updated at various times. *See col. 4 ll. 40-45; col. 10 ll. 60-62*. As taught in Willens, the communications server 14 can be configured to “control[] access by a user to sites based on the nature of their content.” *Col. 6 ll. 66-67*. Thus, Willens teaches a redirection server responsive to data transmitted to or from the user. Moreover, as stated above regarding Claim 16, the Board declared that modifying rule sets based on data transmitted to or from the user

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the server in Willens to allow removal or reinstatement of rules as a function of data the user sends or receives.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 20 are obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**8. Claim 21**

In addition to common elements (a) through (d) described above, Claim 21 contains the following limitation:

*wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses:*

Similar to Claims 16 and 19 above, Claims 18 and 21 differ only in the change of the word "modification" to the words "removal or reinstatement." Willens teaches that filter rules and site lists can be updated at various times. *See col. 4 ll. 40-45; col. 10 ll. 60-62.* As taught in Willens, a redirection server can perform a rule look-up when a user attempts to access a particular location. "This look-up contains the list name 'PTA List' and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it's [sic] local cache 50." *Col. 5 l. 64-col. 6 l. 7.* As described, the rule set stored in the local cache 50 on the communications server 14 is modified, including possibly removing or reinstating rules, based on the location a user tries to access. *See id.* Moreover, as stated above regarding Claim 16, the Board declared that modifying rule sets based on the location or locations the user accesses would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the server in Willens to allow removal or reinstatement of rules as a function of locations the user attempts to access.

Therefore, in view of the discussion above, Requestor respectfully submits that Claims 18 and 21 are obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**9. Claim 22**

In addition to common elements (a) through (d) described above, Claim 22 contains the following limitation:

*wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or*

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*from the user, or location or locations the user accesses*: Willens teaches “controlling access by a user to sites based on the nature of their content.” *Col. 6 ll. 66-67*. Willens also teaches that a rule set can be modified based on a location the user accesses: “the [communications] server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the [remote access control] server 18.... The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 5 l. 64–col. 6 l. 7*. Thus, Willens teaches a communications server 14 (the redirection server) configured to allow automated modification of a rule set stored in its local cache as a function of data transmitted to or from the user or location the user accesses. Furthermore, the Board stated that “blocking a website based on these bases [time, data, or location] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the server in Willens to allow the modification, removal, or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 22 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**10. Claim 23**

In addition to common elements (a) through (d) described above, Claim 23 contains the following limitation:

*wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server*: As taught in figure 1 in Willens, reproduced above as Diagram 11, a redirection server 14 is connected to a user through a modem 22 on a user side and the Internet or Public/Private network 26 on a network side. *See also* figs. 4, 5 (illustrating similar configurations of users, redirection servers, and computer networks). Willens teaches that the access control subsystem 12 (which includes the communications server 14) “provides a centralized way to operate content monitoring using the very communications servers and routers that users’ traffic travels *through* to get to the Internet.” *Col. 4 ll. 37-40* (emphasis added). Thus, to access the computer network, the user computer connects through the communications server 14. As described above in Sections V.A.2. and V.A.3., Willens in

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

combination with Zenchelsky and the Patent Owner's admissions renders obvious a user computer using a temporarily assigned network address. It would have been obvious to modify the computer in Willens to be associated with a temporary network address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 23 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**11. Claim 24**

Claim 24 depends from Claim 23:

*The system of claim 23 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server:* As taught in Willens, the redirection server (communications server 14) can update its rule set based on information received from a remote server 18 situated on the computer network side of the communications server 14 in figure 1 (Diagram 11). *See col. 5 l. 64-col. 6 l. 7; col. 4 ll. 40-45; fig. 1.* Thus, Willens teaches a redirection server receiving instructions to modify a rule set from its computer network side.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 24 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**12. Claim 36**

In addition to common elements (a) through (d) described above, Claim 36 contains the following limitation:

*wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service:* The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11.* Furthermore, the '118 Patent declares that "[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header." *Col. 2 ll. 11-13.* Willens teaches "[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]." *Col. 6 ll. 16-22.* Thus, Willens teaches filter rules that block and allow based on IP services because they detect protocols and ports such as http traffic. *See id.* In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, "redirection is not limited to WWW traffic, and the concept is valid for all IP services." *Col. 1 ll. 41-42; see Linksmart Wireless, No. 2011-009566, at 8, fn.24.* Accordingly, it would have been obvious to modify the server in Willens to filter based on IP service.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 36 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**13. Claim 38**

In addition to common elements (a) through (d) described above, Claim 38 contains the following limitation:

*wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address:* Claim 38 is analogous to Claim 30, and for reasons analogous to those described in Section V.A.11., Claim 38 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

The '118 Patent gives examples of "request type" as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36.* Therefore, the broadest reasonable interpretation of request type includes http requests. Willens teaches filters that are "an explicit set of rules based on either permit or deny syntax" and "[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]." *Col. 6 ll. 15-22.* Furthermore, "[t]he server 14 uses such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security." *Col. 6 ll. 44-47.* Thus, Willens teaches filter rules that allow access based on a destination address and "request type," such as http requests.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 38 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**14. Claim 39**

In addition to common elements (a) through (d) described above, Claim 39 contains the following limitation:

*wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address:* Claim 39 is analogous to Claim 31, and for reasons analogous to those described in Section V.A.12., Claim 39 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

Furthermore, Claim 39 is identical to the Claim 38 described above, except that Claim 39 is directed to "redirecting the data to a new destination address" instead of "allowing access" based on a request type and an attempted destination address. Willens teaches permitting or

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

denying access based on a request type and destination address, as discussed above in Sections V.A.11., V.B.10., and V.C.13. In the prior reexamination, the Board declared, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in Willens to redirect data based on a request type and destination address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 39 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**D. Claims 26-27, 40, and 42-43 Are Obvious over Willens in view of Zenchelsky and the Patent Owner's Admissions**

**1. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of Willens in relation to canceled Claim 25 which forms the common elements of Claims 26-27, 40, and 42-43. In the Prior Reexamination, the Board found Claim 25 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. Each of Claims 26-27, 40, and 42-43 add limitations to Claim 25. As described in more detail below, these limitations would have been obvious in view of Willens and the prior art at the time of invention, as admitted by the Patent Owner and demonstrated by Zenchelsky. The Appendix features claim charts of Claims 26-27, 40, and 42-43 which shows that each limitation is present in Willens when combined with Zenchelsky and the Patent Owner's admissions in the '118 Patent. In relation to the common elements of Claims 26-27, 40, and 42-43, Willens teaches or renders obvious a system comprising:

***a redirection server containing a user's rule set correlated to a temporarily assigned network address:*** This limitation is nearly identical to the limitation in the common elements of Claims 16-24, 36, and 38-39 identified as (a) in Section V.C.1., the difference between the two being one minor change in the language. Limitation (a) in the common elements of Claims 16-24, 36, and 38-39 states "the redirection server *programmed* with a user's rule set" and the limitation here states "the redirection server *containing* a user's rule set." Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that "the RADIUS server 16 supplies the filter identification through the RADIUS client 45 software along with the verification acknowledgement for the user 22 for use by client software 44." *Col. 5 ll.* 10-18. Additionally, "the client software 44 and permit-based filtering technology is integrated in the communications operating system software that runs on

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

the server 14 or routers 24, 32, or 34.” *Col. 5 ll. 34-47*. Thus, the client software 44 integrated into the communications server 14 is programmed with filter rules based on the filter identification sent from the RADIUS server 16. Therefore, Willens teaches a redirection server containing a user’s rule set.

Willens teaches that “[t]he source and destination addresses in the header packet are used to identify the user, allowing selection of the appropriate user filter, and to identify the site for which the user desires access.” *Col. 6 ll. 35-38*. In addition, Willens teaches that “[i]f multiple users are associated with a particular address node, then login information is used to determine which user filter should be applied for access requests.” *Col. 6 ll. 52-55*. These teachings demonstrate that users’ rule sets are correlated with a particular network address; else the communication and capabilities described by Willens would not be possible.

***wherein the user’s rule set contains at least one of a plurality of functions used to control data passing between the user and a public network:*** This language is identical to the language in the limitation in the common elements of Claims 16-24, 36, and 38-39 identified as (b) in Section V.C.1. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that the control access system uses IP firewall packet filtering in the communications server 14 which connects user 22 to the public network 26. *Col. 6 ll. 10-20*. The filter rules implemented on server 14 contain a plurality of functions because traffic is either permitted or denied access based on filter rules. *See id; col. 6 ll. 5-9*. Thus, Willens teaches or renders obvious a user rule set with a plurality of functions used to control data passing between the user and a public network.

***the method comprising the step of: modifying at least a portion of the user’s rule set while the user’s rule set remains correlated to the temporarily assigned network address in the redirection server:*** This limitation is analogous to the limitation identified as (c) in the common elements of Claims 16-24, 36, and 38-39 in Section V.C.1., except that the form of the limitation has been changed to be a step in a method rather than functionality in a system. Thus, according to the discussion above and for analogous reasons, this limitation is taught or rendered obvious by Willens.

Willens teaches “[t]he server software also automatically maintains the permit list by downloading updated versions of the list over the Internet and compiling the list for use by the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

client software [44]. As a result of this self maintenance [sic] capability, the [remote access control] server 18 requires minimal administrative attention.” *Col. 5 ll. 41-46*. “[C]ontinuously updated versions of the permit list that reside on the server 18” can be provided. *Col. 5 ll. 55-57*. Furthermore, Willens teaches that “said network access server automatically maintains and compiles said list of permitted sites” and filters stored in local cache are “automatically updated based on said access determination.” *Col. 7 ll. 65-67; col. 8 ll. 39-42*. Thus, Willens teaches that at least a portion of the filter rules implemented in the client software 44 can be updated through an automated process. As described above, Willens teaches that the rule set is correlated to a network address and nowhere does it state that modification of the rule set alters the correlated network address. *See col. 6 ll. 35-38, 52-55*.

*wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server:* This limitation corresponds to the limitation in Claim 23, discussed above in Section V.C.10. Thus, according to the discussion above and for analogous reasons, this limitation is taught or rendered obvious by Willens.

As taught in figure 1 in Willens, reproduced above as Diagram 11, a redirection server 14 is connected to a user through a modem 22 on a user side and the Internet or Public/Private network 26 on a network side. *See also* figs. 4, 5 (illustrating similar configurations of users, redirection servers, and computer networks). Willens teaches that the access control subsystem 12 (which includes the communications server 14) “provides a centralized way to operate content monitoring using the very communications servers and routers that users’ traffic travels *through* to get to the Internet.” *Col. 4 ll. 37-40* (emphasis added). Thus, to access the computer network, the user computer connects through the communications server 14. As described above in Sections V.A.2. and V.A.3., Willens in combination with Zenchelsky and the Patent Owner’s admissions renders obvious a user computer using a temporarily assigned network address. It would have been obvious to modify the computer in Willens to be associated with a temporary network address.

*and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user’s rule set through one or more of the user side of the redirection server and the network side of the redirection server:* This limitation is

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

analogous to the limitation in Claim 24, discussed above in Section V.C.11., except that the form of the limitation has been changed to be a step in a method rather than functionality in a system. Thus, according to the discussion above and for analogous reasons, this limitation is taught or rendered obvious by Willens.

As taught in Willens, the redirection server (communications server 14) can update its rule set based on information received from a remote server 18 situated on the computer network side of the communications server 14 in figure 1 (Diagram 11 above). *See col. 5 l. 64-col. 6 l. 7; col. 4 ll. 40-45; fig. 1.* Thus, Willens teaches a redirection server receiving instructions to modify a rule set from its computer network side.

**2. The Combination of Willens, Zenchelsky, and the Patent Owner's Admissions Renders the Common Elements of Claims 26-27, 40, and 42-43 Obvious**

Willens may not teach the following two elements of Claims 26-27, 40, and 42-43:

1. A redirection server that performs redirection as well as blocking; and
2. A user's rule set correlated to a temporarily assigned network address.

For reasons analogous to those described in Section V.C.2., these differences between Willens and the common elements of Claims 26-27, 40, and 42-43 would have been obvious modifications to one of ordinary skill in the art at the time of the invention, in view of Zenchelsky and the Patent Owner's admissions of prior art.

In regard to the first of the noted limitations, the Board has determined that it would have been obvious, in view of the Patent Owner's admissions, to modify the communications server 14 of Willens to perform redirection as well as blocking by stating "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Thus, it would have been obvious to modify the communications server 14 of Willens to perform redirection in addition to blocking.

In regard to the second of the noted limitations, to the extent the examiner does not find that Willens teaches "a user's rule set correlated to a temporarily assigned network address," Willens combined with Zenchelsky and the Patent Owner's admissions does.

In the '118 Patent, the Patent Owner admits that in "prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server 104."

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*Col. 1 ll. 21-24.* Additionally, the Patent Owner admits that “the end user would be identified by the temporarily assigned IP address.” *Col. 1 ll. 35-37.* Thus, by the Patent Owner’s admission, identifying a user with a temporarily assigned IP address was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and identifying a user with the temporary IP address and that this teaching was within the prior art as admitted by the Patent Owner in the background section of the ’118 Patent. Thus, Willens, in view of Zenchelsky and the Patent Owner’s Admissions, renders obvious a user’s rule set correlated to a temporarily assigned network address.

**3. Claim 26**

In addition to the common elements described above, Claim 26 contains the following limitation:

*further including the step of modifying at least a portion of the user’s rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses:* Claim 26 is analogous to Claim 22, and for reasons analogous to those described in Section V.C.9., Claim 26 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

Willens teaches “controlling access by a user to sites based on the nature of their content.” *Col. 6 ll. 66-67.* Willens also teaches that a rule set can be modified based on a location the user accesses: “the [communications] server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the [remote access control] server 18.... The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 5 l. 64–col. 6 l. 7.* Thus, Willens teaches a communications server 14 (the redirection server) configured to allow automated modification of a rule set stored in its local cache as a function of data transmitted to or from the user or location the user accesses. Furthermore, the Board stated that “blocking a website based on these bases [time, data, or

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

location] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the server in Willens to allow the modification of rules based on some combination of time, data transmitted or received, or locations accessed.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 26 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**4. Claim 27**

In addition to the common elements described above, Claim 27 contains the following limitation:

*further including the step of removing or reinstating at least a portion of the user’s rule set as a function of one or more of: time, the data transmitted to or from the user and the location or locations the user accesses:* Claim 27 is analogous to Claim 22, and for reasons analogous to those described in Section V.C.9., Claim 27 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

Willens teaches “controlling access by a user to sites based on the nature of their content.” *Col. 6 ll. 66-67*. Willens also teaches that a rule set can be modified based on a location the user accesses: “the [communications] server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the [remote access control] server 18.... The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 5 l. 64–col. 6 l. 7*. Thus, Willens teaches a communications server 14 (the redirection server) configured to allow automated modification of a rule set stored in its local cache as a function of data transmitted to or from the user or location the user accesses. Furthermore, the Board stated that “blocking a website based on these bases [time, data, or location] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the server in Willens to allow the removal or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 27 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**5. Claim 40**

In addition to the common elements described above, Claim 40 contains the following limitation:

*wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service:* Claim 40 is analogous to Claim 28, and for reasons analogous to those described in Section V.A.10., Claim 40 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11*. Furthermore, the '118 Patent declares that "[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header." *Col. 2 ll. 11-13*. Willens teaches "[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]." *Col. 6 ll. 16-22*. Thus, Willens teaches filter rules that block and allow based on IP services because they detect protocols and ports such as http traffic. *See id.* In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, "redirection is not limited to WWW traffic, and the concept is valid for all IP services." *Col. 1 ll. 41-42; see Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the server in Willens to filter based on IP service.

Therefore, Requestor respectfully submits that Claim 40 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**6. Claim 42**

In addition to the common elements described above, Claim 42 contains the following limitation:

*wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address:* Claim 42 is analogous to Claim 30, and for reasons analogous to those described in Section V.A.11., Claim 42 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

The '118 Patent gives examples of "request type" as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36*. Therefore, the broadest reasonable interpretation of request type includes http requests. Willens teaches filters that are "an explicit set of rules based on either permit or deny syntax" and "[t]he firewall filtering of server 14

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.].” *Col. 6 ll. 15-22*. Furthermore, “[t]he server 14 uses such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security.” *Col. 6 ll. 44-47*. Thus, Willens teaches filter rules that allow access based on a destination address and “request type,” such as http requests.

Therefore, Requestor respectfully submits that Claim 42 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**7. Claim 43**

In addition to the common elements described above, Claim 43 contains the following limitation:

*wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address:* Claim 43 is analogous to Claim 31, and for reasons analogous to those described in Section V.A.12., Claim 43 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

Furthermore, Claim 43 is identical to Claim 42 described above, except that Claim 43 is directed to “redirecting the data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. Willens teaches permitting or denying access based on a request type and an attempted destination address, as discussed above in Sections V.A.11., V.B.10., V.C.13., and V.D.6. In the prior reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in Willens to redirect data based on a request type and destination address.

Therefore, Requestor respectfully submits that Claim 43 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**E. Claim 44 Is Obvious over Willens in View of Zenchelsky and the Patent Owner’s Admissions**

**1. Overview of Obviousness**

Claim 44 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner’s admissions in the Background section of the ’118 Patent. In the Prior Reexamination, the Board

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

found Claim 1 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. The Patent Owner stated that Claim 44 corresponds to Claim 1 with language to clarify the “‘between’ location of the redirection server.” Response and Proposed Amendment, at 3. The only difference between canceled Claim 1 and Claim 44 is Claim 1 recites “a redirection server connected *to* the dial-up network server and a public network” (emphasis added), and Claim 44 recites “a redirection server connected *between* the dial-up network server and a public network” (emphasis added). Willens teaches a network topology having a redirection server situated logically between a dial-up network server and a public network, as described below and shown in Diagram 13.

**2. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of Willens in relation to Claim 44. Each limitation has been identified using letters (a) through (g) for ease of description. The Appendix features claim charts of Claim 44 and shows that each limitation of Claim 44 is present in Willens when combined with Zenchelsky and the Patent Owner’s admissions in the ’118 Patent. In relation to Claims 44, Willens teaches or renders obvious a system comprising:

***(a) a database with entries correlating each of a plurality of user IDs with an individualized rule set:*** Willens teaches “the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46.” *Col. 5 ll.* 10-11. Willens also teaches filters 47 associated with the user profiles, where the filters 47 are used “for determining if a request by a user for access to a desired site in the system should be permitted.” *Col. 1 ll.* 12-16. The user profiles 46 and filters 47 stored on the RADIUS server 16 in Willens correspond to the entries in the database which correlate user IDs with an individualized rule set. *See* fig. 3. Thus, Willens teaches a database with entries correlating user IDs with an individualized rule set.

***(b) a dial-up network server that receives user IDs from users’ computers:*** Willens teaches that “users are connected to the network by dial-up connections 22 through the communications server 14 or via a local area network (LAN) router 24, also through the communications server 14.” *Col. 3 ll.* 60-64. The local area network router 24 or the communications server 14 can act as the dial-up network server. *See col. 3 ll.* 60-64; fig. 1. As illustrated in figure 3 from Willens (reproduced in Diagram 12), when users log in to the communications server 14, their information is authenticated by the RADIUS server 16 which therefore receives user IDs. *See col. 5 ll.* 10-18. Thus, in Willens the local area network router

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

24 and/or the communications server 14 receives user IDs from users' computers. *See col. 5 ll. 10-18; fig. 3.*

**(c) a redirection server connected between the dial-up network server and a public network:** According to figure 1 from Willens (Diagram 11), the communications server 14 is connected to and sits between the local area network router 24 and the Internet or public network 26. Claim 44 differs from canceled Claim 1 and the common elements of Claims 2-7 and 28-31 in that the network topology was changed to specify that the redirection server sits *between* the dial-up network server and a public network rather than merely connected *to* the dial-up network server and a public network. Willens teaches both network topologies. The communications server 14 in Willens corresponds to the redirection server in the limitation above because it applies the filters that block or allow network traffic. *See col. 3 ll. 56-67; col. 5 ll. 34-47; fig. 3.* The communications server 14 is connected to, and sits between, the router 24 and the public network 26, thus teaching each element of the recited limitation.

The communications server 14 of Willens falls within the broadest reasonable interpretation of "redirection server" as used in the claim. The redirection server in the '118 Patent "programs the rule set and IP address so as to control (filter, block, redirect, and the like) the user's data as a function of the rule set." *Col. 6 ll. 1-3.* In Willens, access to the public network is "implemented with a communications server 14" which can include the ChoiceNet client software 44 (illustrated in Diagram 15). *Col. 3 ll. 56-57; see fig. 3.* "In practice, the client software and permit-based filtering technology is integrated in the communications operating system software that runs on the server or routers." *Col. 5 ll. 34-37.* The communications server 14 can be configured to apply the filters associated with a particular user, to permit or deny access to data according to the filters.

In another embodiment, the communications server 14 acts as both the dial-up server (see above) and the redirection server through the ChoiceNet Client 44. *See col. 3 ll. 60-64; col. 5 ll. 18-37.* In this embodiment, traffic directed to the public network passes through the communications server 14 where it is processed by the ChoiceNet Client software 44 before continuing to the public network, if it is not blocked. Thus, the functionality of the communications server 14 when it acts as both the redirection server and the dial-up network server is the same as having the redirection server sit between the dial-up network server and the public network, as well as having it connect to both.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Therefore, Willens teaches a redirection server (the communications server 14) connected *between* the dial-up network server (the local area network router 24 or the communications server 14) and a public network (the Internet 26).

***(d) an authentication accounting server connected to the database, the dial-up network server and the redirection server:*** Willens teaches that “[t]he access control subsystem 12 is implemented with a communications server 14, one or more Remote Authentication Dial In User Service (RADIUS) servers 16, and a remote access server 18, all connected to a network backbone 20.” *Col. 3 ll. 56-60*. The RADIUS Server 16 in Willens provides authentication, authorization, and accounting functionality. *See fig. 1*. Thus, the RADIUS Server 16 in Willens corresponds to the authentication accounting server in the limitation above. The RADIUS Server 16 is connected to the communications server 14 which is connected to the local area network router 24. *See id.* As described above, the RADIUS server 16 accesses user information stored on the server. Thus, Willens teaches an authentication accounting server (the RADIUS Server 16) connected to the database (stored user information on the server), the dial-up network server (the local area network 24 or the communications server 14), and the redirection server (the communications server 14).

***(e) wherein the dial-up network server communicates a first user ID for one of the users’ computers and a temporarily assigned network address for the first user ID to the authentication accounting server:*** Willens teaches that communication occurs using packets that contain addresses that are associated with particular users. *See col. 6 ll. 35-38; col. 6 ll. 52-55*. Furthermore, users are authorized through communication with the RADIUS server 16. *See col. 5 ll. 9-12*. Combining these teachings demonstrates that the communication between the components of the system in Willens utilizes network addresses and these network addresses are associated with user IDs. Thus, Willens teaches that the dial-up network server (the local area network 24 or the communications server 14) communicates a user ID and network address to the authentication accounting server (the RADIUS server 16).

***(f) wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server:*** Willens teaches: “The user profiles 46 also identify a filter ‘F(Timmy)’ in his user profile 46. After checking user 22’s authorization, the RADIUS server 16 supplies the filter identification through the RADIUS client

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

45 software along with the verification acknowledgment for the user 22 for use by client software 44 for controlling access by the user 22 to Internet sites.” *Col. 5 ll. 12-18*. Willens also teaches that communication among the components in the network occurs via transmitting IP packets, which contain source and destination network addresses. *See Col. 6 ll. 10-15, 44-46*. Thus, Willens teaches an authentication accounting server (the RADIUS server 16) that accesses a database and communicates the individualized rule set (the filter information 46 and 47) to the redirection server (the communications server 14) where the user ID is associated with a network address.

*(g) wherein data directed toward the public network from the one of the users’ computers are processed by the redirection server according to the individualized rule set:* Willens teaches that “[i]n response to the user 22 request for access...the server 14 applies the filter ‘F(Timmy)’ 54 as a mask to the site list in the local cache to determine if the request will be granted.” *Col. 5 ll. 60-64*. In addition, Willens teaches that “[b]ased on the result [of searching a list of sites in the filter], the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 6 ll. 4-7*. Thus, data directed toward the public network is processed by the communications server 14 (corresponding to the redirection server) according to the rules in the filters (corresponding to the individualized rule set).

**3. The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 44 Obvious**

Willens may not teach the following two elements of Claim 44:

1. A redirection server that performs redirection as well as blocking; and
2. A dial-up network server that communicates a first user ID for one of the users’ computers and a temporarily assigned network address for the first user ID to the authentication and accounting server.

However, these differences between Willens and Claim 44 would have been obvious modifications to one of ordinary skill in the art at the time of the invention, in view of Zenchelsky and the Patent Owner’s admissions of prior art.

In regard to the first of the noted limitations, the Board has determined that it would have been obvious, in view of the Patent Owner’s admissions, to modify the communications server 14 of Willens to perform redirection as well as blocking by stating “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Thus, it would have been obvious to modify the communications server 14 of Willens to perform redirection in addition to blocking.

In regard to the second of the noted limitations, to the extent the examiner does not find that Willens teaches that “the dial-up network server communicates a first user ID for one of the users’ computers and a temporarily assigned network address for the first user ID to the authentication accounting server,” Willens combined with Zenchelsky and the Patent Owner’s admissions does.

In the ’118 Patent, the Patent Owner admits that in “prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP’s authentication and accounting server 104.” *Col. 1 ll. 21-24*. Thus, by the Patent Owner’s admission, this limitation was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and communicating using IP addresses and that this teaching was within the prior art as admitted by the Patent Owner in the Background section of the ’118 Patent.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 44 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions.

**F. Claim 56 Is Obvious over Willens in view of Zenchelsky and the Patent Owner’s Admissions**

**1. Detailed Explanation of Obviousness**

Claim 56 is an independent claim that is identical to canceled Claim 8 in the ’118 Patent except that the limitation in the preamble related to the location of the redirection server has been changed to specify that it is *between* a dial-up network server and a public network rather than merely connected to the server and network. This change is identical to the change made between canceled Claim 1 and Claim 44, discussed above in Section V.A.1. Moreover, Claim 56 includes limitations analogous to those in Claim 44, and so Claim 56 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner’s admissions for analogous reasons as

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

discussed above with respect to Claim 44 in Section V.A. In relation to Claim 56, Willens teaches or renders obvious a system comprising:

***a database with entries correlating each of a plurality of user IDs with an individualized rule set.*** This language is identical to the language in the limitation identified as (a) above in Sections V.A. and V.E. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches “the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46.” *Col. 5 ll. 10-11.* Willens also teaches filters 47 associated with the user profiles, where the filters 47 are used “for determining if a request by a user for access to a desired site in the system should be permitted.” *Col. 1 ll. 12-16.* The user profiles 46 and filters 47 stored on the RADIUS server 16 in Willens correspond to the entries in the database which correlate user IDs with an individualized rule set. *See fig. 3.* Therefore, Willens teaches a database with entries correlating user IDs with an individualized rule set.

***a dial-up network server that receives user IDs from users’ computers.*** This language is identical to the language in the limitation identified as (b) above in Sections V.A. and V.E. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that “users are connected to the network by dial-up connections 22 through the communications server 14 or via a local area network (LAN) router 24, also through the communications server 14.” *Col. 3 ll. 60-64.* The local area network router 24 or the communications server 14 can act as the dial-up network server. *See col. 3 ll. 60-64; fig. 1.* As illustrated in figure 3 from Willens (reproduced in Diagram 12), when users log in to the communications server 14, their information is authenticated by the RADIUS server 16 which therefore receives user IDs. *See col. 5 ll. 10-18.* Therefore, in Willens the local area network router 24 and/or the communications server 14 receives user IDs from users’ computers. *See col. 5 ll. 10-18; fig. 3.*

***a redirection server connected between the dial-up network server and a public network.*** This language is identical to the language in the limitation identified as (c) above in Section V.E. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

According to figure 1 from Willens (Diagram 11), the communications server 14 is connected to and sits between the local area network router 24 and the Internet or public network 26. The communications server 14 in Willens corresponds to the redirection server in the limitation above because it applies the filters that block or allow network traffic. *See col. 3 ll. 56-67; col. 5 ll. 34-47; fig. 3.* The communications server 14 is connected to, and sits between, the router 24 and the public network 26, thus teaching each element of the recited limitation.

The communications server 14 of Willens falls within the broadest reasonable interpretation of “redirection server” as used in the claim. In another embodiment, the communications server 14 acts as both the dial-up server and the redirection server through the ChoiceNet Client 44. *See col. 3 ll. 60-64; col. 5. ll. 18-37.* In this embodiment, traffic directed to the public network passes through the communications server 14 where it is processed by the ChoiceNet Client software 44 before continuing to the public network, if it is not blocked. Thus, the functionality of the communications server 14 when it acts as both the redirection server and the dial-up network server is the same as having the redirection server sit between the dial-up network server and the public network, as well as having it connect to both.

Therefore, Willens teaches a redirection server (the communications server 14) connected *between* the dial-up network server (the local area network router 24 or the communications server 14) and a public network (the Internet 26).

***an authentication accounting server connected to the database, the dial-up network server and the redirection server:*** This language is identical to the language in the limitation identified as (d) above in Sections V.A. and V.E. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that “[t]he access control subsystem 12 is implemented with a communications server 14, one or more Remote Authentication Dial In User Service (RADIUS) servers 16, and a remote access server 18, all connected to a network backbone 20.” *Col. 3 ll. 56-60.* The RADIUS Server 16 in Willens provides authentication, authorization, and accounting functionality. *See fig. 1.* Thus, the RADIUS Server 16 in Willens corresponds to the authentication accounting server in the limitation above. The RADIUS Server 16 is connected to the communications server 14 which is connected to the local area network router 24. *See id.* As described above, the RADIUS server 16 accesses user information stored on the server. Thus, Willens teaches an authentication accounting server (the RADIUS Server 16) connected to the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

database (stored user information on the server), the dial-up network server (the local area network 24 or the communications server 14), and the redirection server (the communications server 14).

*a method comprising the steps of: communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server:* This language is identical to the language in the limitation identified as (e) above in Sections V.A. and V.E. except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that communication occurs using packets that contain addresses that are associated with particular users. *See col. 6 ll. 35-38; col. 6 ll. 52-55.* Furthermore, users are authorized through communication with the RADIUS server 16. *See col. 5 ll. 9-12.* Combining these teachings demonstrates that the communication between the components of the system in Willens utilizes network addresses and these network addresses are associated with user IDs. Thus, Willens teaches that the dial-up network server (the local area network 24 or the communications server 14) communicates a user ID and network address to the authentication accounting server (the RADIUS server 16).

*communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server:* This language is identical to the language in the limitation identified as (f) above in Sections V.A. and V.E. except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches: "The user profiles 46 also identify a filter 'F(Timmy)' in his user profile 46. After checking user 22's authorization, the RADIUS server 16 supplies the filter identification through the RADIUS client 45 software along with the verification acknowledgment for the user 22 for use by client software 44 for controlling access by the user 22 to Internet sites." *Col. 5 ll. 12-18.* Willens also teaches that communication among the components in the network occurs via transmitting IP packets, which contain source and

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

destination network addresses. *See Col. 6 ll. 10-15, 44-46.* Therefore, Willens teaches an authentication accounting server (the RADIUS server 16) that accesses a database and communicates the individualized rule set (the filter information 46 and 47) to the redirection server (the communications server 14) where the user ID is associated with a network address.

*processing data directed toward the public network from the one of the users' computers according to the individualized rule set:* This language is identical to the language in the limitation identified as (g) above in Sections V.A. and V.E. except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that “[i]n response to the user 22 request for access...the server 14 applies the filter ‘F(Timmy)’ 54 as a mask to the site list in the local cache to determine if the request will be granted.” *Col. 5 ll. 60-64.* In addition, Willens teaches that “[b]ased on the result [of searching a list of sites in the filter], the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 6 ll. 4-7.* Therefore, data directed toward the public network is processed by the communications server 14 (corresponding to the redirection server) according to the rules in the filters (corresponding to the individualized rule set).

**2. The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 56 Obvious**

Willens may not teach the following two elements of Claim 56:

1. A redirection server that performs redirection as well as blocking; and
2. A dial-up network server that communicates a first user ID for one of the users’ computers and a temporarily assigned network address for the first user ID to the authentication and accounting server.

For reasons analogous to those described in Section V.E.3., these differences between Willens and Claim 56 would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner’s admissions of prior art.

In regard to the first of the noted limitations, the Board has determined that it would have been obvious, in view of the Patent Owner’s admissions, to modify the communications server 14 of Willens to perform redirection as well as blocking by stating “redirection is an obvious

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Thus, it would have been obvious to modify the communications server 14 of Willens to perform redirection in addition to blocking.

In regard to the second of the noted limitations, to the extent the examiner does not find that Willens teaches that “the dial-up network server communicates a first user ID for one of the users’ computers and a temporarily assigned network address for the first user ID to the authentication accounting server,” Willens combined with Zenchelsky and the Patent Owner’s admissions does.

In the ’118 Patent, the Patent Owner admits that in “prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP’s authentication and accounting server 104.” *Col. 1 ll. 21-24*. Thus, by the Patent Owner’s admission, this limitation was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and communicating using IP addresses and that this teaching was within the prior art as admitted by the Patent Owner in the Background section of the ’118 Patent.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 56 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**G. Claim 68 Is Obvious over Willens in view of Zenchelsky and the Patent Owner’s Admissions**

**1. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of Willens in relation to Claim 68. Claim 68 is identical to canceled Claim 15 except that the location of the redirection server is specified with the addition of the following language: “a redirection server connected between a user computer and a public network.” In the Prior Reexamination, the Board found Claim 15 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. The added limitation, specifying the location of the redirection server, is taught by Willens, as illustrated in Diagram 11. Each

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

limitation has been identified using letters (a) through (d) for ease of description and for later reference. In relation to Claim 68, Willens teaches or renders obvious a system comprising:

***(a) a redirection server connected between a user computer and a public network, the redirection server programmed with a user's rule set correlated to a temporarily assigned network address:*** Willens teaches that “the RADIUS server 16 supplies the filter identification through the RADIUS client 45 software along with the verification acknowledgement for the user 22 for use by client software 44.” *Col. 5 ll.* 10-18. Additionally, “the client software 44 and permit-based filtering technology is integrated in the communications operating system software that runs on the server 14 or routers 24, 32, or 34.” *Col. 5 ll.* 34-47. Thus, the client software 44 integrated into the communications server 14 is programmed with filter rules based on the filter identification sent from the RADIUS server 16. Therefore, Willens teaches a redirection server programmed with a user's rule set.

Willens also teaches a communications server 14 connected between a user computer 22 and a public network 26. *See col. 3 ll.* 56-64; fig. 1. The communications server 14 filters network traffic and acts as the redirection server. *See col. 5 ll.* 34-37. Thus, Willens teaches a redirection server connected between a user computer and a public network.

Willens teaches that “[t]he source and destination addresses in the header packet are used to identify the user, allowing selection of the appropriate user filter, and to identify the site for which the user desires access.” *Col. 6 ll.* 35-38. In addition, Willens teaches that “[i]f multiple users are associated with a particular address node, then login information is used to determine which user filter should be applied for access requests.” *Col. 6 ll.* 52-55. These teachings demonstrate that users' rule sets are correlated with a particular network address; else the communication and capabilities described by Willens would not be possible.

***(b) wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network:*** Willens teaches:

“the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or drop packets to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. The firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]”

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*Col. 6 ll. 10-20.* The communications server 14 of Willens contains a plurality of functions to control data passing between the user and a public network, i.e., the server 14 can permit or deny access requests or route or drop network packets passing between source and destination addresses. *See id.* The decision to permit or deny access is based on rules contained in filters. *See id; col. 6 ll. 5-9.* Thus, Willens teaches or renders obvious each element in the above limitation.

***(c) wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address:*** Willens teaches “[t]he server software also automatically maintains the permit list by downloading updated versions of the list over the Internet and compiling the list for use by the client software [44]. As a result of this self maintenance [sic] capability, the [remote access control] server 18 requires minimal administrative attention.” *Col. 5 ll. 41-46.* “[C]ontinuously updated versions of the permit list that reside on the server 18” can be provided. *Col. 5 ll. 55-57.* Furthermore, Willens teaches that “said network access server automatically maintains and compiles said list of permitted sites” and filters stored in local cache are “automatically updated based on said access determination.” *Col. 7 ll. 65-67; col. 8 ll. 39-42.* Thus, Willens teaches that at least a portion of the filter rules implemented in the client software 44 can be updated through an automated process. As described above, Willens teaches that the rule set is correlated to a network address. *See col. 6 ll. 35-38, 52-55.*

***(d) wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses:*** Willens teaches “controlling access by a user to sites based on the nature of their content.” *Col. 6 ll. 66-67.* Willens also teaches that a rule set can be modified based on a location the user accesses: “the [communications] server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the [remote access control] server 18.... The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 5 l. 64-col. 6 l. 7.* Thus, Willens teaches a communications server 14 (the redirection server) configured to allow automated modification of a rule set stored in its local cache as a function of data transmitted to or from the user or location the user accesses. Furthermore, the Board stated that “blocking a website based on these bases

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

[time, data, or location] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Therefore, Willens teaches or renders obvious the above limitation.

**2. The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 68 Obvious**

Willens may not teach the following two elements of Claim 68:

1. A redirection server that performs redirection as well as blocking; and
2. A user’s rule set correlated to a temporarily assigned network address.

However, these differences between Willens and the claims would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner’s admissions of prior art.

In regard to the first of the noted limitations, the Board has determined that it would have been obvious, in view of the Patent Owner’s admissions, to modify the communications server 14 of Willens to perform redirection as well as blocking by stating “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Thus, it would have been obvious to modify the communications server 14 of Willens to perform redirection in addition to blocking.

In regard to the second of the noted limitations, to the extent the examiner does not find that Willens teaches “a user’s rule set correlated to a temporarily assigned network address,” Willens combined with Zenchelsky and the Patent Owner’s admissions does.

In the ’118 Patent, the Patent Owner admits that in “prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP’s authentication and accounting server 104.” *Col. 1 ll. 21-24*. Additionally, the Patent Owner admits that “the end user would be identified by the temporarily assigned IP address.” *Col. 1 ll. 35-37*. Thus, by the Patent Owner’s admission, identifying a user with a temporarily assigned IP address was known in the prior art at the time of the invention.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and identifying a user with the temporary IP address and that this teaching was within the prior art as admitted by the Patent Owner in the background section of the '118 Patent. Thus, Willens, in view of Zenchelsky and the Patent Owner's Admissions, renders obvious a user's rule set correlated to a temporarily assigned network address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 68 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**H. Claim 83 Is Obvious over Willens in View of Zenchelsky and the Patent Owner's Admissions**

**1. Detailed Explanation of Obviousness**

The combination of Willens, Zenchelsky, and the Patent Owner's admissions renders independent Claim 83 obvious. Claim 83 is identical to canceled Claim 25 in the '118 Patent except that the limitation related to the location of the redirection server has been changed to specify that it is *between* a dial-up network server and a public network. This change is identical to the change made between canceled Claim 1 and Claim 44, discussed above in Section V.E.1. Claim 83 is an independent claim that includes limitations analogous to those in Claims 68, 76, and 77. Therefore, Claim 83 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions for reasons analogous to those discussed above with respect to Claim 68 in Section V.G. and below in Claims 76 and 77 in Sections V.I.28., and V.I.29., respectively. For ease of description, the limitations below are identified using the letters (a) through (e). In relation to Claim 83, Willens teaches or renders obvious a system comprising:

***(a) a redirection server connected between a user computer and a public network, the redirection server containing a user's rule set correlated to a temporarily assigned network address:*** This language is identical to the language in the limitation in Claim 68 identified as (a) in Section V.G.1., except for one non-substantive change in the language. Claim 68 states "the redirection server *programmed* with a user's rule set" and Claim 83 states "the redirection server

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*containing* a user's rule set." Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches that "the RADIUS server 16 supplies the filter identification through the RADIUS client 45 software along with the verification acknowledgement for the user 22 for use by client software 44." *Col. 5 ll.* 10-18. Additionally, "the client software 44 and permit-based filtering technology is integrated in the communications operating system software that runs on the server 14 or routers 24, 32, or 34." *Col. 5 ll.* 34-47. Thus, the client software 44 integrated into the communications server 14 is programmed with filter rules based on the filter identification sent from the RADIUS server 16. Therefore, Willens teaches a redirection server containing a user's rule set.

Willens also teaches a communications server 14 connected between a user computer 22 and a public network 26. *See col. 3 ll.* 56-64; fig. 1. The communications server 14 filters network traffic and acts as the redirection server. *See col. 5 ll.* 34-37. Therefore, Willens teaches a redirection server connected between a user computer and a public network.

Willens teaches that "[t]he source and destination addresses in the header packet are used to identify the user, allowing selection of the appropriate user filter, and to identify the site for which the user desires access." *Col. 6 ll.* 35-38. In addition, Willens teaches that "[i]f multiple users are associated with a particular address node, then login information is used to determine which user filter should be applied for access requests." *Col. 6 ll.* 52-55. These teachings demonstrate that users' rule sets are correlated with a particular network address; else the communication and capabilities described by Willens would not be possible.

***(b) wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network:*** This language is identical to the language in the limitation in Claim 68 identified as (b) in Section V.G.1. Thus, according to the discussion above and for analogous reasons, this limitation is taught by Willens.

Willens teaches:

"the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or drop packets to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. The firewall filtering of server 14 provides bidirectional (input/output) packet filtering for

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]”

*Col. 6 ll. 10-20.* The communications server 14 of Willens contains a plurality of functions to control data passing between the user and a public network, i.e., the server 14 can permit or deny access requests or route or drop network packets passing between source and destination addresses. *See id.* The decision to permit or deny access is based on rules contained in filters. *See id; col. 6 ll. 5-9.* Therefore, Willens teaches or renders obvious each element in the above limitation.

***(c) the method comprising the step of: modifying at least a portion of the user’s rule set while the user’s rule set remains correlated to the temporarily assigned network address in the redirection server:*** This limitation is analogous to the limitation in Claim 68 identified as (c) in Section V.G.1. except that the form of the limitation has been changed to be a step in a method rather than functionality in a system. Thus, according to the discussion above and for analogous reasons, this limitation is taught or rendered obvious by Willens.

Willens teaches “[t]he server software also automatically maintains the permit list by downloading updated versions of the list over the Internet and compiling the list for use by the client software [44]. As a result of this self maintenance [sic] capability, the [remote access control] server 18 requires minimal administrative attention.” *Col. 5 ll. 41-46.* “[C]ontinuously updated versions of the permit list that reside on the server 18” can be provided. *Col. 5 ll. 55-57.* Furthermore, Willens teaches that “said network access server automatically maintains and compiles said list of permitted sites” and filters stored in local cache are “automatically updated based on said access determination.” *Col. 7 ll. 65-67; col. 8 ll. 39-42.* Thus, Willens teaches that at least a portion of the filter rules implemented in the client software 44 can be updated through an automated process. As described above, Willens teaches that the rule set is correlated to a network address and nowhere does it state that modification of the rule set alters the correlated network address. *See col. 6 ll. 35-38, 52-55.*

***(d) wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network, and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server:*** This language is identical to the language in the limitation in Claim 76, discussed below in Section V.I.28. As taught in

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

figure 1 in Willens, reproduced above as Diagram 11, a redirection server 14 is connected to a user through a modem 22 on a user side and the Internet or Public/Private network 26 on a network side. *See also* figs. 4, 5 (illustrating similar configurations of users, redirection servers, and computer networks). Willens teaches that the access control subsystem 12 (which includes the communications server 14) “provides a centralized way to operate content monitoring using the very communications servers and routers that users’ traffic travels *through* to get to the Internet.” *Col. 4 ll. 37-40* (emphasis added). Thus, to access the computer network, the user computer connects through the communications server 14. As described above in Sections V.C.2. and V.G.2., Willens in combination with Zenchelsky and the Patent Owner’s admissions renders obvious a user computer using a temporarily assigned network address. It would have been obvious to modify the computer in Willens to be associated with a temporary network address. Therefore, Willens renders obvious each element of this limitation.

*(e) and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user’s rule set through one or more of the user side of the redirection server and the network side of the redirection server.* This limitation is analogous to the limitation in Claim 77, discussed in Section V.I.29., except that the form of the limitation has been changed to be a step in a method rather than functionality in a system. As taught in Willens, the redirection server (communications server 14) can update its rule set based on information received from a remote server 18 situated on the computer network side of the communications server 14 in figure 1 (Diagram 11). *See col. 5 l. 64-col. 6 l. 7; col. 4 ll. 40-45; fig. 1.* Thus, Willens teaches a redirection server receiving instructions to modify a rule set from its computer network side. Therefore, Willens teaches or renders obvious all the above limitations.

**2. The Combination of Willens, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 83 Obvious**

Willens may not teach the following two elements of Claim 83:

1. A redirection server that performs redirection as well as blocking; and
2. A user’s rule set correlated to a temporarily assigned network address.

However, these differences between Willens and the claims would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner’s admissions of prior art.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

In regard to the first of the noted limitations, the Board has determined that it would have been obvious, in view of the Patent Owner's admissions, to modify the communications server 14 of Willens to perform redirection as well as blocking by stating "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Thus, it would have been obvious to modify the communications server 14 of Willens to perform redirection in addition to blocking.

In regard to the second of the noted limitations, to the extent the examiner does not find that Willens teaches "a user's rule set correlated to a temporarily assigned network address," Willens combined with Zenchelsky and the Patent Owner's admissions does.

In the '118 Patent, the Patent Owner admits that in "prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server 104." *Col. 1 ll. 21-24*. Additionally, the Patent Owner admits that "the end user would be identified by the temporarily assigned IP address." *Col. 1 ll. 35-37*. Thus, by the Patent Owner's admission, identifying a user with a temporarily assigned IP address was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and identifying a user with the temporary IP address and that this teaching was within the prior art as admitted by the Patent Owner in the background section of the '118 Patent. Thus, Willens, in view of Zenchelsky and the Patent Owner's Admissions, renders obvious a user's rule set correlated to a temporarily assigned network address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 83 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions.

**I. Claims 45-51, 53-55, 57-63, 65-67, 69-78, 80-82, 84-86, and 88-90 are Obvious over Willens in View of Zenchelsky and the Patent Owner's Admissions**

**1. Claim 45**

Claim 45 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 45 recites:

45. The system of claim 44, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.

Claim 45 corresponds to Claim 2, discussed in Section V.A.4., and is rendered obvious for analogous reasons. As Willens taught, "the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or drop packets to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax." *Col. 6 ll. 10-17*. In addition, "[a]ll communications initiated by the user to sites that are on the permit list are allowed, while access to all other sites is denied by default." *Col. 4 ll. 26-35; see also col. 5 l. 58—col. 6 l. 9* (describing the process of permitting or denying access to a user based on filter rules). Thus, Willens teaches a redirection server that provides control over a plurality of data to and from the user's computer, *e.g.* either routing or denying IP packets, based on filter rules. Therefore, Willens teaches all the limitations of Claim 45.

**2. Claim 46**

Claim 46 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 46 recites:

46. The system of claim 44, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.

Claim 46 corresponds to Claim 3, discussed in Section V.A.5, and is rendered obvious for analogous reasons. As Willens taught, a communications server 14 checks access requests against stored rules and "[b]ased on the result, the server 14 either permits or denies access and updates it's [sic] local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site." *Col. 6 ll. 5-9*. Thus,

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Willens teaches a communications server that blocks and allows data as a function of filter rules. Therefore, Willens teaches the limitations in Claim 46.

**3. Claim 47**

Claim 47 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 47 recites:

47. The system of claim 44, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.

Claim 47 corresponds to Claim 4, discussed in Section V.A.6., and is rendered obvious for analogous reasons. As Willens taught, a communications server 14 checks access requests against stored rules and "[b]ased on the result, the server 14 either permits or denies access and updates it's [sic] local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site." *Col. 6 ll. 5-9*. Thus, Willens teaches a communications server that allows data as a function of filter rules. Therefore, Willens teaches the limitations in Claim 47.

**4. Claim 48**

Claim 48 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 48 recites:

48. The system of claim 44, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.

Claim 48 corresponds to Claim 5, discussed in Section V.A.7., and is rendered obvious for analogous reasons. As Willens taught, a redirection server checks access requests against stored rules and "[b]ased on the result, the server 14 either permits or denies access and updates it's [sic] local cache 50." *Col. 6 ll. 5-7*. As discussed in Section IV.F., the Board declared that, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user" and "redirection would have been an obvious extension of blocking." *Linksmart Wireless*, No. 2011-009566, at 9, 10. Based on the statement by the Board, it would have been obvious to modify the communications server in Willens to redirect data to and from a user's computer as a function of filter rules. Therefore, Willens renders obvious all the limitations of Claim 48.

**5. Claim 49**

Claim 49 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 49 recites:

49. The system of claim 44, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.

Claim 49 corresponds to Claim 6, discussed in Section V.A.8., and is rendered obvious for analogous reasons. Requestor respectfully submits that, given its broadest reasonable interpretation, Claim 49 encompasses at least a redirection server that redirects some data to one destination based on one rule, another destination based on another rule, and so on. As taught in Willens, filters contain one or more filter rules comprising an instruction to permit or deny access for each site listed. *See col. 5 ll. 11-12, 27-34, 60-66.* A user can request access to a site and the redirection server can check the filter rules stored locally and on a remote server, and "[b]ased on the result, the server 14 either permits or denies access." *Col. 6 ll. 5-6.* Thus, Willens teaches a system that permits or denies access to multiple destinations. As discussed in Section IV.F., the Board stated that, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the communications server of Willens to perform redirection to multiple destinations. Therefore, Willens renders obvious Claim 49.

**6. Claim 50**

Claim 50 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 50 recites:

50. The system of claim 44, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.

Claim 50 corresponds to Claim 7, discussed in Section V.A.9., and is rendered obvious for analogous reasons. Willens teaches that the access control system can have common rules for groups of users. For example, "[w]hen a game subscriber logs in, a user filter can be used to permit access to a game server, while allowing the ISP to deny access to non-subscribers." *Col. 7 ll. 3-6.* Game subscribers can have a common rule set allowing access to the same game server. *See id.* Filters are stored in the RADIUS server 16 database and associate a filter with a user. *See col. 5 ll. 12-13.* Thus, Willens teaches that a plurality of user IDs can be associated

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

with a common rule set, *e.g.*, the game subscriber filter rules. Therefore, Willens teaches all the limitations of Claim 50.

**7. Claim 51**

Claim 51 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 51 recites:

51. The system of claim 44, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

Claim 51 corresponds to Claim 28, discussed in Section V.A.10., and is rendered obvious for analogous reasons. The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11*. Furthermore, the '118 Patent declares that “[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header.” *Col. 2 ll. 11-13*. Willens teaches “[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]” *Col. 6 ll. 16-22*. Thus, Willens teaches filter rules that block and allow based on IP services because they detect protocols and ports such as http traffic. *See id.* In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, “redirection is not limited to WWW traffic, and the concept is valid for all IP services.” *Col. 1 ll. 41-42; see Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the server in Willens to filter based on IP service. Therefore, Willens teaches or renders obvious each limitation in Claim 51.

**8. Claim 53**

Claim 53 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 53 recites:

53. The system of claim 44, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

Claim 53 corresponds to Claim 30, discussed in Section V.A.11., and is rendered obvious for analogous reasons. The '118 Patent gives examples of “request type” as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36*. Therefore, the broadest reasonable interpretation of request type includes http requests. Willens teaches filters that are “an explicit set of rules based on either permit or deny syntax” and “[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.].” *Col. 6 ll. 15-22.* Furthermore, “[t]he server 14 uses such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security.” *Col. 6 ll. 44-47.* Thus, Willens teaches filter rules that allow access based on a destination address and “request type,” such as http requests. Therefore, Willens teaches every limitation in Claim 53.

**9. Claim 54**

Claim 54 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 54 recites:

54. The system of claim 44, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 54 corresponds to Claim 31, discussed in Section V.A.12., and is rendered obvious for analogous reasons. Furthermore, Claim 54 is identical to Claim 53 described above, except that Claim 54 is directed to “redirecting the data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. Willens teaches permitting or denying access based on a request type and destination address, as discussed above in Section V.I.8. In the Prior Reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in Willens to redirect data based on a request type and destination address. Therefore, Willens renders obvious Claim 54.

**10. Claim 55**

Claim 55 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 55 recites:

55. The system of claim 44, wherein the redirection server is configured to redirect data from the users’ computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

Claim 55 contains language that is identical to the language in canceled Claim 32, whose rejection based on obviousness was affirmed by the Board in the Prior Reexamination. *Linksmart Wireless*, No. 2011-009566, at 10. Willens teaches a communications server which “provides bidirectional (input/output) packet filtering for source and destination addresses, for

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

protocol [TCP, UDP, IP, IPX], and port [http, etc.]" *Col. 6 ll.* 16-22. The redirection server in Willens utilizes IP packets and "such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security." *Col. 6 ll.* 44-49. Thus, Willens teaches a redirection server that extracts destination address information from IP packet headers to permit or deny a request for access. As the Board stated, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the server in Willens to perform redirection by replacing a first destination address in an IP packet header by a second destination address according to filter rules. Therefore, Claim 55 is rendered obvious by Willens.

**11. Claim 57**

Claim 57 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 57 recites:

57. The method of claim 56, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.

Claim 57 corresponds to Claim 9, discussed in Section V.B.3., and is rendered obvious for analogous reasons. As Willens taught, "the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or drop packets to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax." *Col. 6 ll.* 10-17. In addition, "[a]ll communications initiated by the user to sites that are on the permit list are allowed, while access to all other sites is denied by default." *Col. 4 ll.* 26-35; *see also col. 5 l.* 58–*col. 6 l.* 9 (describing the process of permitting or denying access to a user based on filter rules). Thus, Willens teaches a redirection server that provides control over a plurality of data to and from the user's computer, *e.g.* either routing or denying IP packets, based on filter rules. Therefore, Willens teaches all the limitations of Claim 57.

**12. Claim 58**

Claim 58 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 58 recites:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

58. The method of claim 56, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.

Claim 58 corresponds to Claim 10, discussed in Section V.B.4., and is rendered obvious for analogous reasons. As Willens taught, a communications server 14 checks access requests against stored rules and “[b]ased on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site.” *Col. 6 ll. 5-9*. Thus, Willens teaches a communications server that blocks and allows data as a function of filter rules. Therefore, Willens teaches the limitations in Claim 58.

**13. Claim 59**

Claim 59 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 59 recites:

59. The method of claim 56, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.

Claim 59 corresponds to Claim 11, discussed in Section V.B.5., and is rendered obvious for analogous reasons. As Willens taught, a communications server 14 checks access requests against stored rules and “[b]ased on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site.” *Col. 6 ll. 5-9*. Thus, Willens teaches a communications server that blocks and allows data as a function of filter rules. Therefore, Willens teaches the limitations in Claim 59.

**14. Claim 60**

Claim 60 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 60 recites:

60. The method of claim 56, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.

Claim 60 corresponds to Claim 12, discussed in Section V.B.6., and is rendered obvious for analogous reasons. As Willens taught, a redirection server checks access requests against stored rules and “[b]ased on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 6 ll. 5-7*. As discussed in Section IV.F., the Board declared that, in view of the Patent Owner's admissions, “redirection is an obvious extension of the use of a

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

control to block the user” and “redirection would have been an obvious extension of blocking.” *Linksmart Wireless*, No. 2011-009566, at 9, 10. Based on the statement by the Board, it would have been obvious to modify the communications server in Willens to redirect data to and from a user’s computer as a function of filter rules. Therefore, Willens renders obvious all the limitations of Claim 60.

**15. Claim 61**

Claim 61 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 61 recites:

61. The method of claim 56, further including the step of redirecting the data from the users’ computers to multiple destinations a function of the individualized rule set.

Claim 61 corresponds to Claim 13, discussed in Section V.B.7., and is rendered obvious for analogous reasons. Requestor respectfully submits that, given its broadest reasonable interpretation, Claim 61 encompass at least a redirection server that redirects some data to one destination based on one rule, another destination based on another rule, and so on. As taught in Willens, filters contain one or more filter rules comprising an instruction to permit or deny access for each site listed. *See col. 5 ll. 11-12, 27-34, 60-66*. A user can request access to a site and the redirection server can check the filter rules stored locally and on a remote server, and “[b]ased on the result, the server 14 either permits or denies access.” *Col. 6 ll. 5-6*. Thus, Willens teaches a system that permits or denies access to multiple destinations. As discussed in Section IV.F., the Board stated that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the communications server of Willens to perform redirection to multiple destinations. Therefore, Willens renders obvious Claim 61.

**16. Claim 62**

Claim 62 is rendered obvious by Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 62 recites:

62. The method of claim 56, further including the step of creating database entries for a plurality of the plurality of users’ IDs, the plurality of users’ ID further being correlated with a common individualized rule set.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Claim 62 corresponds to Claim 14, discussed in Section V.B.8., and is rendered obvious for analogous reasons. Willens teaches that the access control system can have common rules for groups of users. For example, “[w]hen a game subscriber logs in, a user filter can be used to permit access to a game server, while allowing the ISP to deny access to non-subscribers.” *Col. 7 ll. 3-6*. Game subscribers can have a common rule set allowing access to the same game server. *See id.* Filters are stored in the RADIUS server 16 database and associate a filter with a user. *See col. 5 ll. 12-13*. Thus, Willens teaches that a plurality of user IDs can be associated with a common rule set, *e.g.*, the game subscriber filter rules. Therefore, Willens teaches all the limitations of Claim 62.

**17. Claim 63**

Claim 63 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 63 recites:

63. The method of claim 56, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

Claim 63 corresponds to Claim 32, discussed in Section V.B.9., and is rendered obvious for analogous reasons. The ’118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11*. Furthermore, the ’118 Patent declares that “[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header.” *Col. 2 ll. 11-13*. Willens teaches “[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]” *Col. 6 ll. 16-22*. Thus, Willens teaches filter rules that block and allow based on IP services because they detect protocols and ports such as http traffic. *See id.* In addition, as the Patent Owner admitted in the ’118 Patent and the Board recognized, “redirection is not limited to WWW traffic, and the concept is valid for all IP services.” *Col. 1 ll. 41-42; see Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the server in Willens to filter based on IP service. Therefore, Willens teaches or renders obvious each limitation in Claim 63.

**18. Claim 65**

Claim 65 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 65 recites:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

65. The method of claim 56, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

Claim 65 corresponds to Claim 34, discussed in Section V.B.10., and is rendered obvious for analogous reasons. The '118 Patent gives examples of “request type” as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36.* Therefore, the broadest reasonable interpretation of request type includes http requests. Willens teaches filters that are “an explicit set of rules based on either permit or deny syntax” and “[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]” *Col. 6 ll. 15-22.* Furthermore, “[t]he server 14 uses such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security.” *Col. 6 ll. 44-47.* Thus, Willens teaches filter rules that allow access based on a destination address and “request type,” such as http requests. Therefore, Willens teaches every limitation in Claim 65.

**19. Claim 66**

Claim 66 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 66 recites:

66. The method of claim 56, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 66 corresponds to Claim 35, discussed in Section V.B.11., and is rendered obvious for analogous reasons. Claim 66 is also identical to Claim 65 described above, except that Claim 66 is directed to “redirecting the data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. Willens teaches permitting or denying access based on a request type and destination address, as discussed above in Section V.I.18. In the Prior Reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in Willens to redirect data based on a request type and destination address. Therefore, Willens renders obvious Claim 66.

**20. Claim 67**

Claim 67 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 67 recites:

67. The method of claim 56, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

Claim 67 contains language that is identical to the language in canceled Claim 37, whose rejection based on obviousness was affirmed by the Board in the Prior Reexamination. *Linksmart Wireless*, No. 2011-009566, at 10. Willens teaches a communications server which "provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX], and port [http, etc.]" *Col. 6 ll.* 16-22. The redirection server in Willens utilizes IP packets and "such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security." *Col. 6 ll.* 44-49. Thus, Willens teaches a redirection server that extracts destination address information from IP packet headers to permit or deny a request for access. As the Board stated, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the server in Willens to perform redirection by replacing a first destination address in an IP packet header by a second destination address according to filter rules. Therefore, Claim 67 is rendered obvious by Willens.

**21. Claim 69**

Claim 69, depending from Claim 68, is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 69 recites:

69. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

Claim 69 corresponds to Claim 16, discussed in Section V.C.3., and is rendered obvious for analogous reasons. Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of "modification" of a portion of a rule set because updating a rule set can change or modify a rule.

As taught in Willens, the access control system 12 (which includes the communication server 14) "provides for a central, server based permit list that can be easily updated on a daily or

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

hourly basis.” *Col. 4 ll. 40-45*. Willens also teaches a “list of permitted sites being automatically maintained by periodically downloading updated versions of said list over the Internet.” *Col. 10 ll. 60-62*. Thus, Willens teaches a communications server 14 (corresponding to the redirection server) that can update rules as a function of time. Furthermore, the Board stated that “blocking a website based on these bases [as a function of time, data sent or received, or location accessed] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, the Board stated it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Based on the statements by the Board, it would have been obvious to modify the server in Willens to be configured to allow portions of rule sets to be modified, removed, or reinstated as a function of time. Therefore, Willens teaches or renders obvious all the limitations in Claim 69.

**22. Claim 70**

Claim 70, depending from Claim 68, is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 70 recites:

70. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

Claim 70 corresponds to Claim 17, discussed in Section V.C.4., and is rendered obvious for analogous reasons. Similar to Claim 69 above, Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of “modification” of a portion of a rule set because updating a rule set can change or modify a rule.

Willens teaches that filter rules and site lists can be updated at various times. *See col. 4 ll. 40-45; col. 10 ll. 60-62*. As taught in Willens, the communications server 14 can be configured to “control[] access by a user to sites based on the nature of their content” *Col. 6 ll. 66-67*. Thus, Willens teaches a redirection server responsive to data transmitted to or from the user. Moreover, as stated above regarding Claim 69, the Board declared that modifying rule sets based on data transmitted to or from the user would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the server in Willens to allow modification, removal, or reinstatement of rules as a function of data the user sends or receives. Therefore, Willens renders obvious Claims 70 and 73.

**23. Claim 71**

Claim 71, depending from Claim 68, is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 71 recites:

71. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.

Claim 71 corresponds to Claim 18, discussed in Section V.C.5., and is rendered obvious for analogous reasons. Similar to Claim 69 above, Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of "modification" of a portion of a rule set because updating a rule set can change or modify a rule.

Willens teaches that filter rules and site lists can be updated at various times. *See col. 4 ll. 40-45; col. 10 ll. 60-62.* As taught in Willens, a redirection server can perform a rule look-up when a user attempts to access a particular location. "This look-up contains the list name 'PTA List' and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it's [sic] local cache 50." *Col. 5 l. 64-col. 6 l. 7.* As described, the rule set stored in the local cache 50 on the communications server 14 is modified, including possibly removing or reinstating rules, based on the location a user tries to access. *See id.* Moreover, as stated above regarding Claim 69, the Board declared that modifying rule sets based on the location or locations the user accesses would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the server in Willens to allow modification of rules as a function of locations the user attempts to access. Therefore, Willens renders obvious Claims 71 and 74.

**24. Claim 72**

Claim 72, depending from Claim 68, is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 72 recites:

72. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

Claim 72 corresponds to Claim 19, discussed in Section V.C.6., and is rendered obvious for analogous reasons. The difference between Claim 69 and Claim 72 is that the limitation in Claim 69 states a portion of the rule set can be modified as a function of time and the limitation

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

in Claim 72 states a portion of the rule set can be removed or reinstated as a function of time. Thus, the difference between Claims 69 and 72 is a change from “modification” to “removal or reinstatement.” Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of “modification” and “removal or reinstatement” of a portion of a rule set because updating a rule set can change a rule, remove a rule, or reinstate a rule.

As taught in Willens, the access control system 12 (which includes the communication server 14) “provides for a central, server based permit list that can be easily updated on a daily or hourly basis.” *Col. 4 ll. 40-45*. Willens also teaches a “list of permitted sites being automatically maintained by periodically downloading updated versions of said list over the Internet.” *Col. 10 ll. 60-62*. Thus, Willens teaches a communications server 14 (corresponding to the redirection server) that can update rules as a function of time. Furthermore, the Board stated that “blocking a website based on these bases [as a function of time, data sent or received, or location accessed] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, the Board stated it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Based on the statements by the Board, it would have been obvious to modify the server in Willens to be configured to allow portions of rule sets to be modified, removed, or reinstated as a function of time. Therefore, Willens teaches or renders obvious all the limitations in Claim 72.

**25. Claim 73**

Claim 73, depending from Claim 68, is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 73 recites:

73. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

Claim 73 corresponds to Claim 20, discussed in Section V.C.7., and is rendered obvious for analogous reasons. Similar to Claims 69 and 72 above, the difference between Claims 70 and 73 is the change of the word “modification” to the words “removal or reinstatement.” Willens teaches that filter rules and site lists can be updated at various times. *See col. 4 ll. 40-45; col. 10 ll. 60-62*. As taught in Willens, the communications server 14 can be configured to “control[]

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

access by a user to sites based on the nature of their content” *Col. 6 ll. 66-67*. Thus, Willens teaches a redirection server responsive to data transmitted to or from the user. Moreover, as stated above regarding Claim 69, the Board declared that modifying rule sets based on data transmitted to or from the user would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the server in Willens to allow modification, removal, or reinstatement of rules as a function of data the user sends or receives. Therefore, Willens renders obvious Claim 73.

**26. Claim 74**

Claim 74, depending from Claim 68, is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 74 recites:

74. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.

Claim 74 corresponds to Claim 21, discussed in Section V.C.8., and is rendered obvious for analogous reasons. Similar to Claims 69 and 72 above, Claims 71 and 74 differ only in the change of the word “modification” to the words “removal or reinstatement.” Willens teaches that filter rules and site lists can be updated at various times. *See col. 4 ll. 40-45; col. 10 ll. 60-62*. As taught in Willens, a redirection server can perform a rule look-up when a user attempts to access a particular location. “This look-up contains the list name ‘PTA List’ and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 5 l. 64–col. 6 l. 7*. As described, the rule set stored in the local cache 50 on the communications server 14 is modified, including possibly removing or reinstating rules, based on the location a user tries to access. *See id.* Moreover, as stated above regarding Claim 69, the Board declared that modifying rule sets based on the location or locations the user accesses would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the server in Willens to allow modification of rules as a function of locations the user attempts to access. Therefore, Willens renders obvious Claim 74.

**27. Claim 75**

Claim 75 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 75 recites:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

75. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.

Claim 75 corresponds to Claim 22, discussed in Section V.C.9., and is rendered obvious for analogous reasons. Similar to Claim 72, Requestor respectfully submits that updating filter rules falls within the broadest reasonable interpretation of “removal or reinstatement” of a portion of the user’s rule set because updating a rule set can include removing or reinstating rules.

Willens teaches “controlling access by a user to sites based on the nature of their content.” *Col. 6 ll. 66-67*. Willens also teaches that a rule set can be modified based on a location the user accesses: “the [communications] server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the [remote access control] server 18.... The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 5 l. 64–col. 6 l. 7*. Thus, Willens teaches a communications server 14 (the redirection server) configured to allow automated modification of a rule set stored in its local cache as a function of data transmitted to or from the user or location the user accesses. Furthermore, the Board stated that “blocking a website based on these bases [time, data, or location] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the server in Willens to allow the modification, removal, or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed. Therefore, Willens renders obvious Claim 75.

**28. Claim 76**

Claim 76 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 76 recites:

76. The system of claim 68, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Claim 76 corresponds to Claim 23, discussed in Section V.C.10., and is rendered obvious for analogous reasons. As taught in figure 1 in Willens, reproduced above as Diagram 11, a redirection server 14 is connected to a user through a modem 22 on a user side and the Internet or Public/Private network 26 on a network side. *See also* figs. 4, 5 (illustrating similar configurations of users, redirection servers, and computer networks). Willens teaches that the access control subsystem 12 (which includes the communications server 14) “provides a centralized way to operate content monitoring using the very communications servers and routers that users’ traffic travels *through* to get to the Internet.” *Col. 4 ll. 37-40* (emphasis added). Thus, to access the computer network, the user computer connects through the communications server 14. As described above in Sections V.C.2. and V.G.2., Willens in combination with Zenchelsky and the Patent Owner’s admissions renders obvious a user computer using a temporarily assigned network address. It would have been obvious to modify the computer in Willens to be associated with a temporary network address. Therefore, Willens, in view of Zenchelsky and the Patent Owner’s admissions, renders obvious Claim 76.

**29. Claim 77**

Claim 77 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 77 depends from Claim 76, discussed above in Section V.I.28., and recites:

77. The system of claim 76 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.

Claim 77 corresponds to Claim 24, discussed in Section V.C.11., and is rendered obvious for analogous reasons. As taught in Willens, the redirection server (communications server 14) can update its rule set based on information received from a remote server 18 situated on the computer network side of the communications server 14 in figure 1 (Diagram 11). *See col. 5 l. 64-col. 6 l. 7; col. 4 ll. 40-45; fig. 1*. Thus, Willens teaches a redirection server receiving instructions to modify a rule set from its computer network side. Therefore, Willens teaches all the limitations of Claim 77.

**30. Claim 78**

Claim 78 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 78 recites:

78. The system of claim 68, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Claim 78 corresponds to Claim 36, discussed in Section V.C.12., and is rendered obvious for analogous reasons. The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11*. Furthermore, the '118 Patent declares that “[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header.” *Col. 2 ll. 11-13*. Willens teaches “[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]” *Col. 6 ll. 16-22*. Thus, Willens teaches filter rules that block and allow based on IP services because they detect protocols and ports such as http traffic. *See id.* In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, “redirection is not limited to WWW traffic, and the concept is valid for all IP services.” *Col. 1 ll. 41-42; see Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the server in Willens to filter based on IP service. Therefore, Willens teaches or renders obvious each limitation in Claim 78.

**31. Claim 80**

Claim 80 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 80 recites:

80. The system of claim 68, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

Claim 80 corresponds to Claim 38, discussed in Section V.C.13., and is rendered obvious for analogous reasons. The '118 Patent gives examples of “request type” as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36*. Therefore, the broadest reasonable interpretation of request type includes http requests. Willens teaches filters that are “an explicit set of rules based on either permit or deny syntax” and “[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]” *Col. 6 ll. 15-22*. Furthermore, “[t]he server 14 uses such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security.” *Col. 6 ll. 44-47*. Thus, Willens teaches filter rules that allow access based on a destination address and “request type,” such as http requests. Therefore, Willens teaches every limitation in Claim 80.

**32. Claim 81**

Claim 81 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 81 recites:

81. The system of claim 68, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 81 corresponds to Claim 39, discussed in Section V.C.14., and is rendered obvious for analogous reasons. Furthermore, Claim 81 is identical to Claim 80, except that Claim 81 is directed to "redirecting the data to a new destination address" instead of "allowing access" based on a request type and an attempted destination address. Willens teaches permitting or denying access based on a request type and destination address, as discussed above in Section V.I.31. In the Prior Reexamination, the Board declared, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in Willens to redirect data based on a request type and destination address. Therefore, Willens renders obvious Claim 81.

**33. Claim 82**

Claim 82 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 82 recites:

82. The system of claim 68, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the modified rule set.

Claim 82 contains language that is identical to the language in canceled Claim 42, whose rejection based on obviousness was affirmed by the Board in the Prior Reexamination. *Linksmart Wireless*, No. 2011-009566, at 10. Willens teaches a communications server which "provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX], and port [http, etc.]." *Col. 6 ll. 16-22*. The redirection server in Willens utilizes IP packets and "such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security." *Col. 6 ll. 44-49*. Thus, Willens teaches a redirection server that extracts destination address information from IP packet headers to permit or deny a request for access. As the Board stated, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the server in Willens to perform redirection by replacing a first destination address in an IP packet header by a second destination address according to filter rules. Therefore, Claim 82 is rendered obvious by Willens.

**34. Claim 84**

Claim 84 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 84 recites:

84. The method of claim 83, further including the step of modifying at least a portion of the user’s rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.

Claim 84 corresponds to Claim 26, discussed in Section V.D.3., and is rendered obvious for analogous reasons. As stated above, updating filter rules falls within the broadest reasonable interpretation of “modifying” and “removing or reinstating at least a portion of the user’s rule set” because updating a rule set can include altering, removing, or reinstating rules.

Willens teaches “controlling access by a user to sites based on the nature of their content.” *Col. 6 ll. 66-67*. Willens also teaches that a rule set can be modified based on a location the user accesses: “the [communications] server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the [remote access control] server 18.... The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it’s [sic] local cache 50.” *Col. 5 l. 64–col. 6 l. 7*. Thus, Willens teaches a communications server 14 (the redirection server) configured to allow automated modification of a rule set stored in its local cache as a function of data transmitted to or from the user or location the user accesses. Furthermore, the Board stated that “blocking a website based on these bases [time, data, or location] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the server in Willens to allow the modification, removal, or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed. Therefore, Willens renders obvious Claim 84.

**35. Claim 85**

Claim 85 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 85 recites:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

85. The method of claim 83, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and the location or locations the user accesses.

Claim 85 corresponds to Claim 27, discussed in Section V.D.4., and is rendered obvious for analogous reasons. Furthermore, Claims 84 and 85 differ only in the change of the word "modification" to the words "removal or reinstatement." As stated above, Requestor respectfully submits that updating filter rules falls within the broadest reasonable interpretation of "removing or reinstating at least a portion of the user's rule set" because updating a rule set can include removing or reinstating rules.

Willens teaches "controlling access by a user to sites based on the nature of their content." *Col. 6 ll. 66-67*. Willens also teaches that a rule set can be modified based on a location the user accesses: "the [communications] server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the [remote access control] server 18.... The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it's [sic] local cache 50." *Col. 5 l. 64-col. 6 l. 7*. Thus, Willens teaches a communications server 14 (the redirection server) configured to allow automated modification of a rule set stored in its local cache as a function of data transmitted to or from the user or location the user accesses. Furthermore, the Board stated that "blocking a website based on these bases [time, data, or location] would have been obvious" to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the server in Willens to allow the modification, removal, or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed. Therefore, Willens renders obvious Claim 85.

**36. Claim 86**

Claim 86 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 86 recites:

86. The method of claim 83, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

Claim 86 corresponds to Claim 40, discussed in Section V.D.5., and is rendered obvious for analogous reasons. The '118 Patent gives examples of IP services which include FTP,

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

WWW data, or Telnet session data. *Col. 2 ll. 7-11*. Furthermore, the '118 Patent declares that “[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header.” *Col. 2 ll. 11-13*. Willens teaches “[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]” *Col. 6 ll. 16-22*. Thus, Willens teaches filter rules that block and allow based on IP services because they detect protocols and ports such as http traffic. *See id.* In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, “redirection is not limited to WWW traffic, and the concept is valid for all IP services.” *Col. 1 ll. 41-42; see Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the server in Willens to filter based on IP service. Therefore, Willens teaches or renders obvious each limitation in Claim 86.

**37. Claim 88**

Claim 88 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 88 recites:

88. The method of claim 83, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

Claim 88 corresponds to Claim 42, discussed in Section V.D.6., and is rendered obvious for analogous reasons. The '118 Patent gives examples of “request type” as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36*. Therefore, the broadest reasonable interpretation of request type includes http requests. Willens teaches filters that are “an explicit set of rules based on either permit or deny syntax” and “[t]he firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX] and port [http, etc.]” *Col. 6 ll. 15-22*. Furthermore, “[t]he server 14 uses such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security.” *Col. 6 ll. 44-47*. Thus, Willens teaches filter rules that allow access based on a destination address and “request type,” such as http requests. Therefore, Willens teaches every limitation in Claim 88.

**38. Claim 89**

Claim 89 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 89 recites:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

89. The method of claim 83, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 89 corresponds to Claim 43, discussed in Section V.D.7., and is rendered obvious for analogous reasons. Furthermore, Claim 89 is identical to Claim 88 described above, except that Claim 89 is directed to “redirecting the data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. Willens teaches permitting or denying access based on a request type and destination address, as discussed above in Section V.I.37. In the Prior Reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in Willens to redirect data based on a request type and destination address. Therefore, Willens renders obvious Claim 89.

**39. Claim 90**

Claim 90 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 90 recites:

90. The method of claim 83, wherein the redirection server is configured to redirect data from the users’ computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

Claim 90 contains language that is identical to the language in canceled Claim 47, whose rejection based on obviousness was affirmed by the Board in the Prior Reexamination. *Linksmart Wireless*, No. 2011-009566, at 10. Willens teaches a communications server which “provides bidirectional (input/output) packet filtering for source and destination addresses, for protocol [TCP, UDP, IP, IPX], and port [http, etc.]” *Col. 6 ll. 16-22*. The redirection server in Willens utilizes IP packets and “such addresses [source and destination addresses] in packet headers for making decisions on the handing [sic] of IP packets, such as for firewall security.” *Col. 6 ll. 44-49*. Thus, Willens teaches a redirection server that extracts destination address information from IP packet headers to permit or deny a request for access. As the Board stated, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the server in Willens to perform redirection by replacing a first

destination address in an IP packet header by a second destination address according to filter rules. Therefore, Claim 90 is rendered obvious by Willens.

**VI. CLAIMS 29, 33, 37, 41, 52, 64, 79, AND 87 ARE OBVIOUS OVER WILLENS IN VIEW OF HE, ZENCHELSKY, AND THE PATENT OWNER'S ADMISSIONS**

Claims 29, 33, 52, and 64 contain the following limitation:

*wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set*

Claims 37, 41, 79, and 87 contain the following limitation:

*wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set*

The only difference between the language in the first noted limitation and the second is a change from “the individualized rule set” to “the modified rule set.” This change corresponds to the difference in the two general groups of claims, as described in Section II.B., where the first group pertains to controlling access to the Internet based on rule sets and the second group pertains to modification of the rule sets. However, as described in the '118 Patent, the individualized rule set and the modified rule set both refer to rule sets which are “personalized filtering and redirection information for the particular user ID.” *Col. 3 ll. 3-4.*

**A. Claims 29, 33, 52, and 64**

Claims 29, 33, 52, and 64 depend respectively from canceled Claim 1, canceled Claim 8, Claim 44, and Claim 56. Each of the limitations in canceled Claim 1, canceled Claim 8, Claim 44, and Claim 56 are taught by Willens or are rendered obvious by the combination of Willens, Zenchelsky, and the Patent Owner's admissions as described above in Sections V.A., V.B., V.E., and V.F., respectively.

In regard to the limitation in Claims 29, 33, 52, and 64, Willens teaches that rule sets and filters can be modified based on time parameters. The system in Willens “provides for a central, server based permit list that can be easily updated on a daily or hourly basis, and that cannot be tampered with by the end users.” *Col. 4 ll. 40-45.* The system in Willens can also be used to provide rule sets to different groups of people, such as subscribers to a service and non-subscribers. *See col. 7 ll. 3-10; fig. 4.* For example, Willens teaches “[w]hen a game subscriber

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

logs in, a user filter can be used to permit access to a game server, while allowing the ISP to deny access to non-subscribers.” *Col. 7 ll. 3-10*. In such a scenario, a non-subscriber can be associated with one set of rules for an initial period of time until he or she becomes a subscriber, wherein a different set of rules would be associated with the subscriber. *See id.* As another example, Willens teaches “[w]hen the manufacturer’s clients dial into network 82 and log in as VIPguest, a network access filter can be downloaded to the communications server 84 from access server 86 which only permits visibility to the predefined auto dealer sites 87.” *Col. 7 ll. 31-35; fig. 5*. In this instance, the clients have a temporary rule set associated with them for an initial period of time during the initial log in process, and after logging in a standard filter set is downloaded and applied. *See id.*

The system taught in He is generally an authentication system that enables users to gain access to online services such as server computers and printers. He discloses “a network security architecture to provide protection to user access to the resources and information in network elements.” *Col. 33 ll. 8-10*. In one embodiment, the system in He allows or denies access based on duration of a timed session. *See col. 28 ll. 26-41*. He states “[a] session length is typically defined as the period between log-ons for a user element coupled to the network 106, or for dial-up sessions delimited by the dial-up communication protocol software.” *Col. 28 ll. 26-29*. The administrator of the system in He can limit the “time that the user element and selected network can communicate with each other.” *Col. 28 ll. 31-33*. Furthermore, He states that “if the length of time that is allowed for the log-on session is exceeded, all the tickets [granting access to network elements] that have been issued to the user will also become invalid and therefore be destroyed.” *Col. 28 ll. 36-38*. Thus, He teaches a first rule set which allows access to network elements which can expire after a defined amount of time wherein a second rule set is applied which denies access to network elements.

Hence, it would have been obvious to modify the rule sets in Willens to include a temporary rule set for an initial period of time and a standard rule set thereafter, as taught in He. Therefore, Requestor respectfully submits that Claims 29, 33, 52, and 64 are obvious over Willens in view of He, Zenchelsky, and the Patent Owner’s admissions.

**B. Claims 37, 41, 79, and 87**

Claims 37, 41, 79, and 87 depend respectively from canceled Claim 15, canceled Claim 25, Claim 68, and Claim 83. Each of the limitations in canceled Claim 15, canceled Claim 25,

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Claim 68, and Claim 83 are taught by Willens or are rendered obvious by the combination of Willens, Zenchelsky, and the Patent Owner's admissions as described above in Sections V.C., V.D., V.G., and V.H., respectively.

In regard to the limitation in Claims 37, 41, 79, and 87, Willens teaches that rule sets and filters can be modified based on time parameters. The system in Willens "provides for a central, server based permit list that can be easily updated on a daily or hourly basis, and that cannot be tampered with by the end users." *Col. 4 ll. 40-45*. The system in Willens can also be used to provide rule sets to different groups of people, such as subscribers to a service and non-subscribers. *See col. 7 ll. 3-10; fig. 4*. For example, Willens teaches "[w]hen a game subscriber logs in, a user filter can be used to permit access to a game server, while allowing the ISP to deny access to non-subscribers." *Col. 7 ll. 3-10*. In such a scenario, a non-subscriber can be associated with one set of rules for an initial period of time until he or she becomes a subscriber, wherein a different set of rules would be associated with the subscriber. *See id.* As another example, Willens teaches "[w]hen the manufacturer's clients dial into network 82 and log in as VIPguest, a network access filter can be downloaded to the communications server 84 from access server 86 which only permits visibility to the predefined auto dealer sites 87." *Col. 7 ll. 31-35; fig. 5*. In this instance, the clients have a temporary rule set associated with them for an initial period of time during the initial log in process, and after logging in a standard filter set is downloaded and applied. *See id.*

The system taught in He is generally an authentication system that enables users to gain access to online services such as server computers and printers. He discloses "a network security architecture to provide protection to user access to the resources and information in network elements." *Col. 33 ll. 8-10*. In one embodiment, the system in He allows or denies access based on duration of a timed session. *See col. 28 ll. 26-41*. He states "[a] session length is typically defined as the period between log-ons for a user element coupled to the network 106, or for dial-up sessions delimited by the dial-up communication protocol software." *Col. 28 ll. 26-29*. The administrator of the system in He can limit the "time that the user element and selected network can communicate with each other." *Col. 28 ll. 31-33*. Furthermore, He states that "if the length of time that is allowed for the log-on session is exceeded, all the tickets [granting access to network elements] that have been issued to the user will also become invalid and therefore be destroyed." *Col. 28 ll. 36-38*. Thus, He teaches a first rule set which allows access to network

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

elements which can expire after a defined amount of time wherein a second rule set is applied which denies access to network elements.

Hence, it would have been obvious to modify the rule sets in Willens to include a temporary rule set for an initial period of time and a standard rule set thereafter, as taught in He. Therefore, Requestor respectfully submits that Claims 37, 41, 79, and 87 are obvious over Willens in view of He, Zenchelsky, and the Patent Owner's admissions.

**VII. THE CLAIMS OF THE '118 PATENT ARE OBVIOUS OVER CHOICENET IN VIEW OF ZENCHELSKY AND THE PATENT OWNER'S ADMISSIONS, RAISING SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY**

With the above understanding of the prior art references, the following argument is presented to show that the claims of the '118 Patent are obvious under 35 U.S.C. § 103. The Appendix features claim charts showing that each limitation of the claims in this request is present in ChoiceNet when combined with Zenchelsky and the Patent Owner's admissions in the '118 Patent. Thus, Requestor has raised a substantial new question of patentability.

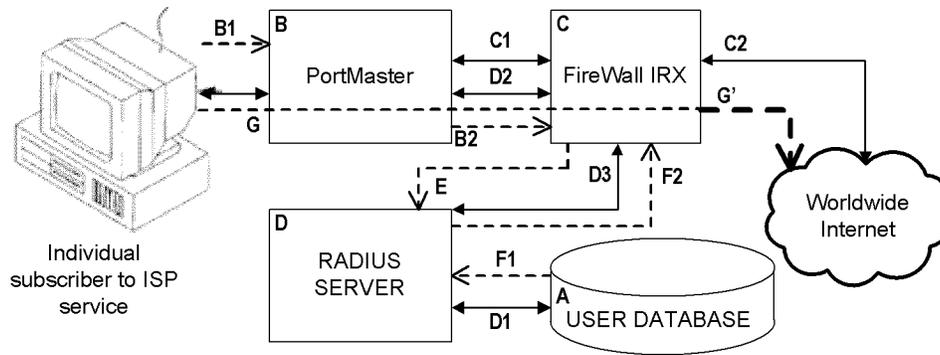
**A. Claims 2-7, 28, and 30-31 Are Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's Admissions**

**1. Overview of Obviousness**

Claims 2-7 and 28-31 are rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner's admissions in the Background section of the '118 Patent. Claims 2-7 and 28-31 are dependent on canceled Claim 1, thus each of the claims share common elements corresponding to canceled Claim 1. Reproduced below is the Patent Owner's annotated figure 2, identifying the common elements of Claims 2-7 and 28-31 (with explanatory text removed for clarity):

Diagram 16 depicts the elements taught in ChoiceNet, arranged in the form of the above Diagram 9, to demonstrate the correspondences between the claim elements and elements of the prior art reference:

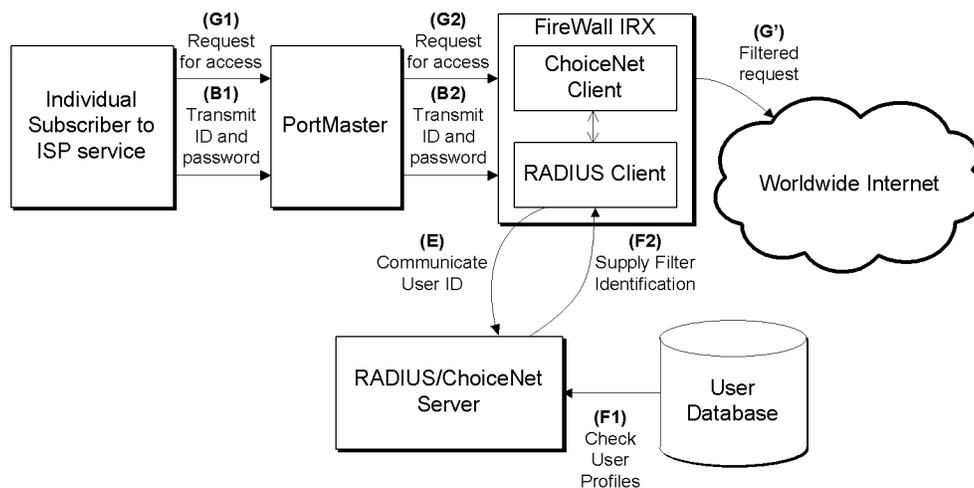
**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**



**Comparison Figure of Teachings of ChoiceNet**

**Diagram 16 – Embodiment of the system taught in ChoiceNet arranged like the '118 Patent system**

For comparison, the schematic diagram from ChoiceNet is reproduced below in Diagram 17, to show that Diagram 9 in fact corresponds to elements of Willens.



**Schematic Diagram of ChoiceNet**

**Diagram 17 - Schematic diagram of the system in ChoiceNet**

An individual subscriber to an ISP service transmits a username and a password to the PortMaster server (B1). *ChoiceNet™ Administrator's Guide* 1-6, figs. 1-2, 5-10. The PortMaster server then transmits this information to the FireWall IRX router (B2). The RADIUS client running on the FireWall IRX router communicates this information to the RADIUS server (E). *Id.* at 1-6, fig. 1-2. The RADIUS server authorizes the user through the user database (F1). *Id.* at 1-6, fig. 1-2. The RADIUS server supplies a filter identification to the ChoiceNet client through the RADIUS client (F2). *Id.* at 1-6, fig. 1-2. The filter identification corresponds to filter rules found in the ChoiceNet client or retrieved from the ChoiceNet server. *Id.* at 1-7, fig. 1-3. The subscriber requests access to a network location and the request gets passed to the ChoiceNet client 44 on the FireWall IRX router which processes that request (G1, G2). *Id.* at 1-

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

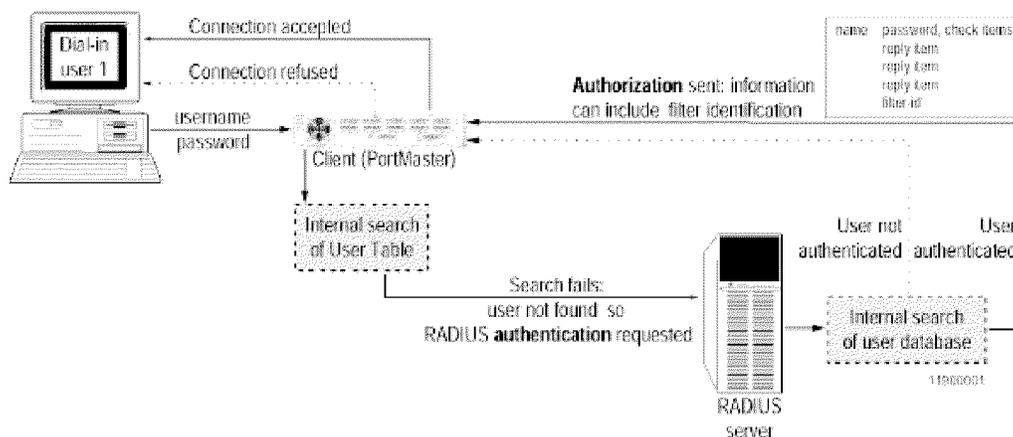
7, fig. 1-4. The FireWall IRX router, through the ChoiceNet client, applies the filter rules and either permits or denies the requested access. (G'). *Id.* at 1-7, fig. 1-4.

In the Prior Reexamination, the Board found Claim 1 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. Each of claims 2-7 and 28-31 add limitations to Claim 1 which, as described in more detail below, would have been obvious in view of ChoiceNet and the prior art at the time of invention, as admitted by the Patent Owner and demonstrated by Zenchelsky.

**2. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of ChoiceNet in relation to the common elements of Claims 2-7 and 28-31. Each limitation has been identified using letters (a) through (g) for ease of description and for later reference. The Appendix features claim charts of Claims 2-7 and 28-31 which shows that each limitation of Claims 2-7 and 28-31 is present in ChoiceNet when combined with Zenchelsky and the Patent Owner's admissions in the '118 Patent. In relation to the common elements of Claims 2-7 and 28-31, ChoiceNet teaches or renders obvious a system comprising:

(a) *a database with entries correlating each of a plurality of user IDs with an individualized rule set*: ChoiceNet teaches that in figure 1-2, reproduced below as Diagram 18, "the PortMaster requests the RADIUS server to authenticate the user" and "[t]he RADIUS server searches its user database." *ChoiceNet™ Administrator's Guide* 1-6, fig. 1-2. Moreover, "[o]ne of the reply items [from the RADIUS server] is the *Filter-Id* that associates a filter with the user." *Id.* (emphasis original). ChoiceNet states that an administrator "can create filters...to permit or deny user access." *Id.* at 5-1. Thus, ChoiceNet teaches a database with entries correlating a user with a filter, which is the individualized rule set in the limitation.

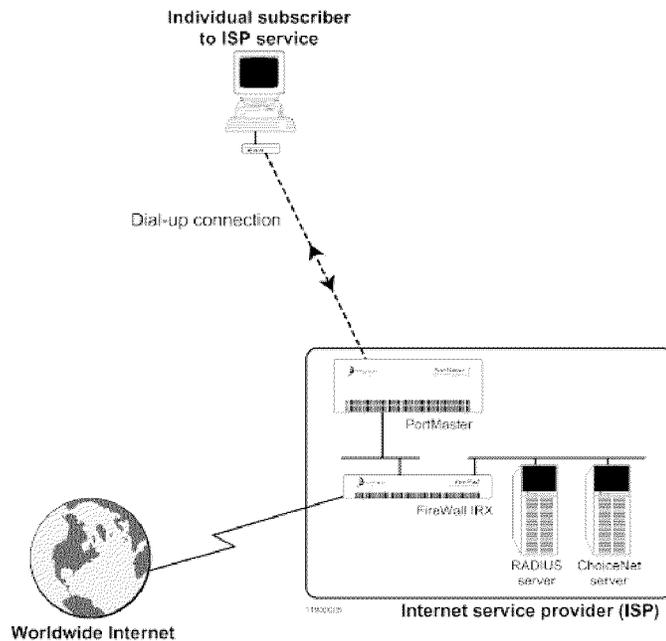


**Diagram 18 – Figure 1-2 from ChoiceNet**

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

**(b) a dial-up network server that receives user IDs from users' computers:** As shown in Diagram 18 above, ChoiceNet teaches a dial-up network server, the "PortMaster" in the figure. See *ChoiceNet* fig. 5-10. As described above, the dial-up network server in the '118 Patent "is used to establish a communication link with the user's PC." *Col. 3 ll. 60-63.* Figure 1-2 from ChoiceNet, Diagram 18 above, teaches a subscriber connecting to the PortMaster through a dial-up connection. Thus, the PortMaster from ChoiceNet corresponds to the dial-up network server in the limitation. Furthermore, figure 1-2 from ChoiceNet teaches that the PortMaster receives a user ID (or username) and password from the user's computer (Dial-in user 1 in the figure). Therefore, ChoiceNet teaches each element of the above recited limitation.

**(c) a redirection server connected to the dial-up network server and a public network:** Figure 5-10 from ChoiceNet, reproduced as Diagram 19 below, shows a FireWall IRX router connected to, and situated between, the PortMaster and the World Wide Internet. ChoiceNet teaches that "ChoiceNet clients communicate with the ChoiceNet server to determine user access" and that ChoiceNet clients can be FireWall IRX Routers. *ChoiceNet* 1-1. Furthermore, "a ChoiceNet filter contains a list of rules" and "[a] ChoiceNet client executes the rules from the top down as they are presented in the filter text file." *Id.* at 1-4. Thus, the ChoiceNet client, such as the FireWall IRX Router, corresponds to the redirection server in the limitation. Therefore, ChoiceNet teaches a redirection server (the FireWall IRX) connected to, and sitting between, the dial-up network server (the PortMaster) and a public network (the Worldwide Internet).



**Diagram 19 – Network topology in the ChoiceNet system**

**(d) an authentication accounting server connected to the database, the dial-up network server and the redirection server:** As illustrated above in Diagram 18 and Diagram 19, the RADIUS Server is connected to the FireWall IRX and the PortMaster. *ChoiceNet* figs. 1-2, 5-10. The RADIUS Server authenticates a user based on the username and password by “search[ing] its user database.” *Id.* at 1-6; *see id.* fig. 1-2. In the ’118 Patent, the authentication accounting server “is used to authenticate user ID and permit, or deny, access to the network.” *Col. 4 ll. 5-7.* Thus, the RADIUS Server taught in ChoiceNet falls within a reasonable interpretation of the authentication accounting server in the limitation. Therefore, ChoiceNet teaches an authentication accounting server (the RADIUS Server) connected to the database, the dial-up network server (the PortMaster) and the redirection server (the FireWall IRX Router).

**(e) wherein the dial-up network server communicates a first user ID for one of the users’ computers and a temporarily assigned network address for the first user ID to the authentication accounting server:** ChoiceNet teaches in figure 1-2, included above as Diagram 18, that the login process is as follows:

[A] dial-in user logs in to a PortMaster. The PortMaster first searches its User Table for the dial-in user. If the user is found in the User Table, the user is authenticated for the User Table. If the user is not found in the User Table, the PortMaster requests the RADIUS server to authenticate the user. The RADIUS server searches its user database.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*ChoiceNet* 1-6. The PortMaster (corresponding to the dial-up network server) receives the username and password directly from the dial-in user for authentication purposes. *See id.* The PortMaster can then communicate that information to the RADIUS server (corresponding to the authentication accounting server), see Diagram 18. The communication between the PortMaster and RADIUS server includes the transmission of IP packets, which contain network address information. *Id.* at 5-5. Thus, the PortMaster passes the network address to the RADIUS server along with the user ID to complete the authentication process. Therefore, each element of the above recited claim is taught or is rendered obvious by *ChoiceNet*.

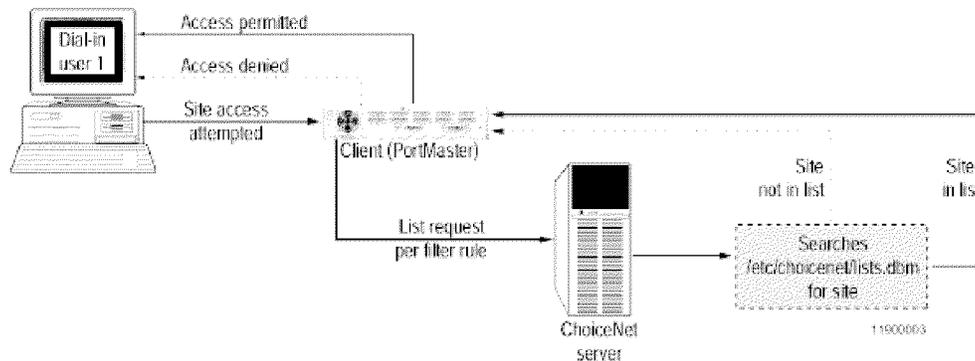
***(f) wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server:*** *ChoiceNet* teaches that the RADIUS server replies to an authentication request with “the *Filter-Id* that associates a filter with the user.” *Id.* at 1-6. In Diagram 18, the RADIUS server sends filter information to the *ChoiceNet* client (running on the PortMaster in this embodiment) that may have the rules associated with the filter information in local cache or it may request the rules from a *ChoiceNet* server. *See id.* at 1-6 to 1-7, 5-10; fig. 1-3. In Diagram 19, the FireWall IRX Router is running the *ChoiceNet* client and applying the filter rules. *See id.* at 1-1. Thus, the RADIUS server (corresponding to the authentication accounting server) communicates filter rules associated with a user to the *ChoiceNet* client (corresponding to the redirection server).

Furthermore, filter rules can be based on source or destination IP addresses. *See id.* at 5-1. The *ChoiceNet* client must know the source IP address, or the address associated with the user, to be able to apply the filter rules. *See id.* Thus, in addition to the user ID, the network address must be communicated to the redirection server. Therefore, each element of the above recited claim is taught or is rendered obvious by *ChoiceNet*.

***(g) wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set:*** In Diagram 20 below, *ChoiceNet* teaches that “the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7. In Diagram 19, the FireWall IRX Router, instead of the PortMaster in Diagram 20,

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

runs the ChoiceNet client which applies the filter rules to data directed toward the Internet. Thus, each element of the above recited limitation is taught by ChoiceNet.



**Diagram 20 - ChoiceNet client applying filter rules**

**3. The Combination of ChoiceNet, Zenchelsky, and the Patent Owner's Admissions Renders the Common Elements of Claims 2-7 and 28-31 Obvious**

ChoiceNet may not teach the following two elements of Claims 2-7 and 28-31:

1. A redirection server that performs redirection as well as blocking; and
2. A dial-up network server that communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication and accounting server.

However, these differences between ChoiceNet and the claims would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner's admissions of prior art.

In regard to the first of the noted limitations, the Board has already stated that it would have been obvious at the time of the invention to modify a ChoiceNet client, such as one running on the FireWall IRX Router of ChoiceNet, to perform redirection as well as permitting or denying access to the user. The Board stated that, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Because a ChoiceNet client can be configured as a control to block the user, it would have been obvious to alter it to redirect the user as well. Thus, the FireWall IRX Router in Diagram 19, as taught in ChoiceNet, corresponds to the redirection server of the '118 Patent because it applies filter rules through the ChoiceNet client to permit or deny access to users and it would have been obvious to alter its functionality to include redirection capabilities.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

In regard to the second of the noted limitations, to the extent the examiner does not find that ChoiceNet teaches that “the dial-up network server communicates a first user ID for one of the users’ computers and a temporarily assigned network address for the first user ID to the authentication accounting server,” ChoiceNet combined with Zenchelsky and the Patent Owner admitted prior art does.

As described above, in the background section of the ’118 Patent, the Patent Owner admits that in “prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP’s authentication and accounting server 104.” *Col. 1 ll. 21-24*. Thus, by the Patent Owner’s admission, this limitation was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found:

It would have been obvious to one of ordinary skill in the art to modify He et al [U.S. Patent No. 6,088,451]; so to provide temporary IP address to a user node and additionally encode communications packets with source and destination addresses as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.

Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and communicating using IP addresses and that this teaching was within the prior art as admitted by the Patent Owner in the background section of the ’118 Patent.

**4. Claim 2**

In addition to common elements (a) through (g) described above, Claim 2 contains the following limitation:

***wherein the redirection server further provides control over a plurality of data to and from the users’ computers as a function of the individualized rule set:*** ChoiceNet teaches that “filter rules [can be written] to specify a site list in place of an IP address.... Each site list is a text file that contains the hostnames or IP addresses of hosts for which access is controlled. The rule can permit or deny access by hosts on the list or to hosts on the list.” *ChoiceNet* 1-3. ChoiceNet also teaches a redirection server that “searches the Filter Table for the filters specified by Filter-Id in the user entry. If the filters are present in the Filter Table, then they are applied to the connection.” *Id.* at 1-6. Thus, ChoiceNet teaches filter rules implemented by a redirection server that control a plurality of data to and from a user computer.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 2 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**5. Claim 3**

In addition to common elements (a) through (g) described above, Claim 3 contains the following limitation:

*wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set:* ChoiceNet teaches that the system "enables both inbound and outbound traffic filtering for each interface and user." *ChoiceNet* 1-2. In addition, ChoiceNet teaches that "the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule." *Id.* at 1-7; figure 1-4. As described above, the PortMaster running the ChoiceNet client acts as the redirection server in the '118 Patent. The ChoiceNet client can deny traffic to and from a user's computer based on input filter rules. The input filter rules correspond to the individualized rule set of the '118 Patent. Therefore, ChoiceNet teaches a redirection server that blocks data to and from the users' computers as a function of the individualized rule set.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 3 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**6. Claim 4**

In addition to common elements (a) through (g) described above, Claim 4 contains the following limitation:

*wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set:* ChoiceNet teaches that the system "enables both inbound and outbound traffic filtering for each interface and user." *ChoiceNet* 1-2. In addition, ChoiceNet teaches that "the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule." *Id.* at 1-7; figure 1-4. As described above, the PortMaster running the ChoiceNet client acts as the redirection server in the '118 Patent. The ChoiceNet client can permit traffic to and from a user's computer based on input filter rules. The input filter rules correspond to the individualized rule set of the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

'118 Patent. Therefore, ChoiceNet teaches a redirection server that permits data to and from the users' computers as a function of the individualized rule set.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 4 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**7. Claim 5**

In addition to common elements (a) through (g) described above, Claim 5 contains the following limitation:

*wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set:* ChoiceNet teaches a system that controls access to a user by blocking data based on filter rules: "the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule." *Id.* at 1-7; figure 1-4. As discussed in Section IV.F., the Board declared that, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user" and "redirection would have been an obvious extension of blocking." *Linksmart Wireless*, No. 2011-009566, at 9, 10. Based on the statement by the Board, it would have been obvious to modify the system in ChoiceNet to redirect data to and from a user's computer as a function of filter rules.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 5 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**8. Claim 6**

In addition to common elements (a) through (g) described above, Claim 6 contains the following limitation:

*wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set:* Requestor respectfully submits that, given its broadest reasonable interpretation, Claim 6 encompasses at least a redirection server that redirects some data to one destination based on one rule, another destination based on another rule, and so on. ChoiceNet teaches filter rules that "specify a site list in place of an IP address.... Each site list is a text file that contains the hostnames or IP addresses of hosts for which access is controlled. The rule can permit or deny access by hosts on the list or to hosts on the list." *ChoiceNet* 1-3. Thus, ChoiceNet teaches filters that can specify

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

multiple rules, each rule directed to unique destinations. As discussed in Section IV.F., the Board stated that, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system of ChoiceNet that blocks and allows data to multiple destinations to perform redirection to multiple destinations.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 6 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**9. Claim 7**

In addition to common elements (a) through (g) described above, Claim 7 contains the following limitation:

***wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set:*** ChoiceNet teaches that a filter rule can be specified for a user by "defin[ing] the *Filter-Id* reply item in [the user's] RADIUS entry as the filter name" where "*Filter-Id* is a reply item that identifies the filter to be associated with that user." *ChoiceNet* 5-14, 5-10. By defining the same *Filter-Id* in multiple users' RADIUS entries, ChoiceNet teaches that multiple users can be correlated with a common rule set. *See id.* at 5-10, 5-15. For example, ChoiceNet teaches that an "ISP can customize access to sites or services for groups of subscribers that share similar interests" through the use of filter rules. *Id.* at 5-10. Thus, multiple users can be correlated with a common rule set.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 7 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**10. Claim 28**

In addition to common elements (a) through (g) described above, Claim 28 contains the following limitation:

***wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service:*** The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll.* 7-11. Furthermore, the '118 Patent declares that IP "[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header." *Col. 2 ll.* 11-13. ChoiceNet teaches that "[p]ackets can be filtered according to...source and destination port numbers to control access to certain network services." *ChoiceNet* 5-6; *see also ChoiceNet* Appx. C (listing common port numbers assigned

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

to TCP and UDP services). Thus, ChoiceNet teaches filtering based on a type of IP service by specifying a source or destination port in the filter rule.

In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, "redirection is not limited to WWW traffic, and the concept is valid for all IP services." *Col. 1 ll. 41-42; see Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the system in ChoiceNet to filter based on IP service.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 28 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**11. Claim 30**

In addition to common elements (a) through (g) described above, Claim 30 contains the following limitation:

*wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address:* The '118 Patent gives examples of "request type" as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36*. Therefore, the broadest reasonable interpretation of request type includes http requests. ChoiceNet teaches that filters can be implemented based on port numbers which correlate to IP services: "Rules can use the source and destination port numbers to control access to certain network services." *ChoiceNet* 5-6. For example, in Appendix C in the ChoiceNet reference, port 80 is associated with "World Wide Web Hypertext Transfer Protocol (HTTP)." In an example filter rule, access is permitted for "Web access via HTTP to the addresses in the site list **wwwok**." *Id.* at 5-9, fig. 8, Table 5-1. Furthermore, ChoiceNet teaches "[a] rule can evaluate either the source or destination address of a packet." *Id.* at 5-6. Thus, ChoiceNet teaches filter rules that allow access based on a request type and destination address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 30 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**12. Claim 31**

In addition to common elements (a) through (g) described above, Claim 31 contains the following limitation:

*wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address:* Claim 31 is identical to Claim 30 described above, except that Claim 31 is directed to "redirecting the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. ChoiceNet teaches permitting or denying access based on a request type and destination address, as discussed above in Section VI.A.11. In the Prior Reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to redirect data based on a request type and destination address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 31 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**B. Claims 9-14, 32, and 34-35 Are Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s Admissions**

**1. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of ChoiceNet in relation to canceled Claim 8 which forms the common elements of Claims 9-14 and 32-35. In the Prior Reexamination, the Board found Claim 8 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. Each of claims 9-14 and 32-35 add limitations to Claim 8. As described in more detail below, these limitations would have been obvious in view of ChoiceNet and the prior art at the time of invention, as admitted by the Patent Owner and demonstrated by Zenchelsky.

The common elements of Claims 9-14 and 32-35 are analogous to the common elements of Claims 2-7 and 28-31, and so the common elements of Claims 9-14 and 32-35 are rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions for analogous reasons as discussed above with respect to the common elements of Claims 2-7 and 28-31 in Section VI.A. In relation to the common elements of Claims 9-14 and 32-35, ChoiceNet teaches or renders obvious a system comprising:

*a database with entries correlating each of a plurality of user IDs with an individualized rule set.* This language is identical to the language in the limitation identified as (a) above in Section VI.A. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches “the PortMaster requests the RADIUS server to authenticate the user” and “[t]he RADIUS server searches its user database.” *ChoiceNet™ Administrator’s Guide* 1-6, fig. 1-2. Moreover, “[o]ne of the reply items [from the RADIUS server] is the *Filter-Id* that

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

associates a filter with the user.” *ChoiceNet* 1-6 (emphasis original). Thus, ChoiceNet teaches a database with entries correlating a user with a filter, which is the individualized rule set in the limitation.

***a dial-up network server that receives user IDs from users’ computers:*** This language is identical to the language in the limitation identified as (b) above in Section VI.A. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

Figure 1-2 (Diagram 18) from ChoiceNet teaches a subscriber connecting to the PortMaster through a dial-up connection. Furthermore, the PortMaster receives a user ID (or username) and password from the user’s computer (Dial-in user 1 in the figure). *ChoiceNet* fig. 1-2. Thus, the PortMaster from ChoiceNet corresponds to the dial-up network server in the limitation and the PortMaster receives user IDs from users’ computers.

***a redirection server connected to the dial-up network server and a public network:*** This language is identical to the language in the limitation identified as (c) above in Section VI.A. Thus, according to the discussion above in those sections and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that “ChoiceNet clients communicate with the ChoiceNet server to determine user access.” *ChoiceNet* 1-1. It further teaches that ChoiceNet clients can run on FireWall IRX Routers, as illustrated in Diagram 17 above. *Id.* “A ChoiceNet filter contains a list of rules” and “[a] ChoiceNet client executes the rules from the top down as they are presented in the filter text file.” *Id.* at 1-4. Thus, the system running a ChoiceNet client, such as the FireWall IRX Router in Diagram 17, corresponds to the redirection server in the limitation.

In Diagram 19 the FireWall IRX (corresponding to the redirection server) is connected *between* the PortMaster (corresponding to the dial-up network server) and the Worldwide Internet (corresponding to the public network). Therefore, each element of the above recited limitation is taught or rendered obvious by ChoiceNet.

***an authentication accounting server connected to the database, the dial-up network server and the redirection server:*** This language is identical to the language in the limitation identified as (d) above in Section VI.A. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

ChoiceNet teaches that the RADIUS Server authenticates a user based on their username and password by checking a user database. *ChoiceNet* 1-6. The RADIUS Server is connected to the FireWall IRX and the PortMaster. *Id.* Therefore, ChoiceNet teaches an authentication accounting server (the RADIUS Server) connected to the database, the dial-up network server (the PortMaster) and the redirection server (the FireWall IRX Router).

***a method comprising the steps of: communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server:*** This language is identical to the language in the limitation identified as (e) above in Section VI.A., except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that “a dial-in user logs in to a PortMaster.... [T]he PortMaster requests the RADIUS server to authenticate the user. The RADIUS server searches its user database.” *ChoiceNet* 1-6; fig. 1-2. The PortMaster (corresponding to the dial-up network server) receives the username and password directly from the dial-in user for authentication purposes and communicates that information to the RADIUS server (corresponding to the authentication accounting server). *See id.* Communication between the PortMaster and the RADIUS server includes the transmission of IP packets, which contain network address information. *Id.* at 5-5. Thus, the PortMaster passes the network address to the RADIUS server along with the user ID to complete the authentication process. Therefore, each element of the above recited claim is taught or is rendered obvious by ChoiceNet.

***communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server:*** This language is identical to the language in the limitation identified as (f) above in Section VI.A. except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that the RADIUS server replies to an authentication request with “the *Filter-Id* that associates a filter with the user.” *Id.* at 1-6. The RADIUS server sends filter

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

information to the system running a ChoiceNet client. *See id.* at 1-6 to 1-7, 5-10; fig. 1-3. The FireWall IRX Router can run the ChoiceNet client, and can thus apply the filter rules. *See id.* at 1-1. Therefore, the RADIUS server (corresponding to the authentication accounting server) communicates filter rules associated with a user to the FireWall IRX Router running a ChoiceNet client (corresponding to the redirection server).

Furthermore, filter rules can be based on source or destination IP addresses, which the ChoiceNet client must know. *See id.* at 5-1. Thus, in addition to the user ID, the network address must be communicated to the redirection server. Therefore, each element of the above recited claim is taught or is rendered obvious by ChoiceNet.

***processing data directed toward the public network from the one of the users' computers according to the individualized rule set:*** This language is identical to the language in the limitation identified as (g) above in Section VI.A. except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that “the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7. The PortMaster is running the ChoiceNet client in the above description, but the ChoiceNet client can also run on the FireWall IRX Router. *See id.* at 1-1. Therefore, the ChoiceNet client running on the FireWall IRX Router applies the filter rules to data directed toward the Internet.

**2. The Combination of ChoiceNet, Zenchelsky, and the Patent Owner's Admissions Renders the Common Elements of Claims 9-14 and 32-35 Obvious**

ChoiceNet may not teach the following two elements of Claims 9-14 and 32-35:

1. A redirection server that performs redirection as well as blocking; and
2. A dial-up network server that communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication and accounting server.

For reasons analogous to those described in Section VI.A.3., these differences between ChoiceNet and the common elements of Claims 9-14 and 32-35 would have been obvious

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

modifications to one of ordinary skill in the art at the time of the invention, in view of Zenchelsky and the Patent Owner's admissions of prior art.

In regard to the first of the noted limitations, the Board has determined that it would have been obvious to modify a ChoiceNet client, such as one running on the FireWall IRX Router of ChoiceNet, to perform redirection as well as permitting or denying access to the user. The Board stated that, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Because a ChoiceNet client can be configured as a control to block the user, it would have been obvious to alter it to redirect the user as well. Thus, the server in ChoiceNet running a ChoiceNet client renders obvious a redirection server that performs redirection as well as blocking.

In regard to the second of the noted limitations, to the extent the examiner does not find that ChoiceNet teaches that "the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server," ChoiceNet combined with Zenchelsky and the Patent Owner's admissions does.

In the '118 Patent, the Patent Owner admits that in "prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server 104." *Col. 1 ll. 21-24*. Thus, by the Patent Owner's admission, this limitation was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and communicating using IP addresses and that this teaching was within the prior art as admitted by the Patent Owner in the Background section of the '118 Patent.

**3. Claim 9**

In addition to the common elements described above, Claim 9 contains the following limitation:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.* Claim 9 is analogous to Claim 2, and for reasons analogous to those described in Section VI.A.4., Claim 9 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

ChoiceNet teaches that "filter rules [can be written] to specify a site list in place of an IP address.... Each site list is a text file that contains the hostnames or IP addresses of hosts for which access is controlled. The rule can permit or deny access by hosts on the list or to hosts on the list." *ChoiceNet* 1-3. ChoiceNet also teaches a redirection server that "searches the Filter Table for the filters specified by Filter-Id in the user entry. If the filters are present in the Filter Table, then they are applied to the connection." *Id.* at 1-6. Thus, ChoiceNet teaches filter rules implemented by a redirection server that control a plurality of data to and from a user computer.

Therefore, Requestor respectfully submits that Claim 9 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**4. Claim 10**

In addition to the common elements described above, Claim 10 contains the following limitation:

*further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.* Claim 10 is analogous to Claim 3, and for reasons analogous to those described in Section VI.A.5., Claim 10 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

ChoiceNet teaches that the system "enables both inbound and outbound traffic filtering for each interface and user." *ChoiceNet* 1-2. In addition, ChoiceNet teaches that "the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule." *Id.* at 1-7; figure 1-4. As described above, the PortMaster running the ChoiceNet client acts as the redirection server in the '118 Patent. The ChoiceNet client can deny traffic to and from a user's computer based on input filter rules. The input filter rules correspond to the individualized rule set of the '118 Patent. Therefore, ChoiceNet teaches a redirection server that blocks data to and from the users' computers as a function of the individualized rule set.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Therefore, Requestor respectfully submits that Claim 10 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**5. Claim 11**

In addition to the common elements described above, Claim 11 contains the following limitation:

*further including the step of allowing the data to and from the users' computers as a function of the individualized rule set:* Claim 11 is analogous to Claim 4, and for reasons analogous to those described in Section VI.A.6., Claim 11 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

ChoiceNet teaches that the system "enables both inbound and outbound traffic filtering for each interface and user." *ChoiceNet* 1-2. In addition, ChoiceNet teaches that "the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule." *Id.* at 1-7; figure 1-4. As described above, the PortMaster running the ChoiceNet client acts as the redirection server in the '118 Patent. The ChoiceNet client can permit traffic to and from a user's computer based on input filter rules. The input filter rules correspond to the individualized rule set of the '118 Patent. Therefore, ChoiceNet teaches a redirection server that permits data to and from the users' computers as a function of the individualized rule set.

Therefore, Requestor respectfully submits that Claim 11 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**6. Claim 12**

In addition to the common elements described above, Claim 12 contains the following limitation:

*further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set:* Claim 12 is analogous to Claim 5, and for reasons analogous to those described in Section VI.A.7., Claim 12 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

ChoiceNet teaches a system that controls access to a user by blocking data based on filter rules: "the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7; figure 1-4. As discussed in Section IV.F., the Board declared that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user” and “redirection would have been an obvious extension of blocking.” *Linksmart Wireless*, No. 2011-009566, at 9, 10. Based on the statement by the Board, it would have been obvious to modify the system in ChoiceNet to redirect data to and from a user’s computer as a function of filter rules.

Therefore, Requestor respectfully submits that Claim 12 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**7. Claim 13**

In addition to the common elements described above, Claim 13 contains the following limitation:

***further including the step of redirecting the data from the users’ computers to multiple destinations a function of the individualized rule set.*** Claim 13 is analogous to Claim 6, and for reasons analogous to those described in Section VI.A.8., Claim 13 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

Requestor respectfully submits that, given its broadest reasonable interpretation, Claim 13 encompasses at least a redirection server that redirects some data to one destination based on one rule, another destination based on another rule, and so on. ChoiceNet teaches filter rules that “specify a site list in place of an IP address.... Each site list is a text file that contains the hostnames or IP addresses of hosts for which access is controlled. The rule can permit or deny access by hosts on the list or to hosts on the list.” *ChoiceNet* 1-3. Thus, ChoiceNet teaches filters that can specify multiple rules, each rule directed to unique destinations. As discussed in Section IV.F., the Board stated that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system of ChoiceNet that blocks and allows data to multiple destinations to perform redirection to multiple destinations.

Therefore, Requestor respectfully submits that Claim 13 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**8. Claim 14**

In addition to the common elements described above, Claim 14 contains the following limitation:

*further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set:* Claim 14 is analogous to Claim 7, and for reasons analogous to those described in Section VI.A.9., Claim 14 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

ChoiceNet teaches that a filter rule can be specified for a user by "defin[ing] the *Filter-Id* reply item in [the user's] RADIUS entry as the filter name" where "*Filter-Id* is a reply item that identifies the filter to be associated with that user." *ChoiceNet* 5-14, 5-10. By defining the same *Filter-Id* in multiple users' RADIUS entries, ChoiceNet teaches that multiple users can be correlated with a common rule set. *See id.* at 5-10, 5-15. For example, ChoiceNet teaches that an "ISP can customize access to sites or services for groups of subscribers that share similar interests" through the use of filter rules. *Id.* at 5-10. Thus, multiple users can be correlated with a common rule set.

Therefore, Requestor respectfully submits that Claim 14 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

#### **9. Claim 32**

In addition to the common elements described above, Claim 32 contains the following limitation:

*wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service:* Claim 32 is analogous to Claim 28, and for reasons analogous to those described in Section VI.A.10., Claim 32 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11.* Furthermore, the '118 Patent declares that IP "[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header." *Col. 2 ll. 11-13.* ChoiceNet teaches that "[p]ackets can be filtered according to...source and destination port numbers to control access to certain network services." *ChoiceNet* 5-6; *see also ChoiceNet* Appx. C (listing common port numbers assigned to TCP and UDP services). Thus, ChoiceNet teaches filtering based on a type of IP service by specifying a source or destination port in the filter rule.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, "redirection is not limited to WWW traffic, and the concept is valid for all IP services." *Col. 1 ll. 41-42*; see *Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the system in ChoiceNet to filter based on IP service.

Therefore, Requestor respectfully submits that Claim 32 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**10. Claim 34**

In addition to the common elements described above, Claim 34 contains the following limitation:

*wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address*: Claim 34 is analogous to Claim 30, and for reasons analogous to those described in Section VI.A.11., Claim 34 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

The '118 Patent gives examples of "request type" as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36*. Therefore, the broadest reasonable interpretation of request type includes http requests. ChoiceNet teaches that filters can be implemented based on port numbers which correlate to IP services: "Rules can use the source and destination port numbers to control access to certain network services." *ChoiceNet* 5-6. For example, in Appendix C in the ChoiceNet reference, port 80 is associated with "World Wide Web Hypertext Transfer Protocol (HTTP)." In an example filter rule, access is permitted for "Web access via HTTP to the addresses in the site list **wwwok**." *Id.* at 5-9, fig. 8, Table 5-1. Furthermore, ChoiceNet teaches "[a] rule can evaluate either the source or destination address of a packet." *Id.* at 5-6. Thus, ChoiceNet teaches filter rules that allow access based on a request type and destination address.

Therefore, Requestor respectfully submits that Claim 34 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**11. Claim 35**

In addition to the common elements described above, Claim 35 contains the following limitation:

*wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address*: Claim

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

35 is analogous to Claim 31, and for reasons analogous to those described in Section VI.A.12., Claim 35 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

Claim 31 is identical to Claim 30 described above, except that Claim 31 is directed to "redirecting the data to a new destination address" instead of "allowing access" based on a request type and an attempted destination address. ChoiceNet teaches permitting or denying access based on a request type and destination address, as discussed above in Sections VI.A.11 and VI.B.10. In the Prior Reexamination, the Board declared, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to redirect data based on a request type and destination address.

Therefore, Requestor respectfully submits that Claim 35 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**C. Claims 16-24, 36, and 38-39 Are Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's Admissions**

**1. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of ChoiceNet in relation to canceled Claim 15 which forms the common elements of Claims 16-24 and 36-39. Each limitation has been identified using letters (a) through (d) for ease of description and for later reference. In the Prior Reexamination, the Board found Claim 15 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. Each of claims 16-24 and 36-39 add limitations to Claim 15. As described in more detail below, these limitations would have been obvious in view of ChoiceNet and the prior art at the time of invention, as admitted by the Patent Owner and demonstrated by Zenchelsky. In relation to the common elements of Claims 16-24 and 36-39, ChoiceNet teaches or renders obvious a system comprising:

***(a) a redirection server connected between a user computer and a public network, the redirection server programmed with a user's rule set correlated to a temporarily assigned network address:*** ChoiceNet teaches that a "*Filter-Id* that associates a filter with the user" is sent to the PortMaster from the RADIUS server. *ChoiceNet* at 1-6; fig. 1-2. ChoiceNet also teaches that when a user attempts to access a site, "[t]he PortMaster compares the access request against the input filter rules. If the request matches the rule, the PortMaster takes the action—permit or deny—specified in the rule." *Id.* at 1-7; fig. 1-4. Thus, the PortMaster corresponds to

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

the redirection server which can be programmed with a user's rule set based on the filter sent from the RADIUS server.

Furthermore, ChoiceNet teaches that "ChoiceNet clients communicate with the ChoiceNet server to determine user access" and that ChoiceNet clients can be FireWall IRX Routers. *Id.* at 1-1; fig. 5-10. In figure 5-10, Diagram 19, the FireWall IRX Router (corresponding to the redirection server) is connected between a user computer and the Worldwide Internet (corresponding to the public network).

Additionally, the communication between the server running the ChoiceNet client and the RADIUS server includes the transmission of IP packets, which contain source and destination network address information. *Id.* at 5-5. Thus, the ChoiceNet client passes the network address to the RADIUS server along with the user ID to complete the authentication process. *See id.* Therefore, a filter is associated with a user which is associated with a network address.

***(b) wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network:*** ChoiceNet teaches that the PortMaster permits or denies a user's access request based on filter rules. *See id.* at 1-7; fig. 1-4. Thus, based on the rules, the PortMaster uses a plurality of functions (permit or deny) to control data passing between the user and the public network.

***(c) wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address:*** ChoiceNet teaches that the ChoiceNet client runs a **filterd** process which can automatically update filter rules based on changes in a filter directory. *See id.* at 2-8, 5-8. Moreover, "ChoiceNet can download filters from the server dynamically—on demand—to asynchronous and synchronous interfaces." *Id.* at 1-3. Thus, the redirection server running the ChoiceNet client allows dynamic and automated modification of filters which are associated with users.

***(d) wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses:*** ChoiceNet teaches that rule sets can be dynamically updated and modified by an administrator. *Id.* at 5-7; *see also id.* at 1-3, 2-8, 5-8. The PortMaster can update a local cache of the rule set based on the result of applying filters from a server in response to a user access request. *See id.* at 1-7; fig. 1-4. Furthermore, the Board stated that "blocking a website based on these bases [time, data, or location] would have

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29.

**2. The Combination of ChoiceNet, Zenchelsky, and the Patent Owner’s Admissions Renders the Common Elements of Claims 16-24 and 36-39 Obvious**

ChoiceNet may not teach the following two elements of Claims 16-24 and 36-39:

1. A redirection server that performs redirection as well as blocking; and
2. A user’s rule set correlated to a temporarily assigned network address.

However, these differences between ChoiceNet and the claims would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner’s admissions of prior art.

In regard to the first of the noted limitations, the Board stated that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Because a ChoiceNet client can be configured as a control to block the user, it would have been obvious to alter it to redirect the user as well. Thus, the PortMaster or the FireWall IRX Router running the ChoiceNet client corresponds to the redirection server of the ’118 Patent because it applies filter rules to permit or deny access to users and it would have been obvious to alter its functionality to perform redirection.

In regard to the second of the noted limitations, to the extent the examiner does not find that ChoiceNet teaches “a user’s rule set correlated to a temporarily assigned network address,” ChoiceNet combined with Zenchelsky and the Patent Owner’s admissions does.

In the ’118 Patent, the Patent Owner admits that in “prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP’s authentication and accounting server 104.” *Col. 1 ll. 21-24*. Additionally, the Patent Owner admits that “the end user would be identified by the temporarily assigned IP address.” *Col. 1 ll. 35-37*. Thus, by the Patent Owner’s admission, identifying a user with a temporarily assigned IP address was known in the prior art at the time of the invention.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and identifying a user with the temporary IP address and that this teaching was within the prior art as admitted by the Patent Owner in the background section of the '118 Patent. Thus, ChoiceNet, in view of Zenchelsky and the Patent Owner's Admissions, renders obvious a user's rule set correlated to a temporarily assigned network address.

**3. Claim 16**

In addition to common elements (a) through (d) described above, Claim 16 contains the following limitation:

*wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time:* Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of "modification" of a portion of a rule set because updating a rule set can change or modify a rule.

As taught in ChoiceNet, an administrator "can create or modify ChoiceNet filters at any time, independent of any active packet filters." *ChoiceNet* at 5-7. ChoiceNet also teaches that an administrator can change rule sets at any time by modifying files, modifications which would then be implemented by the redirection server: "A few days later, suppose you modify the **deny\_list** file and add two new lists, **no\_go** and **permit\_list**, as shown in Figure 5-5. When you run **buildlist** now, it updates and generates the files as shown in Figure 5-6." *Id.* at 5-4; figs. 5-5, 5-6 (emphasis original). Thus, ChoiceNet teaches modifying rules as a function of time. Furthermore, the Board stated that "blocking a website based on these bases [as a function of time, data sent or received, or location accessed] would have been obvious" to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, the Board declared that it would have been obvious to "block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work." *Id.* at fn.29. Based on the statements by the Board, it would have been obvious to modify the system in ChoiceNet to be configured to allow portions of rule sets to be modified as a function of time.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 16 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**4. Claim 17**

In addition to common elements (a) through (d) described above, Claim 17 contains the following limitation:

*wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user:* Similar to Claim 16 above, Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of "modification" of a portion of a rule set because updating a rule set can change or modify a rule. ChoiceNet teaches that an administrator can change filters and filter rules at any time and for any reason. *See ChoiceNet* 5-4. Choice Net teaches that an "ISP can customize access to sites or services for groups of subscribers that share similar interests." *Id.* at 5-10. As an example, "[o]ne group might be interested in access only to the Web, another in access to role-playing games, another only in sites that are church-related, and another only in sites that relate to business and economics." *Id.* Thus, ChoiceNet teaches filter rules that are based on data transmitted to or from the user. Moreover, as stated above regarding Claim 16, the Board declared that modifying rule sets based on data transmitted to or from the user would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the system in ChoiceNet to allow modification of rules as a function of data the user sends or receives.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 17 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**5. Claim 18**

In addition to common elements (a) through (d) described above, Claim 18 contains the following limitation:

*wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses:* Similar to Claim 16, Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of "modification" of a portion of a rule set because updating a rule set can change or modify a rule. ChoiceNet teaches that an administrator can change filters at any time and for any reason. *See ChoiceNet* 5-4. In addition, filter rules on the redirection server

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

can be changed and updated based on a site request. *See id.* at 1-7. For example, “the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules.... If a rule specifies a site list, the PortMaster sends a request to the ChoiceNet server to determine whether the site is on that list.... The PortMaster caches the answer for future use.” *Id.*; *see id.* fig. 1-4. Thus, ChoiceNet teaches a server that can update a local cache of filter rules based on a site request from a user. Moreover, as stated above regarding Claim 16, the Board declared that modifying rule sets based on the location or locations the user accesses would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the PortMaster in ChoiceNet to allow modification of rules as a function of locations the user attempts to access.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 18 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**6. Claim 19**

In addition to common elements (a) through (d) described above, Claim 19 contains the following limitation:

*wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time:* The difference between Claim 16 and Claim 19 is that the limitation in Claim 16 states a portion of the rule set can be modified as a function of time and the limitation in Claim 19 states a portion of the rule set can be removed or reinstated as a function of time. Thus, the difference between Claims 16 and 19 is a change from “modification” to “removal or reinstatement.” Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of “removal or reinstatement” of a portion of a rule set because updating a rule set can remove or reinstate a rule.

As taught in ChoiceNet, an administrator “can create or modify ChoiceNet filters at any time, independent of any active packet filters.” *ChoiceNet* at 5-7. ChoiceNet also teaches that an administrator can change rule sets at any time by adding, deleting, or modifying files, modifications which would then be implemented by the redirection server: “A few days later, suppose you modify the **deny\_list** file and add two new lists, **no\_go** and **permit\_list**, as shown in Figure 5-5. When you run **buildlist** now, it updates and generates the files as shown in Figure 5-6.” *Id.* at 5-4; figs. 5-5, 5-6 (emphasis original). Thus, ChoiceNet teaches modifying,

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

removing, or reinstating rules as a function of time. Furthermore, the Board stated that “blocking a website based on these bases [as a function of time, data sent or received, or location accessed] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, the Board declared that it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Based on the statements by the Board, it would have been obvious to modify the server in ChoiceNet to be configured to allow portions of rule sets to be removed or reinstated as a function of time.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 19 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**7. Claim 20**

In addition to common elements (a) through (d) described above, Claim 20 contains the following limitation:

***wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user:*** Similar to Claims 16 and 19 above, the difference between Claims 17 and 20 is the change of the word “modification” to the words “removal or reinstatement.” ChoiceNet teaches that an administrator can change filters and filter rules at any time and for any reason. *See ChoiceNet* 5-4. Choice Net teaches that an “ISP can customize access to sites or services for groups of subscribers that share similar interests.” *Id.* at 5-10. As an example, “[o]ne group might be interested in access only to the Web, another in access to role-playing games, another only in sites that are church-related, and another only in sites that relate to business and economics.” *Id.* Thus, ChoiceNet teaches filter rules that are based on data transmitted to or from the user. Moreover, as stated above regarding Claim 16, the Board declared that modifying rule sets based on data transmitted to or from the user would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the system in ChoiceNet to allow removal or reinstatement of rules as a function of data the user sends or receives.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 20 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**8. Claim 21**

In addition to common elements (a) through (d) described above, Claim 21 contains the following limitation:

*wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses:* Similar to Claims 16 and 19 above, Claims 18 and 21 differ only in the change of the word “modification” to the words “removal or reinstatement.” ChoiceNet teaches that an administrator can change filters at any time and for any reason. *See ChoiceNet* 5-4. In addition, filter rules on the redirection server can be changed and updated based on a site request. *See id.* at 1-7. For example, “the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules.... If a rule specifies a site list, the PortMaster sends a request to the ChoiceNet server to determine whether the site is on that list.... The PortMaster caches the answer for future use.” *Id.*; *see id.* fig. 1-4. Thus, ChoiceNet teaches a server that can update a local cache of filter rules based on a site request from a user. Moreover, as stated above regarding Claim 16, the Board declared that modifying rule sets based on the location or locations the user accesses would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the PortMaster in ChoiceNet to allow removal or reinstatement of rules as a function of locations the user attempts to access.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 21 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**9. Claim 22**

In addition to common elements (a) through (d) described above, Claim 22 contains the following limitation:

*wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses:* ChoiceNet teaches a redirection server (the server running a ChoiceNet client) that can filter user requests based on a location requested. *See ChoiceNet* 1-7. ChoiceNet also teaches that filter rules can be implemented based on the nature of the content of communication. *See id.* at 5-10. ChoiceNet also teaches that rules can be modified at any time and updated dynamically. *See id.* at 5-4. Thus, ChoiceNet

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

teaches a redirection server that allows the modification, removal, or reinstatement of rules based on at least one of time, data communicated, and location accessed. Furthermore, the Board stated that “blocking a website based on these bases [time, data, or location] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the system in ChoiceNet to allow the modification, removal, or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 22 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**10. Claim 23**

In addition to common elements (a) through (d) described above, Claim 23 contains the following limitation:

*wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server:* ChoiceNet teaches in figure 5-10 (Diagram 19) a FireWall IRX Router, acting as the redirection server, connected to a user through the PortMaster on a user side and the Worldwide Internet, RADIUS server, and ChoiceNet server on a network side. *ChoiceNet* figs. 5-10, 5-12. The user computer’s only route to the Worldwide Internet (corresponding to the computer network) is through the FireWall IRX Router. *See id.* As described above in Sections VI.A.2. and VI.A.3., ChoiceNet in combination with Zenchelsky and the Patent Owner’s admissions renders obvious a user computer using a temporarily assigned network address. It would have been obvious to modify the computer in ChoiceNet to be associated with a temporary network address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 23 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**11. Claim 24**

Claim 24 depends from Claim 24:

*The system of claim 23 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server:* ChoiceNet teaches “[w]hen a user dials in to the network, if the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

appropriate filter does not reside locally on the client, the client sends a request to the ChoiceNet server to look up the filter. If the name of the filter assigned to the interface matches a filter defined on the ChoiceNet server, the filter is downloaded to the client.” *ChoiceNet* 1-3. ChoiceNet also teaches that “ChoiceNet can download filters from the server dynamically.” *Id.* As illustrated in Fig. 5-10, the ChoiceNet server resides on the network side of the FireWall IRX Router. Thus, ChoiceNet teaches a redirection server with rules that can be modified through instructions received from the network side of the redirection server.

Furthermore, ChoiceNet teaches that administrators can “can create or modify ChoiceNet filters at any time, independent of any active packet filters.” *Id.* at 5-7; *see id.* at 5-4. Modifying filters includes changing files on a ChoiceNet server. *Id.* Thus, changes made to filter rules on the ChoiceNet server propagate to the redirection server based on instructions from the network side of the server.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 24 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**12. Claim 36**

In addition to common elements (a) through (d) described above, Claim 36 contains the following limitation:

***wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service:*** The ’118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11.* Furthermore, the ’118 Patent declares that IP “[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header.” *Col. 2 ll. 11-13.* ChoiceNet teaches that “[p]ackets can be filtered according to...source and destination port numbers to control access to certain network services.” *ChoiceNet* 5-6; *see also ChoiceNet* Appx. C (listing common port numbers assigned to TCP and UDP services). Thus, ChoiceNet teaches filtering based on a type of IP service by specifying a source or destination port in the filter rule.

In addition, as the Patent Owner admitted in the ’118 Patent and the Board recognized, “redirection is not limited to WWW traffic, and the concept is valid for all IP services.” *Col. 1 ll. 41-42; see Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the system in ChoiceNet to filter based on IP service.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 36 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**13. Claim 38**

In addition to common elements (a) through (d) described above, Claim 38 contains the following limitation:

*wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address:* The '118 Patent gives examples of "request type" as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36.* Therefore, the broadest reasonable interpretation of request type includes http requests. ChoiceNet teaches that filters can be implemented based on port numbers which correlate to IP services: "Rules can use the source and destination port numbers to control access to certain network services." *ChoiceNet* 5-6. For example, in Appendix C in the ChoiceNet reference, port 80 is associated with "World Wide Web Hypertext Transfer Protocol (HTTP)." In an example filter rule, access is permitted for "Web access via HTTP to the addresses in the site list **wwwok**." *Id.* at 5-9, fig. 8, Table 5-1. Furthermore, ChoiceNet teaches "[a] rule can evaluate either the source or destination address of a packet." *Id.* at 5-6. Thus, ChoiceNet teaches filter rules that allow access based on a request type and destination address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 38 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**14. Claim 39**

In addition to common elements (a) through (d) described above, Claim 39 contains the following limitation:

*wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address:* Claim 39 is identical to Claim 38 described above, except that Claim 39 here is directed to "redirecting the data to a new destination address" instead of "allowing access" based on a request type and an attempted destination address. ChoiceNet teaches permitting or denying access based on a request type and destination address, as discussed above in Section VI.C.13. In the Prior Reexamination, the Board declared, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to redirect data based on a request type and destination address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 39 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**D. Claims 26-27, 40, and 42-43 Are Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's Admissions**

**1. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of ChoiceNet in relation to canceled Claim 25 which forms the common elements of Claims 26-27 and 40-43. In the Prior Reexamination, the Board found Claim 25 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. Each of claims 26-27 and 40-43 add limitations to Claim 25. As described in more detail below, these limitations would have been obvious in view of ChoiceNet and the prior art at the time of invention, as admitted by the Patent Owner and demonstrated by Zenchelsky. The Appendix features claim charts of Claims 26-27 and 40-43 which shows that each limitation is present in ChoiceNet when combined with Zenchelsky and the Patent Owner's admissions in the '118 Patent. In relation to the common elements of Claims 26-27 and 40-43, ChoiceNet teaches or renders obvious a system comprising:

*a redirection server connected between a user computer and a public network, the redirection server containing a user's rule set correlated to a temporarily assigned network address*: This language is identical to the language in the limitation in the common elements of Claims 16-24 and 36-39 identified as (a) in Section VI.C.1., except for one non-substantive change in the language. The limitation in the common elements of Claims 16-24 and 36-39 states "the redirection server *programmed* with a user's rule set" and the limitation here states "the redirection server *containing* a user's rule set." Therefore, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that a "*Filter-Id* that associates a filter with the user" is sent to the PortMaster from the RADIUS server. *ChoiceNet* at 1-6; fig. 1-2. ChoiceNet also teaches that when a user attempts to access a site, "[t]he PortMaster compares the access request against the input filter rules. If the request matches the rule, the PortMaster takes the action—permit or deny—specified in the rule." *Id.* at 1-7; fig. 1-4. Thus, the PortMaster corresponds to the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

redirection server which can be programmed with a user's rule set based on the filter sent from the RADIUS server.

Furthermore, ChoiceNet teaches that "ChoiceNet clients communicate with the ChoiceNet server to determine user access" and that ChoiceNet clients can be FireWall IRX Routers. *Id.* at 1-1; fig. 5-10. In figure 5-10, Diagram 19, the FireWall IRX Router (corresponding to the redirection server) is connected between a user computer and the Worldwide Internet (corresponding to the public network).

Additionally, the communication between the server running the ChoiceNet client and the RADIUS server includes the transmission of IP packets, which contain source and destination network address information. *Id.* at 5-5. Thus, the ChoiceNet client passes the network address to the RADIUS server along with the user ID to complete the authentication process. *See id.* Therefore, a filter is associated with a user which is associated with a network address.

*wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network:* This language is identical to the language in the limitation in the common elements of Claims 16-24 and 36-39 identified as (b) in Section VI.C.1. Therefore, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that the PortMaster permits or denies a user's access request based on filter rules. *See id.* at 1-7; fig. 1-4. Thus, based on the rules, the PortMaster uses a plurality of functions (permit or deny) to control data passing between the user and the public network.

*the method comprising the step of: modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server:* This language is identical to the language in the limitation in the common elements of Claims 16-24 and 36-39 identified as (c) in Section VI.C.1., except that the form of the limitation has been changed to be a step in a method rather than functionality in a system. Therefore, according to the discussion above and for analogous reasons, this limitation is taught or rendered obvious by ChoiceNet.

ChoiceNet teaches that the ChoiceNet client runs a **filterd** process which can automatically update filter rules based on changes in a filter directory. *See id.* at 2-8, 5-8. Moreover, "ChoiceNet can download filters from the server dynamically—on demand—to asynchronous and synchronous interfaces." *Id.* at 1-3. Thus, the redirection server running the

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

ChoiceNet client allows dynamic and automated modification of filters which are associated with users.

*wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network, and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server:* This language is identical to the language in the limitation in Claim 23, discussed above in Section VI.C.10. Therefore, according to the discussion above and for analogous reasons, this limitation is taught or rendered obvious by ChoiceNet.

ChoiceNet teaches in figure 5-10 (Diagram 19) a FireWall IRX Router, acting as the redirection server, connected to a user through the PortMaster on a user side and the Worldwide Internet, RADIUS server, and ChoiceNet server on a network side. *ChoiceNet* figs. 5-10, 5-12. The user computer's only route to the Worldwide Internet (corresponding to the computer network) is through the FireWall IRX Router. *See id.* As described above in Sections VI.A.2. and VI.A.3., ChoiceNet in combination with Zenchelsky and the Patent Owner's admissions renders obvious a user computer using a temporarily assigned network address. It would have been obvious to modify the computer in ChoiceNet to be associated with a temporary network address.

*and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server:* This limitation is analogous to the limitation in Claim 24, discussed above in Section VI.C.11, except that the form of the limitation has been changed to be a step in a method rather than functionality in a system. Therefore, according to the discussion above and for analogous reasons, this limitation is taught or rendered obvious by ChoiceNet.

ChoiceNet teaches "[w]hen a user dials in to the network, if the appropriate filter does not reside locally on the client, the client sends a request to the ChoiceNet server to look up the filter. If the name of the filter assigned to the interface matches a filter defined on the ChoiceNet server, the filter is downloaded to the client." *ChoiceNet* 1-3. ChoiceNet also teaches that "ChoiceNet can download filters from the server dynamically." *Id.* As illustrated in Fig. 5-10, the ChoiceNet server resides on the network side of the FireWall IRX Router. Thus, ChoiceNet

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

teaches a redirection server with rules that can be modified through instructions received from the network side of the redirection server.

Furthermore, ChoiceNet teaches that administrators can “can create or modify ChoiceNet filters at any time, independent of any active packet filters.” *Id.* at 5-7; *see id.* at 5-4. Modifying filters includes changing files on a ChoiceNet server. *Id.* Thus, changes made to filter rules on the ChoiceNet server propagate to the redirection server based on instructions from the network side of the server.

**2. The Combination of ChoiceNet, Zenchelsky, and the Patent Owner’s Admissions Renders the Common Elements of Claims 26-27 and 40-43 Obvious**

ChoiceNet may not teach the following two elements of Claims 26-27 and 40-43:

1. A redirection server that performs redirection as well as blocking; and
2. A user’s rule set correlated to a temporarily assigned network address.

However, these differences between ChoiceNet and the claims would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner’s admissions of prior art.

In regard to the first of the noted limitations, the Board stated that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Because a ChoiceNet client can be configured as a control to block the user, it would have been obvious to alter it to redirect the user as well. Thus, the PortMaster or the FireWall IRX Router running the ChoiceNet client corresponds to the redirection server of the ’118 Patent because it applies filter rules to permit or deny access to users and it would have been obvious to alter its functionality to perform redirection.

In regard to the second of the noted limitations, to the extent the examiner does not find that ChoiceNet teaches “a user’s rule set correlated to a temporarily assigned network address,” ChoiceNet combined with Zenchelsky and the Patent Owner’s admissions does.

In the ’118 Patent, the Patent Owner admits that in “prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP’s authentication and accounting server 104.” *Col. 1 ll. 21-24*. Additionally, the Patent Owner admits that “the end user would be identified by

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

the temporarily assigned IP address.” *Col. 1 ll. 35-37*. Thus, by the Patent Owner’s admission, identifying a user with a temporarily assigned IP address was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and identifying a user with the temporary IP address and that this teaching was within the prior art as admitted by the Patent Owner in the background section of the ’118 Patent. Thus, ChoiceNet, in view of Zenchelsky and the Patent Owner’s Admissions, renders obvious a user’s rule set correlated to a temporarily assigned network address.

**3. Claim 26**

In addition to the common elements described above, Claim 26 contains the following limitation:

*further including the step of modifying at least a portion of the user’s rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses:* Claim 26 is analogous to Claim 22, and for reasons analogous to those described in Section VI.C.9, Claim 26 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

ChoiceNet teaches a redirection server (the server running a ChoiceNet client) that can filter user requests based on a location requested. *See ChoiceNet* 1-7. ChoiceNet also teaches that filter rules can be implemented based on the nature of the content of communication. *See id.* at 5-10. ChoiceNet also teaches that rules can be modified at any time and updated dynamically. *See id.* at 5-4. Thus, ChoiceNet teaches a redirection server that allows the modification, removal, or reinstatement of rules based on at least one of time, data communicated, and location accessed. Furthermore, the Board stated that “blocking a website based on these bases [time, data, or location] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the system in ChoiceNet to allow the modification, removal, or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 26 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**4. Claim 27**

In addition to the common elements described above, Claim 27 contains the following limitation:

*further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and the location or locations the user accesses:* Claim 27 is analogous to Claim 22, and for reasons analogous to those described in Section VI.C.9, Claim 27 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

ChoiceNet teaches a redirection server (the server running a ChoiceNet client) that can filter user requests based on a location requested. *See ChoiceNet* 1-7. ChoiceNet also teaches that filter rules can be implemented based on the nature of the content of communication. *See id.* at 5-10. ChoiceNet also teaches that rules can be modified at any time and updated dynamically. *See id.* at 5-4. Thus, ChoiceNet teaches a redirection server that allows the modification, removal, or reinstatement of rules based on at least one of time, data communicated, and location accessed. Furthermore, the Board stated that "blocking a website based on these bases [time, data, or location] would have been obvious" to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the system in ChoiceNet to allow the modification, removal, or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 27 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**5. Claim 40**

In addition to the common elements described above, Claim 40 contains the following limitation:

*wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service:* Claim 40 is analogous to Claim 28, and for reasons analogous to those described in Section VI.A.10., Claim 40 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11*. Furthermore, the '118 Patent declares that IP “[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header.” *Col. 2 ll. 11-13*. ChoiceNet teaches that “[p]ackets can be filtered according to...source and destination port numbers to control access to certain network services.” *ChoiceNet 5-6; see also ChoiceNet Appx. C* (listing common port numbers assigned to TCP and UDP services). Thus, ChoiceNet teaches filtering based on a type of IP service by specifying a source or destination port in the filter rule.

In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, “redirection is not limited to WWW traffic, and the concept is valid for all IP services.” *Col. 1 ll. 41-42; see Linksmart Wireless, No. 2011-009566, at 8, fn.24*. Accordingly, it would have been obvious to modify the system in ChoiceNet to filter based on IP service.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 40 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**6. Claim 42**

In addition to the common elements described above, Claim 42 contains the following limitation:

***wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address:*** Claim 42 is analogous to Claim 30, and for reasons analogous to those described in Section VI.A.11., Claim 42 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

The '118 Patent gives examples of “request type” as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36*. Therefore, the broadest reasonable interpretation of request type includes http requests. ChoiceNet teaches that filters can be implemented based on port numbers which correlate to IP services: “Rules can use the source and destination port numbers to control access to certain network services.” *ChoiceNet 5-6*. For example, in Appendix C in the ChoiceNet reference, port 80 is associated with “World Wide Web Hypertext Transfer Protocol (HTTP).” In an example filter rule, access is permitted for “Web access via HTTP to the addresses in the site list **wwwok**.” *Id.* at 5-9, fig. 8, Table 5-1. Furthermore, ChoiceNet teaches “[a] rule can evaluate either the source or destination address of

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

a packet.” *Id.* at 5-6. Thus, ChoiceNet teaches filter rules that allow access based on a request type and destination address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 42 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**7. Claim 43**

In addition to the common elements described above, Claim 43 contains the following limitation:

*wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address:* Claim 43 is analogous to Claim 31, and for reasons analogous to those described in Section VI.A.12., Claim 43 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

Furthermore, Claim 43 is identical to Claim 42 described above, except that Claim 43 is directed to “redirecting the data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. ChoiceNet teaches permitting or denying access based on a request type and destination address, as discussed above in Section VI.D.6. In the Prior Reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to redirect data based on a request type and destination address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 43 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**E. Claim 44 Is Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s Admissions**

**1. Overview of Obviousness**

Claim 44 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions in the Background section of the ’118 Patent. In the Prior Reexamination, the Board found Claim 1 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. The Patent Owner stated that Claim 44 corresponds to Claim 1 with language to clarify the “‘between’ location of the redirection server.” Response and Proposed Amendment, at 3. The only difference between canceled Claim 1 and Claim 44 is Claim 1 recites “a redirection server connected *to* the dial-up network server and a public network” (emphasis added), and Claim 44

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

recites “a redirection server connected *between* the dial-up network server and a public network” (emphasis added). ChoiceNet teaches a network topology having a redirection server situated logically between a dial-up network server and a public network, as described below and shown in Diagram 19.

**2. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of ChoiceNet in relation to Claim 44. The elements have been identified below with letters (a) through (g). The Appendix features claim charts of Claim 44 and shows that each limitation is present in ChoiceNet when combined with Zenchelsky and the Patent Owner’s admissions in the ’118 Patent. In relation to each limitation of Claim 44, ChoiceNet teaches or renders obvious a system comprising:

**(a) a database with entries correlating each of a plurality of user IDs with an individualized rule set:** ChoiceNet teaches “the PortMaster requests the RADIUS server to authenticate the user” and “[t]he RADIUS server searches its user database.” *ChoiceNet™ Administrator’s Guide* 1-6, fig. 1-2. Moreover, “[o]ne of the reply items [from the RADIUS server] is the *Filter-Id* that associates a filter with the user.” *ChoiceNet* 1-6 (emphasis original). Thus, ChoiceNet teaches a database with entries correlating a user with a filter, which is the individualized rule set in the limitation.

**(b) a dial-up network server that receives user IDs from users’ computers:** Figure 1-2 from ChoiceNet (Diagram 18) teaches a subscriber connecting to the PortMaster through a dial-up connection. Furthermore, the PortMaster receives a user ID (or username) and password from the user’s computer (Dial-in user 1 in the figure). *ChoiceNet* fig. 1-2. Thus, the PortMaster from ChoiceNet corresponds to the dial-up network server in the limitation and the PortMaster receives user IDs from users’ computers.

**(c) a redirection server connected between the dial-up network server and a public network:** ChoiceNet teaches that “ChoiceNet clients communicate with the ChoiceNet server to determine user access.” *ChoiceNet* 1-1. It further teaches that ChoiceNet clients can run on FireWall IRX Routers, as illustrated in Diagram 17 above. *Id.* “A ChoiceNet filter contains a list of rules” and “[a] ChoiceNet client executes the rules from the top down as they are presented in the filter text file.” *Id.* at 1-4. Thus, the system running a ChoiceNet client, such as the FireWall IRX Router in Diagram 17, corresponds to the redirection server in the limitation.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

In Diagram 19 the FireWall IRX (corresponding to the redirection server) is connected *between* the PortMaster (corresponding to the dial-up network server) and the Worldwide Internet (corresponding to the public network). Therefore, each element of the above recited limitation is taught or rendered obvious by ChoiceNet.

***(d) an authentication accounting server connected to the database, the dial-up network server and the redirection server:*** ChoiceNet teaches that the RADIUS Server authenticates a user based on their username and password by checking a user database. *ChoiceNet* 1-6. The RADIUS Server is connected to the FireWall IRX and the PortMaster. *Id.*, fig. 5-10. Therefore, ChoiceNet teaches an authentication accounting server (the RADIUS Server) connected to the database, the dial-up network server (the PortMaster) and the redirection server (the FireWall IRX Router).

***(e) wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server:*** ChoiceNet teaches that “a dial-in user logs in to a PortMaster.... [T]he PortMaster requests the RADIUS server to authenticate the user. The RADIUS server searches its user database.” *ChoiceNet* 1-6; fig. 1-2. The PortMaster (corresponding to the dial-up network server) receives the username and password directly from the dial-in user for authentication purposes and communicates that information to the RADIUS server (corresponding to the authentication accounting server). *See id.* Communication between the PortMaster and the RADIUS server includes the transmission of IP packets, which contain network address information. *Id.* at 5-5. Thus, the PortMaster passes the network address to the RADIUS server along with the user ID to complete the authentication process. Therefore, each element of the above recited claim is taught or is rendered obvious by ChoiceNet.

***(f) wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server:*** ChoiceNet teaches that the RADIUS server replies to an authentication request with “the *Filter-Id* that associates a filter with the user.” *Id.* at 1-6. The RADIUS server sends filter information to the system running a ChoiceNet client. *See id.* at 1-6 to 1-7, 5-10; fig. 1-3. The FireWall IRX Router can run the ChoiceNet client, and can thus apply the filter rules. *See id.* at 1-1. Therefore, the RADIUS server (corresponding to the authentication accounting server) communicates filter rules

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

associated with a user to the FireWall IRX Router running a ChoiceNet client (corresponding to the redirection server).

Furthermore, filter rules can be based on source or destination IP addresses, which the ChoiceNet client must know. *See id.* at 5-1. Thus, in addition to the user ID, the network address must be communicated to the redirection server. Therefore, each element of the above recited claim is taught or is rendered obvious by ChoiceNet.

*(g) wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set:* ChoiceNet teaches that “the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7. The PortMaster is running the ChoiceNet client in the above description, but the ChoiceNet client can also run on the FireWall IRX Router. *See id.* at 1-1. Therefore, the ChoiceNet client running on the FireWall IRX Router applies the filter rules to data directed toward the Internet.

**3. The Combination of ChoiceNet, Zenchelsky, and the Patent Owner's Admissions Renders Claim 44 Obvious**

ChoiceNet may not teach the following two elements of Claim 44:

1. A redirection server that performs redirection as well as blocking; and
2. A dial-up network server that communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication and accounting server.

However, these differences between ChoiceNet and Claim 44 would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner's admissions of prior art.

In regard to the first of the noted limitations, the Board stated that, in view of the Patent Owner's admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Because a ChoiceNet client can be configured as a control to block the user, it would have been obvious to alter it to redirect the user as well. Thus, the FireWall IRX Router running the ChoiceNet client corresponds to the redirection server of the '118 Patent because it applies filter rules to permit or deny access to users and it would have been obvious to alter its functionality to perform redirection.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

In regard to the second of the noted limitations, to the extent the examiner does not find that ChoiceNet teaches that “the dial-up network server communicates a first user ID for one of the users’ computers and a temporarily assigned network address for the first user ID to the authentication accounting server,” ChoiceNet combined with Zenchelsky and the Patent Owner’s admissions does.

As described above, in the background section of the ’118 Patent, the Patent Owner admits that in “prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP’s authentication and accounting server 104.” *Col. 1 ll. 21-24*. Thus, by the Patent Owner’s admission, this limitation was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and communicating using IP addresses and that this teaching was within the prior art as admitted by the Patent Owner in the Background section of the ’118 Patent.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 44 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**F. Claim 56 Is Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s Admissions**

**1. Detailed Explanation of Obviousness**

Claim 56 is an independent claim that is identical to canceled Claim 8 in the ’118 Patent except that the limitation related to the location of the redirection server has been changed to specify that it is *between* a dial-up network server and a public network. This change is identical to the change made between canceled Claim 1 and Claim 44, discussed above in Section VI.E.1. Claim 56 includes limitations analogous to those in Claim 44, and so Claim 56 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions for analogous reasons as discussed above with respect to Claim 44 in Section VI.E. In relation to Claim 56, ChoiceNet teaches or renders obvious a system comprising:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*a database with entries correlating each of a plurality of user IDs with an individualized rule set:* This language is identical to the language in the limitation identified as (a) above in Sections VI.A. and VI.E. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches “the PortMaster requests the RADIUS server to authenticate the user” and “[t]he RADIUS server searches its user database.” *ChoiceNet™ Administrator’s Guide* 1-6, fig. 1-2. Moreover, “[o]ne of the reply items [from the RADIUS server] is the *Filter-Id* that associates a filter with the user.” *ChoiceNet* 1-6 (emphasis original). Thus, ChoiceNet teaches a database with entries correlating a user with a filter, which is the individualized rule set in the limitation.

*a dial-up network server that receives user IDs from users’ computers:* This language is identical to the language in the limitation identified as (b) above in Sections VI.A. and VI.E. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

Figure 1-2 from ChoiceNet (Diagram 18) teaches a subscriber connecting to the PortMaster through a dial-up connection. Furthermore, the PortMaster receives a user ID (or username) and password from the user’s computer (Dial-in user 1 in the figure). *ChoiceNet* fig. 1-2. Thus, the PortMaster from ChoiceNet corresponds to the dial-up network server in the limitation and the PortMaster receives user IDs from users’ computers.

*a redirection server connected between the dial-up network server and a public network:* This language is identical to the language in the limitation identified as (c) above in Section VI.E. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that “ChoiceNet clients communicate with the ChoiceNet server to determine user access.” *ChoiceNet* 1-1. It further teaches that ChoiceNet clients can run on FireWall IRX Routers, as illustrated in Diagram 17 above. *Id.* “A ChoiceNet filter contains a list of rules” and “[a] ChoiceNet client executes the rules from the top down as they are presented in the filter text file.” *Id.* at 1-4. Thus, the system running a ChoiceNet client, such as the FireWall IRX Router in Diagram 17, corresponds to the redirection server in the limitation.

In Diagram 19 the FireWall IRX (corresponding to the redirection server) is connected *between* the PortMaster (corresponding to the dial-up network server) and the Worldwide

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Internet (corresponding to the public network). Therefore, each element of the above recited limitation is taught or rendered obvious by ChoiceNet.

***an authentication accounting server connected to the database, the dial-up network server and the redirection server:*** This language is identical to the language in the limitation identified as (d) above in Sections VI.A. and VI.E. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that the RADIUS Server authenticates a user based on their username and password by checking a user database. *ChoiceNet* 1-6. The RADIUS Server is connected to the FireWall IRX and the PortMaster. *Id.* Therefore, ChoiceNet teaches an authentication accounting server (the RADIUS Server) connected to the database, the dial-up network server (the PortMaster) and the redirection server (the FireWall IRX Router).

***a method comprising the steps of: communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server:*** This language is identical to the language in the limitation identified as (e) above in Sections VI.A. and VI.E., except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that “a dial-in user logs in to a PortMaster.... [T]he PortMaster requests the RADIUS server to authenticate the user. The RADIUS server searches its user database.” *ChoiceNet* 1-6; fig. 1-2. The PortMaster (corresponding to the dial-up network server) receives the username and password directly from the dial-in user for authentication purposes and communicates that information to the RADIUS server (corresponding to the authentication accounting server). *See id.* Communication between the PortMaster and the RADIUS server includes the transmission of IP packets, which contain network address information. *Id.* at 5-5. Thus, the PortMaster passes the network address to the RADIUS server along with the user ID to complete the authentication process. Therefore, each element of the above recited claim is taught or is rendered obvious by ChoiceNet.

***communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication***

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*accounting server*: This language is identical to the language in the limitation identified as (f) above in Sections VI.A. and VI.E., except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that the RADIUS server replies to an authentication request with “the *Filter-Id* that associates a filter with the user.” *Id.* at 1-6. The RADIUS server sends filter information to the system running a ChoiceNet client. *See id.* at 1-6 to 1-7, 5-10; fig. 1-3. The FireWall IRX Router can run the ChoiceNet client, and can thus apply the filter rules. *See id.* at 1-1. Therefore, the RADIUS server (corresponding to the authentication accounting server) communicates filter rules associated with a user to the FireWall IRX Router running a ChoiceNet client (corresponding to the redirection server).

Furthermore, filter rules can be based on source or destination IP addresses, which the ChoiceNet client must know. *See id.* at 5-1. Thus, in addition to the user ID, the network address must be communicated to the redirection server. Therefore, each element of the above recited claim is taught or is rendered obvious by ChoiceNet.

*processing data directed toward the public network from the one of the users’ computers according to the individualized rule set*: This language is identical to the language in the limitation identified as (g) above in Sections VI.A. and VI.E., except that the form of the limitation has been changed to be a step in a method rather than providing functionality to a system. This change in form does not alter the substance of the limitation. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches that “the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7. The PortMaster is running the ChoiceNet client in the above description, but the ChoiceNet client can also run on the FireWall IRX Router. *See id.* at 1-1. Therefore, the ChoiceNet client running on the FireWall IRX Router applies the filter rules to data directed toward the Internet.

**2. The Combination of ChoiceNet, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 56 Obvious**

ChoiceNet may not teach the following two elements of Claim 56:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

1. A redirection server that performs redirection as well as blocking; and
2. A dial-up network server that communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication and accounting server.

For reasons analogous to those described in Section VI.E.3., these differences between ChoiceNet and Claim 56 would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner's admissions of prior art.

In regard to the first of the noted limitations, the Board stated that, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Because a ChoiceNet client can be configured as a control to block the user, it would have been obvious to alter it to redirect the user as well. Thus, the FireWall IRX Router running the ChoiceNet client corresponds to the redirection server of the '118 Patent because it applies filter rules to permit or deny access to users and it would have been obvious to alter its functionality to perform redirection.

In regard to the second of the noted limitations, to the extent the examiner does not find that ChoiceNet teaches that "the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server," ChoiceNet combined with Zenchelsky and the Patent Owner's admissions does.

As described above, in the background section of the '118 Patent, the Patent Owner admits that in "prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server 104." *Col. 1 ll. 21-24*. Thus, by the Patent Owner's admission, this limitation was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and communicating using IP addresses and

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

that this teaching was within the prior art as admitted by the Patent Owner in the Background section of the '118 Patent.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 56 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**G. Claim 68 Is Obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's Admissions**

**1. Detailed Explanation of Obviousness**

The following is a detailed explanation of the teachings of ChoiceNet in relation to Claim 68. Claim 68 is identical to canceled Claim 15 except that the location of the redirection server is specified with the addition of the following language: "a redirection server connected between a user computer and a public network." In the Prior Reexamination, the Board found Claim 15 to be obvious. *Linksmart Wireless*, No. 2011-009566, at 10. The added limitation, specifying the location of the redirection server, is taught by ChoiceNet, as illustrated in Diagram 19. Each limitation has been identified using letters (a) through (d) for ease of description and for later reference. In relation to Claim 68, ChoiceNet teaches or renders obvious a system comprising:

***(a) a redirection server connected between a user computer and a public network, the redirection server programmed with a user's rule set correlated to a temporarily assigned network address:*** ChoiceNet teaches filters associated with users where the filters are applied by the PortMaster upon an access request by a user. *ChoiceNet* at 1-6, 1-7; figs. 1-2, 1-4. The PortMaster can either permit or deny access based on the filter rules associated with the user. *See id.* Thus, the PortMaster corresponds to the redirection server which can be programmed with a user's rule set based on the filter sent from the RADIUS server.

Furthermore, ChoiceNet teaches that "ChoiceNet clients communicate with the ChoiceNet server to determine user access" and that ChoiceNet clients can be FireWall IRX Routers. *Id.* at 1-1; fig. 5-10. In figure 5-10 (Diagram 19), the FireWall IRX Router (corresponding to the redirection server) is connected *between* a user computer and the Worldwide Internet (corresponding to the public network).

Additionally, the communication between the server running the ChoiceNet client and the RADIUS server includes the transmission of IP packets, which contain source and destination network address information. *Id.* at 5-5. Thus, the ChoiceNet client passes the network address

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

to the RADIUS server along with the user ID to complete the authentication process. *See id.* Therefore, a filter is associated with a user which is associated with a network address.

***(b) wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network:*** ChoiceNet teaches “the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches the rule, the PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7; fig. 1-4. Thus, based on the rules, the PortMaster uses a plurality of functions (permit or deny) to control data passing between the user and the public network.

***(c) wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address:*** ChoiceNet teaches that the ChoiceNet client runs a **filterd** process and “[t]he **filterd** process automatically detects changes in the **clients** file and the **filters** directory.” *Id.* at 2-8. “ChoiceNet filters are simple text files that the system administrator creates in the **filters** directory.... The filter file contains the rules to be followed when the filter is applied.” *Id.* at 5-8. Moreover, “ChoiceNet can download filters from the server dynamically—on demand—to asynchronous and synchronous interfaces.” *Id.* at 1-3. Additionally, an administrator “can associate filters with network users configured for dial-in SLIP or PPP access.” *Id.* at 5-7. Thus, the redirection server running the ChoiceNet client allows dynamic and automated modification of filters which are associated with users.

***(d) wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses:*** ChoiceNet teaches that rule sets can be dynamically updated and modified, stating that an administrator “can create or modify ChoiceNet filters at any time, independent of any active packet filters.” *Id.* at 5-7; *see also id.* at 1-3, 2-8, 5-8. As an example, figure 1-4 illustrates an attempt to access a site or service over a network. “If a rule specifies a site list, the PortMaster sends a request to the ChoiceNet server to determine whether the site is on that list. This operation is called a site list look-up. The PortMaster caches the answer for future use.” *Id.* at 1-7; fig. 1-4. Thus, the PortMaster’s cached rule set can be modified at any time based on a location requested by a user. Furthermore, the Board stated that “blocking a website based on these bases [time, data, or location] would have

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Therefore, ChoiceNet teaches or renders obvious the above limitation.

**2. The Combination of ChoiceNet, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 68 Obvious**

ChoiceNet may not teach the following two elements of Claim 68:

1. A redirection server that performs redirection as well as blocking; and
2. A user’s rule set correlated to a temporarily assigned network address.

However, these differences between ChoiceNet and the claims would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner’s admissions of prior art.

In regard to the first of the noted limitations, the Board stated that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Because a ChoiceNet client can be configured as a control to block the user, it would have been obvious to alter it to redirect the user as well. Thus, the PortMaster or the FireWall IRX Router running the ChoiceNet client corresponds to the redirection server of the ’118 Patent because it applies filter rules to permit or deny access to users and it would have been obvious to alter its functionality to perform redirection.

In regard to the second of the noted limitations, to the extent the examiner does not find that ChoiceNet teaches “a user’s rule set correlated to a temporarily assigned network address,” ChoiceNet combined with Zenchelsky and the Patent Owner’s admissions does.

In the ’118 Patent, the Patent Owner admits that in “prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP’s authentication and accounting server 104.” *Col. 1 ll. 21-24*. Additionally, the Patent Owner admits that “the end user would be identified by the temporarily assigned IP address.” *Col. 1 ll. 35-37*. Thus, by the Patent Owner’s admission, identifying a user with a temporarily assigned IP address was known in the prior art at the time of the invention.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and identifying a user with the temporary IP address and that this teaching was within the prior art as admitted by the Patent Owner in the background section of the '118 Patent. Thus, ChoiceNet, in view of Zenchelsky and the Patent Owner's Admissions, renders obvious a user's rule set correlated to a temporarily assigned network address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 68 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions.

**H. Claim 83 Is Obvious over ChoiceNet in View of Zenchelsky and the Patent Owner's Admissions**

**1. Detailed Explanation of Obviousness**

The combination of ChoiceNet, Zenchelsky, and the Patent Owner's admissions renders independent Claim 83 obvious. Claim 83 is identical to canceled Claim 25 in the '118 Patent except that the limitation related to the location of the redirection server has been changed to specify that it is *between* a dial-up network server and a public network. This change is identical to the change made between canceled Claim 1 and Claim 44, discussed above in Section VI.E.1. Claim 83 is an independent claim that includes limitations analogous to those in Claims 68, 76, and 77. Therefore, Claim 83 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions for reasons analogous to those discussed above with respect to Claim 68 in Section VI.G. and below in Claims 76 and 77 in Sections VI.I.28. and VI.I.29, respectively. For ease of description, the limitations below are identified using the letters (a) through (e). In relation to Claim 83, Willens teaches or renders obvious a system comprising:

***(a) a redirection server connected between a user computer and a public network, the redirection server containing a user's rule set correlated to a temporarily assigned network address:*** This language is identical to the language in the limitation in Claim 68 identified as (a) in Section VI.G.1., except for one non-substantive change in the language. Claim 68 states "the redirection server *programmed* with a user's rule set" and Claim 83 states "the redirection server

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*containing* a user's rule set." Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches filters associated with users where the filters are applied by the PortMaster upon an access request by a user. *ChoiceNet* at 1-6, 1-7; figs. 1-2, 1-4. The PortMaster can either permit or deny access based on the filter rules associated with the user. *See id.* Thus, the PortMaster corresponds to the redirection server which can contain a user's rule set based on the filter sent from the RADIUS server.

Furthermore, ChoiceNet teaches that "ChoiceNet clients communicate with the ChoiceNet server to determine user access" and that ChoiceNet clients can be FireWall IRX Routers. *Id.* at 1-1; fig. 5-10. In figure 5-10 (Diagram 19), the FireWall IRX Router (corresponding to the redirection server) is connected *between* a user computer and the Worldwide Internet (corresponding to the public network).

Additionally, the communication between the server running the ChoiceNet client and the RADIUS server includes the transmission of IP packets, which contain source and destination network address information. *Id.* at 5-5. Thus, the ChoiceNet client passes the network address to the RADIUS server along with the user ID to complete the authentication process. *See id.* Therefore, a filter is associated with a user which is associated with a network address.

***(b) wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network:*** This language is identical to the language in the limitation in Claim 68 identified as (b) in Section VI.G.1. Thus, according to the discussion above and for analogous reasons, this limitation is taught by ChoiceNet.

ChoiceNet teaches "the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches the rule, the PortMaster takes the action—permit or deny—specified in the rule." *Id.* at 1-7; fig. 1-4. Thus, based on the rules, the PortMaster uses a plurality of functions (permit or deny) to control data passing between the user and the public network.

***(c) the method comprising the step of: modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server:*** This limitation is analogous to the limitation in Claim 68 identified as (c) in Section VI.G.1., except that the form of the limitation has been changed to be a step in a method

rather than functionality in a system. Thus, according to the discussion above and for analogous reasons, this limitation is taught or rendered obvious by ChoiceNet.

ChoiceNet teaches that the ChoiceNet client runs a **filterd** process and “[t]he **filterd** process automatically detects changes in the **clients** file and the **filters** directory.” *Id.* at 2-8. “ChoiceNet filters are simple text files that the system administrator creates in the **filters** directory.... The filter file contains the rules to be followed when the filter is applied.” *Id.* at 5-8. Moreover, “ChoiceNet can download filters from the server dynamically—on demand—to asynchronous and synchronous interfaces.” *Id.* at 1-3. Additionally, an administrator “can associate filters with network users configured for dial-in SLIP or PPP access.” *Id.* at 5-7. Thus, the redirection server running the ChoiceNet client allows dynamic and automated modification of filters which are associated with users.

*(d) wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network, and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server:* This language is identical to the language in the limitation in Claim 76, discussed below in Section VI.I.28. Thus, according to the discussion above and for analogous reasons, this limitation is taught or rendered obvious by ChoiceNet.

ChoiceNet teaches in figure 5-10 (Diagram 19) a FireWall IRX Router, acting as the redirection server, connected to a user through the PortMaster on a user side and the Worldwide Internet, RADIUS server, and ChoiceNet server on a network side. *ChoiceNet* figs. 5-10, 5-12. The user computer’s only route to the Worldwide Internet (corresponding to the computer network) is through the FireWall IRX Router. *See id.* As described above in Sections VI.A.2. and VI.A.3., ChoiceNet in combination with Zenchelsky and the Patent Owner’s admissions renders obvious a user computer using a temporarily assigned network address. It would have been obvious to modify the computer in ChoiceNet to be associated with a temporary network address.

*(e) and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user’s rule set through one or more of the user side of the redirection server and the network side of the redirection server:* This limitation is analogous to the limitation in Claim 77, discussed below in Section VI.I.29., except that the form

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

of the limitation has been changed to be a step in a method rather than functionality in a system. Thus, according to the discussion above and for analogous reasons, this limitation is taught or rendered obvious by ChoiceNet.

ChoiceNet teaches “[w]hen a user dials in to the network, if the appropriate filter does not reside locally on the client, the client sends a request to the ChoiceNet server to look up the filter. If the name of the filter assigned to the interface matches a filter defined on the ChoiceNet server, the filter is downloaded to the client.” *ChoiceNet* 1-3. ChoiceNet also teaches that “ChoiceNet can download filters from the server dynamically.” *Id.* As illustrated in Fig. 5-10, the ChoiceNet server resides on the network side of the FireWall IRX Router. Thus, ChoiceNet teaches a redirection server with rules that can be modified through instructions received from the network side of the redirection server.

Furthermore, ChoiceNet teaches that administrators can “can create or modify ChoiceNet filters at any time, independent of any active packet filters.” *Id.* at 5-7; *see id.* at 5-4. Modifying filters includes changing files on a ChoiceNet server. *Id.* Thus, changes made to filter rules on the ChoiceNet server propagate to the redirection server based on instructions from the network side of the server. Therefore, Willens teaches or renders obvious all the above limitations.

**2. The Combination of ChoiceNet, Zenchelsky, and the Patent Owner’s Admissions Renders Claim 83 Obvious**

ChoiceNet may not teach the following two elements of Claim 83:

1. A redirection server that performs redirection as well as blocking; and
2. A user’s rule set correlated to a temporarily assigned network address.

However, these differences between ChoiceNet and the claims would have been obvious modifications to one of ordinary skill in the art at the time of the invention in view of Zenchelsky and the Patent Owner’s admissions of prior art.

In regard to the first of the noted limitations, the Board stated that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Because a ChoiceNet client can be configured as a control to block the user, it would have been obvious to alter it to redirect the user as well. Thus, the PortMaster or the FireWall IRX Router running the ChoiceNet client corresponds to the redirection server of the ’118 Patent because it applies filter rules to permit or

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

deny access to users and it would have been obvious to alter its functionality to perform redirection.

In regard to the second of the noted limitations, to the extent the examiner does not find that ChoiceNet teaches “a user’s rule set correlated to a temporarily assigned network address,” ChoiceNet combined with Zenchelsky and the Patent Owner’s admissions does.

In the ’118 Patent, the Patent Owner admits that in “prior art systems...[t]he dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP’s authentication and accounting server 104.” *Col. 1 ll. 21-24*. Additionally, the Patent Owner admits that “the end user would be identified by the temporarily assigned IP address.” *Col. 1 ll. 35-37*. Thus, by the Patent Owner’s admission, identifying a user with a temporarily assigned IP address was known in the prior art at the time of the invention.

Furthermore, the Examiner found that this limitation was known in the prior art during the Prior Reexamination. In the Final Office Action mailed August 2, 2010, the Examiner found that modifying a network communication system to provide a temporary address to a user node would have been obvious in light of Zenchelsky. Thus, the Examiner recognized that Zenchelsky taught providing a temporary IP address and identifying a user with the temporary IP address and that this teaching was within the prior art as admitted by the Patent Owner in the background section of the ’118 Patent. Thus, ChoiceNet, in view of Zenchelsky and the Patent Owner’s Admissions, renders obvious a user’s rule set correlated to a temporarily assigned network address.

Therefore, in view of the discussion above, Requestor respectfully submits that Claim 83 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions.

**I. Claims 45-51, 53-55, 57-63, 65-67, 69-78, 80-82, 84-86, and 88-90 are Obvious over ChoiceNet in View of Zenchelsky and the Patent Owner’s Admissions**

**1. Claim 45**

Claim 45 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 45 recites:

45. The system of claim 44, wherein the redirection server further provides control over a plurality of data to and from the users’ computers as a function of the individualized rule set.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Claim 45 corresponds to Claim 2, discussed in Section VI.A.4., and is rendered obvious for analogous reasons. ChoiceNet teaches that “filter rules [can be written] to specify a site list in place of an IP address.... Each site list is a text file that contains the hostnames or IP addresses of hosts for which access is controlled. The rule can permit or deny access by hosts on the list or to hosts on the list.” *ChoiceNet* 1-3. ChoiceNet also teaches a redirection server that “searches the Filter Table for the filters specified by Filter-Id in the user entry. If the filters are present in the Filter Table, then they are applied to the connection.” *Id.* at 1-6. Thus, ChoiceNet teaches filter rules implemented by a redirection server that control a plurality of data to and from a user computer. Therefore, ChoiceNet teaches all the limitations of Claim 45.

**2. Claim 46**

Claim 46 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 46 recites:

46. The system of claim 44, wherein the redirection server further blocks the data to and from the users’ computers as a function of the individualized rule set.

Claim 46 corresponds to Claim 3, discussed in Section VI.A.5., and is rendered obvious for analogous reasons. ChoiceNet teaches that a server “enables both inbound and outbound traffic filtering for each interface and user.” *ChoiceNet* 1-2. ChoiceNet also teaches that when a “user attempts to access a particular site or service [t]he PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7; *see* fig. 1-4. Thus, ChoiceNet teaches a redirection server (the PortMaster) that blocks and allows data based on filter rules. Therefore, ChoiceNet teaches the limitations in Claim 46.

**3. Claim 47**

Claim 47 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 47 recites:

47. The system of claim 44, wherein the redirection server further allows the data to and from the users’ computers as a function of the individualized rule set.

Claim 47 corresponds to Claim 4, discussed in Section VI.A.6., and is rendered obvious for analogous reasons. Similar to Claim 46 which is directed to blocking data to and from a user computer, Claim 47 is directed to allowing data to and from a user computer. ChoiceNet teaches

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

that a server “enables both inbound and outbound traffic filtering for each interface and user.” *ChoiceNet* 1-2. ChoiceNet also teaches that when a “user attempts to access a particular site or service [t]he PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7; *see* fig. 1-4. Thus, ChoiceNet teaches a redirection server (the PortMaster) that blocks and allows data based on filter rules. Therefore, ChoiceNet teaches the limitations in Claim 47.

**4. Claim 48**

Claim 48 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 48 is corresponding system and method claims and recite:

48. The system of claim 44, wherein the redirection server further redirects the data to and from the users’ computers as a function of the individualized rule set.

Claim 48 corresponds to Claim 5, discussed in Section VI.A.7., and is rendered obvious for analogous reasons. ChoiceNet teaches that a server “enables both inbound and outbound traffic filtering for each interface and user.” *ChoiceNet* 1-2. ChoiceNet also teaches that when a “user attempts to access a particular site or service [t]he PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7; *see* fig. 1-4. Thus, ChoiceNet teaches a redirection server (the PortMaster) that blocks and allows data based on filter rules. As discussed in Section IV.F., the Board declared that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user” and “redirection would have been an obvious extension of blocking.” *Linksmart Wireless*, No. 2011-009566, at 9, 10. Based on the statement by the Board, it would have been obvious to modify the system in ChoiceNet to redirect data to and from a user’s computer as a function of filter rules. Therefore, ChoiceNet renders obvious all the limitations of Claim 48.

**5. Claim 49**

Claim 49 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 49 recites:

49. The system of claim 44, wherein the redirection server further redirects the data from the users’ computers to multiple destinations as a function of the individualized rule set.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Claim 49 corresponds to Claim 6, discussed in Section VI.A.8, and is rendered obvious for analogous reasons. Requestor respectfully submits that, given its broadest reasonable interpretation, Claim 49 encompasses at least a redirection server that redirects some data to one destination based on one rule, another destination based on another rule, and so on. ChoiceNet teaches filter rules that “specify a site list in place of an IP address.... Each site list is a text file that contains the hostnames or IP addresses of hosts for which access is controlled. The rule can permit or deny access by hosts on the list or to hosts on the list.” *ChoiceNet* 1-3. Thus, ChoiceNet teaches filters that can specify multiple rules, each rule directed to unique destinations. As discussed in Section IV.F., the Board stated that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system of ChoiceNet that blocks and allows data to multiple destinations to perform redirection to multiple destinations. Therefore, ChoiceNet renders obvious Claim 49.

**6. Claim 50**

Claim 50 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 50 recites:

50. The system of claim 44, wherein the database entries for a plurality of the plurality of users’ IDs are correlated with a common individualized rule set.

Claim 50 corresponds to Claim 7, discussed in Section VI.A.9., and is rendered obvious for analogous reasons. ChoiceNet teaches that a filter rule can be specified for a user by “defin[ing] the *Filter-Id* reply item in [the user’s] RADIUS entry as the filter name” where “*Filter-Id* is a reply item that identifies the filter to be associated with that user.” *ChoiceNet* 5-14, 5-10. By defining the same *Filter-Id* in multiple users’ RADIUS entries, ChoiceNet teaches that multiple users can be correlated with a common rule set. *See id.* at 5-10, 5-15. For example, ChoiceNet teaches that an “ISP can customize access to sites or services for groups of subscribers that share similar interests” through the use of filter rules. *Id.* at 5-10. Thus, multiple users can be correlated with a common rule set. Therefore, ChoiceNet teaches all the limitations of Claim 50.

**7. Claim 51**

Claim 51 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 51 recites:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

51. The system of claim 44, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

Claim 51 corresponds to Claim 28, discussed in Section VI.A.10., and is rendered obvious for analogous reasons. The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11*. Furthermore, the '118 Patent declares that IP “[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header.” *Col. 2 ll. 11-13*. ChoiceNet teaches that “[p]ackets can be filtered according to...source and destination port numbers to control access to certain network services.” *ChoiceNet 5-6; see also ChoiceNet Appx. C* (listing common port numbers assigned to TCP and UDP services). Thus, ChoiceNet teaches filtering based on a type of IP service by specifying a source or destination port in the filter rule.

In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, “redirection is not limited to WWW traffic, and the concept is valid for all IP services.” *Col. 1 ll. 41-42; see Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the system in ChoiceNet to filter based on IP service. Therefore, ChoiceNet teaches or renders obvious each limitation in Claim 51.

**8. Claim 53**

Claim 53 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 53 recites:

53. The system of claim 44, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

Claim 53 corresponds to Claim 30, discussed in Section VI.A.11., and is rendered obvious for analogous reasons. The '118 Patent gives examples of “request type” as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36*. Therefore, the broadest reasonable interpretation of request type includes http requests. ChoiceNet teaches that filters can be implemented based on port numbers which correlate to IP services: “Rules can use the source and destination port numbers to control access to certain network services.” *ChoiceNet 5-6*. For example, in Appendix C in the ChoiceNet reference, port 80 is associated with “World Wide Web Hypertext Transfer Protocol (HTTP).” In an example filter rule, access is permitted for “Web access via HTTP to the addresses in the site list **wwwok**.” *Id.* at 5-9, fig. 8, Table 5-1. Furthermore, ChoiceNet teaches “[a] rule can evaluate either the source or

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

destination address of a packet.” *Id.* at 5-6. Thus, ChoiceNet teaches filter rules that allow access based on a request type and destination address. Therefore, ChoiceNet teaches every limitation in Claim 53.

**9. Claim 54**

Claim 54 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 54 recites:

54. The system of claim 44, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 54 corresponds to Claim 31, discussed in Section VI.A.12., and is rendered obvious for analogous reasons. Furthermore, Claim 54 is identical to Claim 53 described above, except that Claim 54 is directed to “redirecting the data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. ChoiceNet teaches permitting or denying access based on a request type and destination address, as discussed above in Section VI.I.8. In the Prior Reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to redirect data based on a request type and destination address. Therefore, ChoiceNet renders obvious Claim 54.

**10. Claim 55**

Claim 55 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 55 recites:

55. The system of claim 44, wherein the redirection server is configured to redirect data from the users’ computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

Claim 55 contains language that is identical to the language in canceled Claim 32, whose rejection based on obviousness was affirmed by the Board in the Prior Reexamination. *Linksmart Wireless*, No. 2011-009566, at 10. “ChoiceNet filters IP traffic by comparing TCP, UDP, and ICMP packets against the filter rules.” *ChoiceNet* 1-2. ChoiceNet controls access through packet filtering which “analyzes the header information contained in each packet sent or received through an interface. The header information is evaluated against a set of rules, which either allow the packet to pass freely through the interface or cause the packet to be discarded

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

without being forwarded.” *Id.* at 5-5. Thus, ChoiceNet teaches analyzing IP packet headers to determine whether to route or drop an IP packet based on header information. As the Board stated, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to perform redirection by replacing a first destination address in an IP packet header by a second destination address according to filter rules. Therefore, Claim 55 is rendered obvious by ChoiceNet.

**11. Claim 57**

Claim 57 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 57 recites:

57. The method of claim 56, further including the step of controlling a plurality of data to and from the users’ computers as a function of the individualized rule set.

Claim 57 corresponds to Claim 9, discussed in Section VI.B.3., and is rendered obvious for analogous reasons. ChoiceNet teaches that “filter rules [can be written] to specify a site list in place of an IP address.... Each site list is a text file that contains the hostnames or IP addresses of hosts for which access is controlled. The rule can permit or deny access by hosts on the list or to hosts on the list.” *ChoiceNet* 1-3. ChoiceNet also teaches a redirection server that “searches the Filter Table for the filters specified by Filter-Id in the user entry. If the filters are present in the Filter Table, then they are applied to the connection.” *Id.* at 1-6. Thus, ChoiceNet teaches filter rules implemented by a redirection server that control a plurality of data to and from a user computer. Therefore, ChoiceNet teaches all the limitations of Claim 57.

**12. Claim 58**

Claim 58 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 58 recites:

58. The method of claim 56, further including the step of blocking the data to and from the users’ computers as a function of the individualized rule set.

Claim 58 corresponds to Claim 10, discussed in Section VI.B.4., and is rendered obvious for analogous reasons. ChoiceNet teaches that a server “enables both inbound and outbound traffic filtering for each interface and user.” *ChoiceNet* 1-2. ChoiceNet also teaches that when a “user attempts to access a particular site or service [t]he PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

permit or deny—specified in the rule.” *Id.* at 1-7; *see* fig. 1-4. Thus, ChoiceNet teaches a redirection server (the PortMaster) that blocks and allows data based on filter rules. Therefore, ChoiceNet teaches the limitations in Claim 58.

**13. Claim 59**

Claim 59 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 59 recites:

59. The method of claim 56, further including the step of allowing the data to and from the users’ computers as a function of the individualized rule set.

Claim 59 corresponds to Claim 11, discussed in Section VI.B.5., and is rendered obvious for analogous reasons. ChoiceNet teaches that a server “enables both inbound and outbound traffic filtering for each interface and user.” *ChoiceNet* 1-2. ChoiceNet also teaches that when a “user attempts to access a particular site or service [t]he PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7; *see* fig. 1-4. Thus, ChoiceNet teaches a redirection server (the PortMaster) that blocks and allows data based on filter rules. Therefore, ChoiceNet teaches the limitations in Claim 59.

**14. Claim 60**

Claim 60 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 60 recites:

60. The method of claim 56, further including the step of redirecting the data to and from the users’ computers as a function of the individualized rule set.

Claim 60 corresponds to Claim 12, discussed in Section VI.B.6., and is rendered obvious for analogous reasons. ChoiceNet teaches that a server “enables both inbound and outbound traffic filtering for each interface and user.” *ChoiceNet* 1-2. ChoiceNet also teaches that when a “user attempts to access a particular site or service [t]he PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule.” *Id.* at 1-7; *see* fig. 1-4. Thus, ChoiceNet teaches a redirection server (the PortMaster) that blocks and allows data based on filter rules. As discussed in Section IV.F., the Board declared that, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user” and “redirection would have been an obvious extension of blocking.” *Linksmart Wireless*, No. 2011-009566, at

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

9, 10. Based on the statement by the Board, it would have been obvious to modify the system in ChoiceNet to redirect data to and from a user's computer as a function of filter rules. Therefore, ChoiceNet renders obvious all the limitations of Claim 60.

**15. Claim 61**

Claim 61 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 61 recites:

61. The method of claim 56, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.

Claim 61 corresponds to Claim 13, discussed in Section VI.B.7., and is rendered obvious for analogous reasons. Requestor respectfully submits that, given its broadest reasonable interpretation, Claim 61 encompasses at least a redirection server that redirects some data to one destination based on one rule, another destination based on another rule, and so on. ChoiceNet teaches filter rules that "specify a site list in place of an IP address.... Each site list is a text file that contains the hostnames or IP addresses of hosts for which access is controlled. The rule can permit or deny access by hosts on the list or to hosts on the list." *ChoiceNet* 1-3. Thus, ChoiceNet teaches filters that can specify multiple rules, each rule directed to unique destinations. As discussed in Section IV.F., the Board stated that, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system of ChoiceNet that blocks and allows data to multiple destinations to perform redirection to multiple destinations. Therefore, ChoiceNet renders obvious Claim 61.

**16. Claim 62**

Claim 62 is rendered obvious by ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 62 recites:

62. The method of claim 56, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.

Claim 62 corresponds to Claim 14, discussed in Section VI.B.8., and is rendered obvious for analogous reasons. ChoiceNet teaches that a filter rule can be specified for a user by "defin[ing] the *Filter-Id* reply item in [the user's] RADIUS entry as the filter name" where "*Filter-Id* is a reply item that identifies the filter to be associated with that user." *ChoiceNet* 5-

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

14, 5-10. By defining the same *Filter-Id* in multiple users' RADIUS entries, ChoiceNet teaches that multiple users can be correlated with a common rule set. *See id.* at 5-10, 5-15. For example, ChoiceNet teaches that an "ISP can customize access to sites or services for groups of subscribers that share similar interests" through the use of filter rules. *Id.* at 5-10. Thus, multiple users can be correlated with a common rule set. Therefore, ChoiceNet teaches all the limitations of Claim 62.

**17. Claim 63**

Claim 63 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 63 recites:

63. The method of claim 56, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

Claim 63 corresponds to Claim 32, discussed in Section VI.B.9., and is rendered obvious for analogous reasons. The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11*. Furthermore, the '118 Patent declares that IP "[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header." *Col. 2 ll. 11-13*. ChoiceNet teaches that "[p]ackets can be filtered according to...source and destination port numbers to control access to certain network services." *ChoiceNet 5-6; see also ChoiceNet Appx. C* (listing common port numbers assigned to TCP and UDP services). Thus, ChoiceNet teaches filtering based on a type of IP service by specifying a source or destination port in the filter rule.

In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, "redirection is not limited to WWW traffic, and the concept is valid for all IP services." *Col. 1 ll. 41-42; see Linksmart Wireless, No. 2011-009566, at 8, fn.24*. Accordingly, it would have been obvious to modify the system in ChoiceNet to filter based on IP service. Therefore, ChoiceNet teaches or renders obvious each limitation in Claim 63.

**18. Claim 65**

Claim 65 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 65 recites:

65. The method of claim 56, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Claim 65 corresponds to Claim 34, discussed in Section VI.B.10., and is rendered obvious for analogous reasons. The '118 Patent gives examples of “request type” as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36.* Therefore, the broadest reasonable interpretation of request type includes http requests. ChoiceNet teaches that filters can be implemented based on port numbers which correlate to IP services: “Rules can use the source and destination port numbers to control access to certain network services.” *ChoiceNet* 5-6. For example, in Appendix C in the ChoiceNet reference, port 80 is associated with “World Wide Web Hypertext Transfer Protocol (HTTP).” In an example filter rule, access is permitted for “Web access via HTTP to the addresses in the site list **wwwok**.” *Id.* at 5-9, fig. 8, Table 5-1. Furthermore, ChoiceNet teaches “[a] rule can evaluate either the source or destination address of a packet.” *Id.* at 5-6. Thus, ChoiceNet teaches filter rules that allow access based on a request type and destination address. Therefore, ChoiceNet teaches every limitation in Claim 65.

**19. Claim 66**

Claim 66 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 66 recites:

66. The method of claim 56, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 66 corresponds to Claim 35, discussed in Section VI.B.11., and is rendered obvious for analogous reasons. Claim 66 is also identical to Claim 65 described above, except that Claim 66 is directed to “redirecting the data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. ChoiceNet teaches permitting or denying access based on a request type and destination address, as discussed above in Section VI.I.18. In the Prior Reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to redirect data based on a request type and destination address. Therefore, ChoiceNet renders obvious Claim 66.

**20. Claim 67**

Claim 67 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 67 recites:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

67. The method of claim 56, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

Claim 67 contains language that is identical to the language in canceled Claim 37, whose rejection based on obviousness was affirmed by the Board in the Prior Reexamination. *Linksmart Wireless*, No. 2011-009566, at 10. "ChoiceNet filters IP traffic by comparing TCP, UDP, and ICMP packets against the filter rules." *ChoiceNet* 1-2. ChoiceNet controls access through packet filtering which "analyzes the header information contained in each packet sent or received through an interface. The header information is evaluated against a set of rules, which either allow the packet to pass freely through the interface or cause the packet to be discarded without being forwarded." *Id.* at 5-5. Thus, ChoiceNet teaches analyzing IP packet headers to determine whether to route or drop an IP packet based on header information. As the Board stated, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to perform redirection by replacing a first destination address in an IP packet header by a second destination address according to filter rules. Therefore, Claim 67 is rendered obvious by ChoiceNet.

**21. Claim 69**

Claim 69, depending from Claim 68, is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 69 recites:

69. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

Claim 69 corresponds to Claim 16, discussed in Section VI.C.3., and is rendered obvious for analogous reasons. Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of "modification" of a portion of a rule set because updating a rule set can change or modify a rule.

As taught in ChoiceNet, an administrator "can create or modify ChoiceNet filters at any time, independent of any active packet filters." *ChoiceNet* at 5-7. ChoiceNet also teaches that an administrator can change rule sets at any time by adding, deleting, or modifying files, modifications which would then be implemented by the redirection server: "A few days later, suppose you modify the **deny\_list** file and add two new lists, **no\_go** and **permit\_list**, as shown

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

in Figure 5-5. When you run **buildlist** now, it updates and generates the files as shown in Figure 5-6.” *Id.* at 5-4; figs. 5-5, 5-6 (emphasis original). Thus, ChoiceNet teaches modifying, removing, or reinstating rules as a function of time. Furthermore, the Board stated that “blocking a website based on these bases [as a function of time, data sent or received, or location accessed] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, the Board declared that it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Therefore, ChoiceNet teaches or renders obvious all the limitations in Claim 69.

**22. Claim 70**

Claim 70, depending from Claim 68, is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 70 recites:

70. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

Claim 70 corresponds to Claim 17, discussed in Section VI.C.4., and is rendered obvious for analogous reasons. Similar to Claim 69 above, Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of “modification” of a portion of a rule set because updating a rule set can change or modify a rule.

ChoiceNet teaches that an administrator can change filters and filter rules at any time and for any reason. *See ChoiceNet* 5-4. Choice Net teaches that an “ISP can customize access to sites or services for groups of subscribers that share similar interests.” *Id.* at 5-10. As an example, “[o]ne group might be interested in access only to the Web, another in access to role-playing games, another only in sites that are church-related, and another only in sites that relate to business and economics.” *Id.* Thus, ChoiceNet teaches filter rules that are based on data transmitted to or from the user. Moreover, as stated above, the Board declared that modifying rule sets based on data transmitted to or from the user would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the system in ChoiceNet to allow modification, removal, or reinstatement of rules as a function of data the user sends or receives. Therefore, ChoiceNet renders obvious Claim 70.

**23. Claim 71**

Claim 71, depending from Claim 68, is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 71 recites:

71. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.

Claim 71 corresponds to Claim 18, discussed in Section VI.C.5., and is rendered obvious for analogous reasons. Similar to Claim 69 above, Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of "modification" of a portion of a rule set because updating a rule set can change or modify a rule.

ChoiceNet teaches that an administrator can change filters at any time and for any reason. *See ChoiceNet* 5-4. In addition, filter rules on the redirection server can be changed and updated based on a site request. *See id.* at 1-7. For example, "the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules.... If a rule specifies a site list, the PortMaster sends a request to the ChoiceNet server to determine whether the site is on that list.... The PortMaster caches the answer for future use." *Id.*; *see id.* fig. 1-4. Thus, ChoiceNet teaches a server that can update a local cache of filter rules based on a site request from a user. Moreover, as stated above, the Board declared that modifying rule sets based on the location or locations the user accesses would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the PortMaster in ChoiceNet to allow modification of rules as a function of locations the user attempts to access. Therefore, ChoiceNet renders obvious Claim 71.

**24. Claim 72**

Claim 72, depending from Claim 68, is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 72 recites:

72. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

Claim 72 corresponds to Claim 19, discussed in Section VI.C.6., and is rendered obvious for analogous reasons. The difference between Claim 69 and Claim 72 is that the limitation in Claim 69 states a portion of the rule set can be modified as a function of time and the limitation in Claim 72 states a portion of the rule set can be removed or reinstated as a function of time.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Thus, the difference between Claims 69 and 72 is a change from “modification” to “removal or reinstatement.” Requestor respectfully submits that updating a portion of a rule set falls within the broadest reasonable interpretation of “removal or reinstatement” of a portion of a rule set because updating a rule set can remove or reinstate a rule.

As taught in ChoiceNet, an administrator “can create or modify ChoiceNet filters at any time, independent of any active packet filters.” *ChoiceNet* at 5-7. ChoiceNet also teaches that an administrator can change rule sets at any time by adding, deleting, or modifying files, modifications which would then be implemented by the redirection server: “A few days later, suppose you modify the **deny\_list** file and add two new lists, **no\_go** and **permit\_list**, as shown in Figure 5-5. When you run **buildlist** now, it updates and generates the files as shown in Figure 5-6.” *Id.* at 5-4; figs. 5-5, 5-6 (emphasis original). Thus, ChoiceNet teaches modifying, removing, or reinstating rules as a function of time. Furthermore, the Board stated that “blocking a website based on these bases [as a function of time, data sent or received, or location accessed] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. For example, the Board declared that it would have been obvious to “block[] a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at a site unrelated to work.” *Id.* at fn.29. Therefore, ChoiceNet teaches or renders obvious all the limitations in Claim 72.

**25. Claim 73**

Claim 73, depending from Claim 68, is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 73 recites:

73. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

Claim 73 corresponds to Claim 20, discussed in Section VI.C.7., and is rendered obvious for analogous reasons. Similar to Claims 69 and 72 above, the difference between Claims 70 and 73 is the change of the word “modification” to the words “removal or reinstatement.” ChoiceNet teaches that an administrator can change filters and filter rules at any time and for any reason. *See ChoiceNet* 5-4. Choice Net teaches that an “ISP can customize access to sites or services for groups of subscribers that share similar interests.” *Id.* at 5-10. As an example, “[o]ne group might be interested in access only to the Web, another in access to role-playing games, another

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

only in sites that are church-related, and another only in sites that relate to business and economics.” *Id.* Thus, ChoiceNet teaches filter rules that are based on data transmitted to or from the user. Moreover, as stated above, the Board declared that modifying rule sets based on data transmitted to or from the user would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the system in ChoiceNet to allow modification, removal, or reinstatement of rules as a function of data the user sends or receives. Therefore, ChoiceNet renders obvious Claim 73.

**26. Claim 74**

Claim 74, depending from Claim 68, is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 74 recites:

74. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.

Claim 74 corresponds to Claim 21, discussed in Section VI.C.8., and is rendered obvious for analogous reasons. Similar to Claims 69 and 72 above, Claims 71 and 74 differ only in the change of the word “modification” to the words “removal or reinstatement.” ChoiceNet teaches that an administrator can change filters at any time and for any reason. *See ChoiceNet* 5-4. In addition, filter rules on the redirection server can be changed and updated based on a site request. *See id.* at 1-7. For example, “the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules.... If a rule specifies a site list, the PortMaster sends a request to the ChoiceNet server to determine whether the site is on that list.... The PortMaster caches the answer for future use.” *Id.*; *see id.* fig. 1-4. Thus, ChoiceNet teaches a server that can update a local cache of filter rules based on a site request from a user. Moreover, as stated above, the Board declared that modifying rule sets based on the location or locations the user accesses would have been obvious. *See Linksmart Wireless*, No. 2011-009566, at 10, fn.29. Accordingly, it would have been obvious to modify the PortMaster in ChoiceNet to allow modification of rules as a function of locations the user attempts to access. Therefore, ChoiceNet renders obvious Claim 74.

**27. Claim 75**

Claim 75 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 75 recites:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

75. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.

Claim 75 corresponds to Claim 22, discussed in Section VI.C.9., and is rendered obvious for analogous reasons. Similar to Claim 72, Requestor respectfully submits that updating filter rules falls within the broadest reasonable interpretation of “removal or reinstatement” of a portion of the user’s rule set because updating a rule set can include removing or reinstating rules.

ChoiceNet teaches a redirection server (the server running a ChoiceNet client) that can filter user requests based on a location requested. *See ChoiceNet* 1-7. ChoiceNet also teaches that filter rules can be implemented based on the nature of the content of communication. *See id.* at 5-10. ChoiceNet also teaches that rules can be modified at any time and updated dynamically. *See id.* at 5-4. Thus, ChoiceNet teaches a redirection server that allows the modification, removal, or reinstatement of rules based on at least one of time, data communicated, and location accessed. Furthermore, the Board stated that “blocking a website based on these bases [time, data, or location] would have been obvious” to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the system in ChoiceNet to allow the modification, removal, or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed. Therefore, ChoiceNet renders obvious Claim 75.

**28. Claim 76**

Claim 76 is obvious over Willens in view of Zenchelsky and the Patent Owner’s admissions. Claim 76 recites:

76. The system of claim 68, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

Claim 76 corresponds to Claim 23, discussed in Section VI.C.10., and is rendered obvious for analogous reasons. ChoiceNet teaches in figure 5-10 (Diagram 19 above) a FireWall IRX Router, acting as the redirection server, connected to a user through the PortMaster on a user side and the Worldwide Internet, RADIUS server, and ChoiceNet server on a network side.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

*ChoiceNet* figs. 5-10, 5-12. The user computer's only route to the Worldwide Internet (corresponding to the computer network) is through the FireWall IRX Router. *See id.* As described above in Sections VI.C.2. and VI.G.2., *ChoiceNet* in combination with Zenchelsky and the Patent Owner's admissions renders obvious a user computer using a temporarily assigned network address. It would have been obvious to modify the computer in *ChoiceNet* to be associated with a temporary network address. Therefore, *ChoiceNet*, in view of Zenchelsky and the Patent Owner's admissions, renders obvious Claim 76.

**29. Claim 77**

Claim 77 is obvious over Willens in view of Zenchelsky and the Patent Owner's admissions. Claim 77 depends from Claim 76, discussed above in Section VI.I.28., and recites:

77. The system of claim 76 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.

Claim 77 corresponds to Claim 24, discussed in Section VI.C.11., and is rendered obvious for analogous reasons. *ChoiceNet* teaches "[w]hen a user dials in to the network, if the appropriate filter does not reside locally on the client, the client sends a request to the *ChoiceNet* server to look up the filter. If the name of the filter assigned to the interface matches a filter defined on the *ChoiceNet* server, the filter is downloaded to the client." *ChoiceNet* 1-3. *ChoiceNet* also teaches that "*ChoiceNet* can download filters from the server dynamically." *Id.* As illustrated in Fig. 5-10, the *ChoiceNet* server resides on the network side of the FireWall IRX Router. Thus, *ChoiceNet* teaches a redirection server with rules that can be modified through instructions received from the network side of the redirection server.

Furthermore, *ChoiceNet* teaches that administrators can "can create or modify *ChoiceNet* filters at any time, independent of any active packet filters." *Id.* at 5-7; *see id.* at 5-4. Modifying filters includes changing files on a *ChoiceNet* server. *Id.* Thus, changes made to filter rules on the *ChoiceNet* server propagate to the redirection server based on instructions from the network side of the server. Therefore, *ChoiceNet* teaches all the limitations of Claim 77.

**30. Claim 78**

Claim 78 is obvious over *ChoiceNet* in view of Zenchelsky and the Patent Owner's admissions. Claim 78 recites:

78. The system of claim 68, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Claim 78 corresponds to Claim 36, discussed in Section VI.C.12., and is rendered obvious for analogous reasons. The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll. 7-11*. Furthermore, the '118 Patent declares that IP “[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header.” *Col. 2 ll. 11-13*. ChoiceNet teaches that “[p]ackets can be filtered according to...source and destination port numbers to control access to certain network services.” *ChoiceNet 5-6; see also ChoiceNet Appx. C* (listing common port numbers assigned to TCP and UDP services). Thus, ChoiceNet teaches filtering based on a type of IP service by specifying a source or destination port in the filter rule.

In addition, as the Patent Owner admitted in the '118 Patent and the Board recognized, “redirection is not limited to WWW traffic, and the concept is valid for all IP services.” *Col. 1 ll. 41-42; see Linksmart Wireless, No. 2011-009566, at 8, fn.24*. Accordingly, it would have been obvious to modify the system in ChoiceNet to filter based on IP service. Therefore, ChoiceNet teaches or renders obvious each limitation in Claim 78.

**31. Claim 80**

Claim 80 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 80 recites:

80. The system of claim 68, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

Claim 80 corresponds to Claim 38, discussed in Section VI.C.13., and is rendered obvious for analogous reasons. The '118 Patent gives examples of “request type” as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36*. Therefore, the broadest reasonable interpretation of request type includes http requests. ChoiceNet teaches that filters can be implemented based on port numbers which correlate to IP services: “Rules can use the source and destination port numbers to control access to certain network services.” *ChoiceNet 5-6*. For example, in Appendix C in the ChoiceNet reference, port 80 is associated with “World Wide Web Hypertext Transfer Protocol (HTTP).” In an example filter rule, access is permitted for “Web access via HTTP to the addresses in the site list **wwwok**.” *Id.* at 5-9, fig. 8, Table 5-1. Furthermore, ChoiceNet teaches “[a] rule can evaluate either the source or destination address of a packet.” *Id.* at 5-6. Thus, ChoiceNet teaches filter rules that allow

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

access based on a request type and destination address. Therefore, ChoiceNet teaches every limitation in Claim 80.

**32. Claim 81**

Claims 81 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 81 recites:

81. The system of claim 68, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 81 corresponds to Claim 39, discussed in Section VI.C.14., and is rendered obvious for analogous reasons. Claim 81 is identical to Claim 80, except that Claim 81 is directed to "redirecting the data to a new destination address" instead of "allowing access" based on a request type and an attempted destination address. ChoiceNet teaches permitting or denying access based on a request type and destination address, as discussed above in Section VI.I.31. In the Prior Reexamination, the Board declared, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to redirect data based on a request type and destination address. Therefore, ChoiceNet renders obvious Claim 81.

**33. Claim 82**

Claim 82 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 82 recites:

82. The system of claim 68, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the modified rule set.

Claim 82 contains language that is identical to the language in canceled Claim 42, whose rejection based on obviousness was affirmed by the Board in the Prior Reexamination. *Linksmart Wireless*, No. 2011-009566, at 10. "ChoiceNet filters IP traffic by comparing TCP, UDP, and ICMP packets against the filter rules." *ChoiceNet* 1-2. ChoiceNet controls access through packet filtering which "analyzes the header information contained in each packet sent or received through an interface. The header information is evaluated against a set of rules, which either allow the packet to pass freely through the interface or cause the packet to be discarded without being forwarded." *Id.* at 5-5. Thus, ChoiceNet teaches analyzing IP packet headers to

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

determine whether to route or drop an IP packet based on header information. As the Board stated, in view of the Patent Owner's admissions, "redirection is an obvious extension of the use of a control to block the user." *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to perform redirection by replacing a first destination address in an IP packet header by a second destination address according to filter rules. Therefore, Claim 82 is rendered obvious by ChoiceNet.

**34. Claim 84**

Claim 84 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 84 recites:

84. The method of claim 83, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.

Claim 84 corresponds to Claim 26, discussed in Section VI.D.3., and is rendered obvious for analogous reasons. As stated above, updating filter rules falls within the broadest reasonable interpretation of "modifying" and "removing or reinstating at least a portion of the user's rule set" because updating a rule set can include altering, removing, or reinstating rules.

ChoiceNet teaches a redirection server (the server running a ChoiceNet client) that can filter user requests based on a location requested. *See ChoiceNet* 1-7. ChoiceNet also teaches that filter rules can be implemented based on the nature of the content of communication. *See id.* at 5-10. ChoiceNet also teaches that rules can be modified at any time and updated dynamically. *See id.* at 5-4. Thus, ChoiceNet teaches a redirection server that allows the modification, removal, or reinstatement of rules based on at least one of time, data communicated, and location accessed. Furthermore, the Board stated that "blocking a website based on these bases [time, data, or location] would have been obvious" to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the system in ChoiceNet to allow the modification, removal, or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed. Therefore, ChoiceNet renders obvious Claim 84.

**35. Claim 85**

Claim 85 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 85 recites:

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

85. The method of claim 83, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and the location or locations the user accesses.

Claim 85 corresponds to Claim 27, discussed in Section VI.D.4., and is rendered obvious for analogous reasons. Furthermore, Claims 84 and 85 differ only in the change of the word "modification" to the words "removal or reinstatement." As stated above, Requestor respectfully submits that updating filter rules falls within the broadest reasonable interpretation of "removing or reinstating at least a portion of the user's rule set" because updating a rule set can include removing or reinstating rules.

ChoiceNet teaches a redirection server (the server running a ChoiceNet client) that can filter user requests based on a location requested. *See ChoiceNet* 1-7. ChoiceNet also teaches that filter rules can be implemented based on the nature of the content of communication. *See id.* at 5-10. ChoiceNet also teaches that rules can be modified at any time and updated dynamically. *See id.* at 5-4. Thus, ChoiceNet teaches a redirection server that allows the modification, removal, or reinstatement of rules based on at least one of time, data communicated, and location accessed. Furthermore, the Board stated that "blocking a website based on these bases [time, data, or location] would have been obvious" to one having ordinary skill in the art at the time of the invention. *Linksmart Wireless*, No. 2011-009566, at 10. Thus, it would have been obvious to modify the system in ChoiceNet to allow the modification, removal, or reinstatement of rules based on some combination of time, data transmitted or received, or locations accessed. Therefore, ChoiceNet renders obvious Claim 85.

**36. Claim 86**

Claim 86 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner's admissions. Claim 86 recites:

86. The method of claim 83, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

Claim 86 corresponds to Claim 40, discussed in Section VI.D.5., and is rendered obvious for analogous reasons. The '118 Patent gives examples of IP services which include FTP, WWW data, or Telnet session data. *Col. 2 ll.* 7-11. Furthermore, the '118 Patent declares that IP "[s]ervice identification is achieved by identifying the terminating port number contained within each IP packet header." *Col. 2 ll.* 11-13. ChoiceNet teaches that "[p]ackets can be filtered

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

according to...source and destination port numbers to control access to certain network services.” *ChoiceNet* 5-6; *see also ChoiceNet* Appx. C (listing common port numbers assigned to TCP and UDP services). Thus, ChoiceNet teaches filtering based on a type of IP service by specifying a source or destination port in the filter rule.

In addition, as the Patent Owner admitted in the ’118 Patent and the Board recognized, “redirection is not limited to WWW traffic, and the concept is valid for all IP services.” *Col. 1 ll. 41-42*; *see Linksmart Wireless*, No. 2011-009566, at 8, fn.24. Accordingly, it would have been obvious to modify the system in ChoiceNet to filter based on IP service. Therefore, ChoiceNet teaches or renders obvious each limitation in Claim 86.

**37. Claim 88**

Claim 88 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 88 recites:

88. The method of claim 83, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

Claim 88 corresponds to Claim 42, discussed in Section VI.D.6., and is rendered obvious for analogous reasons. The ’118 Patent gives examples of “request type” as used in the claim which include http and Telnet requests. *Col. 6 ll. 42-49, col. 7 ll. 31-36*. Therefore, the broadest reasonable interpretation of request type includes http requests. ChoiceNet teaches that filters can be implemented based on port numbers which correlate to IP services: “Rules can use the source and destination port numbers to control access to certain network services.” *ChoiceNet* 5-6. For example, in Appendix C in the ChoiceNet reference, port 80 is associated with “World Wide Web Hypertext Transfer Protocol (HTTP).” In an example filter rule, access is permitted for “Web access via HTTP to the addresses in the site list **wwwok**.” *Id.* at 5-9, fig. 8, Table 5-1. Furthermore, ChoiceNet teaches “[a] rule can evaluate either the source or destination address of a packet.” *Id.* at 5-6. Thus, ChoiceNet teaches filter rules that allow access based on a request type and destination address. Therefore, ChoiceNet teaches every limitation in Claim 88.

**38. Claim 89**

Claim 89 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 89 recites:

89. The method of claim 83, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Claim 89 corresponds to Claim 43, discussed in Section VI.D.7., and is rendered obvious for analogous reasons. Furthermore, Claim 89 is identical to the Claim 88 described above, except that Claim 89 is directed to “redirecting the data to a new destination address” instead of “allowing access” based on a request type and an attempted destination address. ChoiceNet teaches permitting or denying access based on a request type and destination address, as discussed above in Section VI.I.37. In the Prior Reexamination, the Board declared, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to redirect data based on a request type and destination address. Therefore, ChoiceNet renders obvious Claim 89.

**39. Claim 90**

Claim 90 is obvious over ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Claim 90 recites:

90. The method of claim 83, wherein the redirection server is configured to redirect data from the users’ computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

Claim 90 contains language that is identical to the language in canceled Claim 47, whose rejection based on obviousness was affirmed by the Board in the Prior Reexamination. *Linksmart Wireless*, No. 2011-009566, at 10. “ChoiceNet filters IP traffic by comparing TCP, UDP, and ICMP packets against the filter rules.” *ChoiceNet* 1-2. ChoiceNet controls access through packet filtering which “analyzes the header information contained in each packet sent or received through an interface. The header information is evaluated against a set of rules, which either allow the packet to pass freely through the interface or cause the packet to be discarded without being forwarded.” *Id.* at 5-5. Thus, ChoiceNet teaches analyzing IP packet headers to determine whether to route or drop an IP packet based on header information. As the Board stated, in view of the Patent Owner’s admissions, “redirection is an obvious extension of the use of a control to block the user.” *Linksmart Wireless*, No. 2011-009566, at 9. Accordingly, it would have been obvious to modify the system in ChoiceNet to perform redirection by replacing a first destination address in an IP packet header by a second destination address according to filter rules. Therefore, Claim 90 is rendered obvious by ChoiceNet.

**VIII. CLAIMS 29, 33, 37, 41, 52, 64, 79, AND 87 ARE OBVIOUS OVER CHOICENET  
IN VIEW OF HE, ZENCHELSKY, AND THE PATENT OWNER'S ADMISSIONS**

Claims 29, 33, 52, and 64 contain the following limitation:

*wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set*

Claims 37, 41, 79, and 87 contain the following limitation:

*wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set*

The only difference between the language in the first noted limitation and the second is a change from “the individualized rule set” to “the modified rule set.” This change corresponds to the difference in the two general groups of claims, as described in Section II.B., where the first group pertains to controlling access to the Internet based on rule sets and the second group pertains to modification of the rule sets. However, as described in the '118 Patent, the individualized rule set and the modified rule set both refer to rule sets which are “personalized filtering and redirection information for the particular user ID.” *Col. 3 ll. 3-4.*

**A. Claims 29, 33, 52, and 64**

Claims 29, 33, 52, and 64 depend respectively from canceled Claim 1, canceled Claim 8, Claim 44, and Claim 56. Each of the limitations in canceled Claim 1, canceled Claim 8, Claim 44, and Claim 56 are taught by ChoiceNet or are rendered obvious by the combination of ChoiceNet, Zenchelsky, and the Patent Owner's admissions as described above in Sections VI.A., VI.B., VI.E., and VI.F., respectively.

In regard to the limitation in Claims 29, 33, 52, and 64, ChoiceNet teaches that an administrator “can create or modify ChoiceNet filters at any time, independent of any active packet filters.” *ChoiceNet* 5-7. As an example, ChoiceNet teaches that an administrator can “modify the **deny\_list** file and add two new lists, **no\_go** and **permit\_list**.... When you run **builddlist** now, it updates and generates [filter] files.” *Id.* at 5-4; *see* figs. 5-5, 5-6, 5-7. Thus, the ChoiceNet system allows for filters to be modified at any time, allowing an administrator to implement a temporary rule set that lasts for an initial period of time and then implement a standard rule set.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

The system taught in He is generally an authentication system that enables users to gain access to online services such as server computers and printers. He discloses “a network security architecture to provide protection to user access to the resources and information in network elements.” *Col. 33 ll. 8-10*. In one embodiment, the system in He allows or denies access based on duration of a timed session. *See col. 28 ll. 26-41*. He states “[a] session length is typically defined as the period between log-ons for a user element coupled to the network 106, or for dial-up sessions delimited by the dial-up communication protocol software.” *Col. 28 ll. 26-29*. The administrator of the system in He can limit the “time that the user element and selected network can communicate with each other.” *Col. 28 ll. 31-33*. Furthermore, He states that “if the length of time that is allowed for the log-on session is exceeded, all the tickets [granting access to network elements] that have been issued to the user will also become invalid and therefore be destroyed.” *Col. 28 ll. 36-38*. Thus, He teaches a first rule set which allows access to network elements which can expire after a defined amount of time wherein a second rule set is applied which denies access to network elements.

Hence, it would have been obvious to modify the rule sets in ChoiceNet to include a temporary rule set for an initial period of time and a standard rule set thereafter, as taught in He. Therefore, Requestor respectfully submits that Claims 29, 33, 52, and 64 are obvious over ChoiceNet in view of He, Zenchelsky, and the Patent Owner’s admissions.

**B. Claims 37, 41, 79, and 87**

Claims 37, 41, 79, and 87 depend respectively from canceled Claim 15, canceled Claim 25, Claim 68, and Claim 83. Each of the limitations in canceled Claim 15, canceled Claim 25, Claim 68, and Claim 83 are taught by ChoiceNet or are rendered obvious by the combination of ChoiceNet, Zenchelsky, and the Patent Owner’s admissions as described above in Sections VI.C., VI.D., VI.G., and VI.H., respectively.

In regard to the limitation in Claims 37, 41, 79, and 87, ChoiceNet teaches that an administrator “can create or modify ChoiceNet filters at any time, independent of any active packet filters.” *ChoiceNet 5-7*. As an example, ChoiceNet teaches that an administrator can “modify the **deny\_list** file and add two new lists, **no\_go** and **permit\_list**.... When you run **buildlist** now, it updates and generates [filter] files.” *Id.* at 5-4; *see* figs. 5-5, 5-6, 5-7. Thus, the ChoiceNet system allows for filters to be modified at any time, allowing an administrator to

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

implement a temporary rule set that lasts for an initial period of time and then implement a standard rule set.

The system taught in He is generally an authentication system that enables users to gain access to online services such as server computers and printers. He discloses “a network security architecture to provide protection to user access to the resources and information in network elements.” *Col. 33 ll. 8-10*. In one embodiment, the system in He allows or denies access based on duration of a timed session. *See col. 28 ll. 26-41*. He states “[a] session length is typically defined as the period between log-ons for a user element coupled to the network 106, or for dial-up sessions delimited by the dial-up communication protocol software.” *Col. 28 ll. 26-29*. The administrator of the system in He can limit the “time that the user element and selected network can communicate with each other.” *Col. 28 ll. 31-33*. Furthermore, He states that “if the length of time that is allowed for the log-on session is exceeded, all the tickets [granting access to network elements] that have been issued to the user will also become invalid and therefore be destroyed.” *Col. 28 ll. 36-38*. Thus, He teaches a first rule set which allows access to network elements which can expire after a defined amount of time wherein a second rule set is applied which denies access to network elements.

Hence, it would have been obvious to modify the rule sets in ChoiceNet to include a temporary rule set for an initial period of time and a standard rule set thereafter, as taught in He. Therefore, Requestor respectfully submits that Claims 37, 41, 79, and 87 are obvious over ChoiceNet in view of He, Zenchelsky, and the Patent Owner’s admissions.

**IX. CONCLUSION**

For the foregoing reasons, Requestor has identified a substantial new question of the patentability of Claims 2-7, 9-14, 16-24, 26-27, 29-32, 34-36, 38-40, 42-51, 53-63, 65-78, 80-87, and 89-90 of the ’118 Patent based on either of the prior art references Willens or ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions. Requestor has further identified a substantial new question of the patentability of Claims 29, 33, 37, 41, 52, 64, 79, and 87 of the ’118 Patent based on either of the prior art references Willens or ChoiceNet in view of Zenchelsky and the Patent Owner’s admissions, and further in view of He. The references render the claims of the patent obvious, thus raising a substantial question of patentability. The question of patentability is new because Willens and ChoiceNet are being presented in a new light due to the material new interpretation provided by the Board in the Prior Reexamination.

**Patent No.: 6,779,118**  
**Request for *Ex Parte* Reexamination**

Because of this new interpretation, the application of Willens and ChoiceNet is substantially different in both context and scope from their prior consideration, with the differences being substantial and materially important to a reasonable examiner. Accordingly, Requestor respectfully requests that a reexamination be ordered for U.S. Pat. No. 6,779,118 to Ikudome et al.

Respectfully submitted,  
MONUMENT IP LAW GROUP

Dated: June 28, 2012

By: Donald D. Min/  
Donald D. Min  
Registration No. 47,796  
(202) 615-3000

**X. CERTIFICATE OF SERVICE**

Pursuant to 37 C.F.R. § 1.510(b)(5) and 37 C.F.R. § 1.33(c), I hereby certify that on June 28, 2012, a complete copy of this ex parte reexamination request, including the accompanying transmittal and all exhibits, are being served via First Class U.S. Mail upon the current attorneys of record for Applicants:

Herskovitz & Associates, LLC  
2845 Duke Street  
Alexandria VA 22314

By: /Donald D. Min/  
Donald D. Min

---

**EXHIBIT A**

**U.S. PATENT NO.: 6,779,118 (“THE ’118 PATENT”)**



US006779118B1

(12) **United States Patent**  
**Ikudome et al.**

(10) **Patent No.:** **US 6,779,118 B1**  
(45) **Date of Patent:** **Aug. 17, 2004**

(54) **USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM**

(75) Inventors: **Koichiro Ikudome**, Arcadia, CA (US);  
**Moon Tai Yeung**, Alhambra, CA (US)

(73) Assignee: **Auriq Systems, Inc.**, Pasadena, CA (US)

(\* ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

EP	0 854 621	7/1998
EP	0854621 A *	7/1998
WO	WO 96/05549	2/1996
WO	WO9605549 *	2/1996
WO	WO98/03927	1/1998
WO	WO9826548 *	6/1998
WO	WO 98/26548	6/1998
WO	WO 99/57660	11/1999
WO	WO 00/16529	3/2000

\* cited by examiner

(21) Appl. No.: **09/295,966**

(22) Filed: **Apr. 21, 1999**

**Related U.S. Application Data**

(60) Provisional application No. 60/084,014, filed on May 4, 1998.

(51) **Int. Cl.<sup>7</sup>** ..... **G06F 12/14**

(52) **U.S. Cl.** ..... **713/201**

(58) **Field of Search** ..... 713/200, 201, 713/202, 165, 168, 193; 709/229; 380/200, 201, 230; 340/825.31, 825.34; 705/57, 58

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

5,696,898 A	12/1997	Baker et al.	.....	395/187.01
6,157,829 A *	12/2000	Grube et al.	.....	455/414.1
6,233,686 B1	5/2001	Dutta		

**FOREIGN PATENT DOCUMENTS**

CA 2226814 3/2003

*Primary Examiner*—Pierre Elisca

(74) *Attorney, Agent, or Firm*—Christie, Parker & Hale, LLP

(57) **ABSTRACT**

A data redirection system for redirecting user's data based on a stored rule set. The redirection of data is performed by a redirection server, which receives the redirection rule sets for each user from an authentication and accounting server, and a database. Prior to using the system, users authenticate with the authentication and accounting server, and receive a network address. The authentication and accounting server retrieves the proper rule set for the user, and communicates the rule set and the user's address to the redirection server. The redirection server then implements the redirection rule set for the user's address. Rule sets are removed from the redirection server either when the user disconnects, or based on some predetermined event. New rule sets are added to the redirection server either when a user connects, or based on some predetermined event.

**27 Claims, 1 Drawing Sheet**

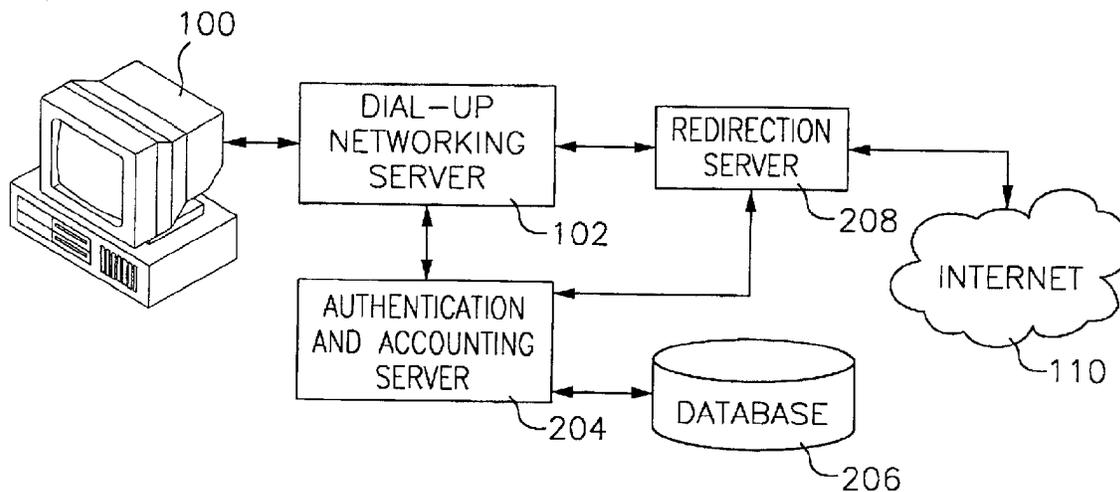


FIG. 1

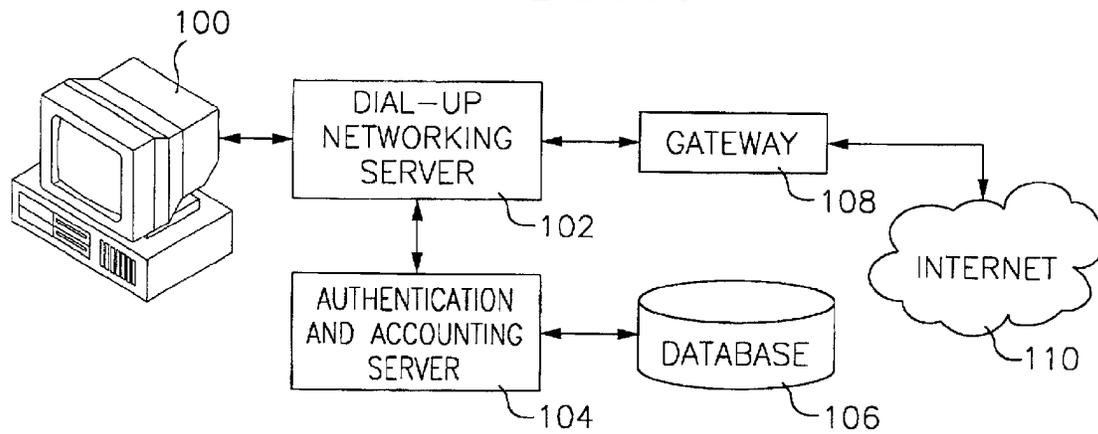
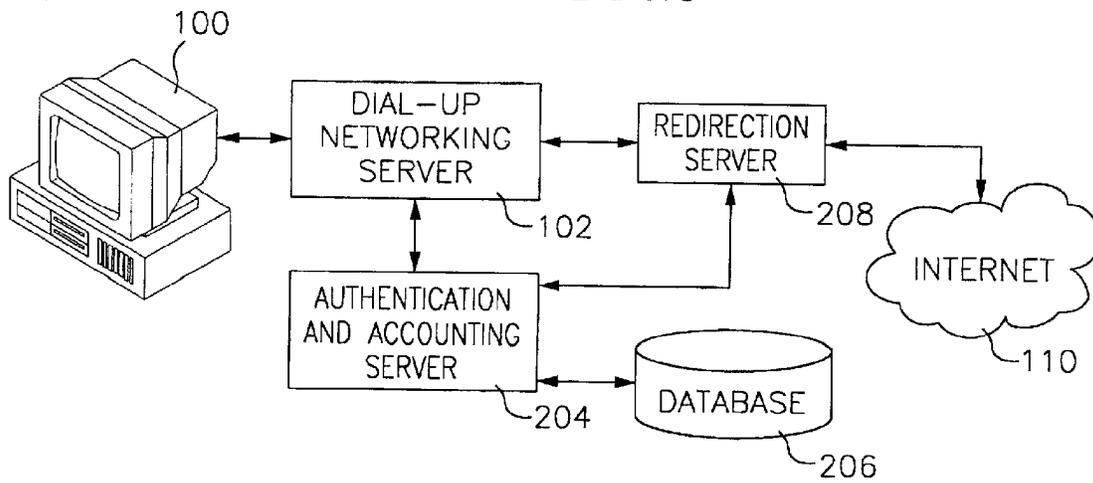


FIG. 2



1

## USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

### RELATED APPLICATION

This application claims priority of U.S. Provisional Application No. 60/084,014 filed May 4, 1998, the disclosure of which is incorporated fully herein by reference.

### FIELD OF THE INVENTION

This invention relates to the field of Internet communications, more particularly, to a database system for use in dynamically redirecting and filtering Internet traffic.

### BACKGROUND OF THE INVENTION

In prior art systems as shown in FIG. 1 when an Internet user establishes a connection with an Internet Service Provider (ISP), the user first makes a physical connection between their computer **100** and a dial-up networking server **102**, the user provides to the dial-up networking server their user ID and password. The dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server **104**. A detailed description of the IP communications protocol is discussed in *Internetworking with TCP/IP*, 3rd ed., Douglas Comer, Prentice Hall, 1995, which is fully incorporated herein by reference. The authentication and accounting server, upon verification of the user ID and password using a database **106** would send an authorization message to the dial-up networking server **102** to allow the user to use the temporary IP address assigned to that user by the dial-up networking server and then logs the connection and assigned IP address. For the duration of that session, whenever the user would make a request to the Internet **110** via a gateway **108**, the end user would be identified by the temporarily assigned IP address.

The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, redirection is not limited to WWW traffic, and the concept is valid for all IP services. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page—hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. Alternately, redirection can also be accomplished by coding the page such that it instructs the browser to run a program, like a Java applet or the like, which then redirects the browser. One disadvantage with current redirection technology is that control of the redirection is at the remote end, or WWW server end—and not the local, or user end. That is to say that the redirection is performed by the remote server, not the user's local gateway.

2

Filtering packets at the Internet Protocol (IP) layer has been possible using a firewall device or other packet filtering device for several years. Although packet filtering is most often used to filter packets coming into a private network for security purposes, once properly programed, they can filter outgoing packets sent from users to a specific destination as well. Packet filtering can distinguish, and filter based on, the type of IP service contained within an IP packet. For example, the packet filter can determine if the packet contains FTP (file transfer protocol) data, WWW data, or Telnet session data. Service identification is achieved by identifying the terminating port number contained within each IP packet header. Port numbers are standard within the industry to allow for interoperability between equipment. Packet filtering devices allow network administrators to filter packets based on the source and/or destination information, as well as on the type of service being transmitted within each IP packet. Unlike redirection technology, packet filtering technology allows control at the local end of the network connection, typically by the network administrator. However, packet filtering is very limited because it is static. Once packet filtering rule sets are programed into a firewall or other packet filter device, the rule set can only be changed by manually reprogramming the device.

Packet filter devices are often used with proxy server systems, which provide access control to the Internet and are most often used to control access to the world wide web. In a typical configuration, a firewall or other packet filtering device filters all WWW requests to the Internet from a local network, except for packets from the proxy server. That is to say that a packet filter or firewall blocks all traffic originating from within the local network which is destined for connection to a remote server on port **80** (the standard WWW port number). However, the packet filter or firewall permits such traffic to and from the proxy server. Typically, the proxy server is programed with a set of destinations that are to be blocked, and packets destined for blocked addresses are not forwarded. When the proxy server receives a packet, the destination is checked against a database for approval. If the destination is allowed, the proxy server simply forwards packets between the local user and the remote server outside the firewall. However, proxy servers are limited to either blocking or allowing specific system terminals access to remote databases.

A recent system is disclosed in U.S. Pat. No. 5,696,898. This patent discloses a system, similar to a proxy server, that allows network administrators to restrict specific IP addresses inside a firewall from accessing information from certain public or otherwise uncontrolled databases (i.e., the WWW/Internet). According to the disclosure, the system has a relational database which allows network administrators to restrict specific terminals, or groups of terminals, from accessing certain locations. Similarly limited as a proxy server, this invention can only block or allow terminals' access to remote sites. This system is also static in that rules programmed into the database need to be reprogramming in order to change which locations specific terminals may access.

### SUMMARY OF THE INVENTION

The present invention allows for creating and implementing dynamically changing rules, to allow the redirection, blocking, or allowing, of specific data traffic for specific users, as a function of database entries and the user's activity. In certain embodiments according to the present invention, when the user connects to the local network, as in the prior art system, the user's ID and password are sent to

the authentication accounting server. The user ID and password are checked against information in an authentication database. The database also contains personalized filtering and redirection information for the particular user ID. During the connection process, the dial-up network server provides the authentication accounting server with the IP address that is going to be temporarily assigned to the user. The authentication accounting server then sends both the user's temporary IP address and all of the particular user's filter and redirection information to a redirection server. The IP address temporarily assigned to the end user is then sent back to the end user for use in connecting to the network.

Once connected to the network, all data packets sent to, or received by, the user include the user's temporary IP address in the IP packet header. The redirection server uses the filter and redirection information supplied by the authentication accounting server, for that particular IP address, to either allow packets to pass through the redirection server unmolested, block the request all together, or modify the request according to the redirection information.

When the user terminates the connection with the network, the dial-up network server informs the authentication accounting server, which in turn, sends a message to the redirection server telling it to remove any remaining filtering and redirection information for the terminated user's temporary IP address. This then allows the dial-up network to reassign that IP address to another user. In such a case, the authentication accounting server retrieves the new user's filter and redirection information from the database and passes it, with the same IP address which is now being used by a different user, to the redirection server. This new user's filter may be different from the first user's filter.

#### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a typical Internet Service Provider environment.

FIG. 2 is a block diagram of an embodiment of an Internet Service Provider environment with integrated redirection system.

#### DETAILED DESCRIPTION OF THE INVENTION

In the following embodiments of the invention, common reference numerals are used to represent the same components. If the features of an embodiment are incorporated into a single system, these components can be shared and perform all the functions of the described embodiments.

FIG. 2. shows a typical Internet Service Provider (ISP) environment with integrated user specific automatic data redirection system. In a typical use of the system, a user employs a personal computer (PC) 100, which connects to the network. The system employs: a dial-up network server 102, an authentication accounting server 204, a database 206 and a redirection server 208.

The PC 100 first connects to the dial-up network server 102. The connection is typically created using a computer modem, however a local area network (LAN) or other communications link can be employed. The dial-up network server 102 is used to establish a communications link with the user's PC 100 using a standard communications protocol. In the preferred embodiment Point to Point Protocol (PPP) is used to establish the physical link between the PC 100 and the dial-up network server 102, and to dynamically assign the PC 100 an IP address from a list of available addresses. However, other embodiments may employ dif-

ferent communications protocols, and the IP address may also be permanently assigned to the PC 100. Dial-up network servers 102, PPP and dynamic IP address assignment are well known in the art.

An authentication accounting server with Auto-Navi component (hereinafter, authentication accounting server) 204 is used to authenticate user ID and permit, or deny, access to the network. The authentication accounting server 204 queries the database 206 to determine if the user ID is authorized to access the network. If the authentication accounting server 204 determines the user ID is authorized, the authentication accounting server 204 signals the dial-up network server 102 to assign the PC 100 an IP address, and the Auto-Navi component of the authentication accounting server 204 sends the redirection server 208 (1) the filter and redirection information stored in database 206 for that user ID and (2) the temporarily assigned IP address for the session. One example of an authentication accounting server is discussed in U.S. Pat. No. 5,845,070, which is fully incorporated here by reference. Other types of authentication accounting servers are known in the art. However, these authentication accounting servers lack an Auto-Navi component.

The system described herein operates based on user ID's supplied to it by a computer. Thus the system does not "know" who the human being "user" is at the keyboard of the computer that supplies a user ID. However, for the purposes of this detailed description, "user" will often be used as a short hand expression for "the person supplying inputs to a computer that is supplying the system with a particular user ID."

The database 206 is a relational database which stores the system data. FIG. 3 shows one embodiment of the database structure. The database, in the preferred embodiment, includes the following fields: a user account number, the services allowed or denied each user (for example: e-mail, Telnet, FTP, WWW), and the locations each user is allowed to access.

Rule sets are employed by the system and are unique for each user ID, or a group of user ID's. The rule sets specify elements or conditions about the user's session. Rule sets may contain data about a type of service which may or may not be accessed, a location which may or may not be accessed, how long to keep the rule set active, under what conditions the rule set should be removed, when and how to modify the rule set during a session, and the like. Rule sets may also have a preconfigured maximum lifetime to ensure their removal from the system.

The redirection server 208 is logically located between the user's computer 100 and the network, and controls the user's access to the network. The redirection server 208 performs all the central tasks of the system. The redirection server 208 receives information regarding newly established sessions from the authentication accounting server 204. The Auto-Navi component of the authentication accounting server 204 queries the database for the rule set to apply to each new session, and forwards the rule set and the currently assigned IP address to the redirection server 208. The redirection server 208 receives the IP address and rule set, and is programed to implement the rule set for the IP address, as well as other attendant logical decisions such as: checking data packets and blocking or allowing the packets as a function of the rule sets, performing the physical redirection of data packets based on the rule sets, and dynamically changing the rule sets based on conditions. When the redirection server 208 receives information

5

regarding a terminated session from the authentication accounting server 204, the redirection server 208 removes any outstanding rule sets and information associated with the session. The redirection server 208 also checks for and removes expired rule sets from time to time.

In an alternate embodiment, the redirection server 208 reports all or some selection of session information to the database 206. This information may then be used for reporting, or additional rule set generation.

System Features Overview

In the present embodiment, each specific user may be limited to, or allowed, specific IP services, such as WWW, FTP and Telnet. This allows a user, for example, WWW access, but not FTP access or Telnet access. A user's access can be dynamically changed by editing the user's database record and commanding the Auto-Navi component of the authentication accounting server 204 to transmit the user's new rule set and current IP address to the redirection server 208.

A user's access can be "locked" to only allow access to one location, or a set of locations, without affecting other users' access. Each time a locked user attempts to access another location, the redirection server 208 redirects the user to a default location. In such a case, the redirection server 208 acts either as proxy for the destination address, or in the case of WWW traffic the redirection server 208 replies to the user's request with a page containing a redirection command.

A user may also be periodically redirected to a location, based on a period of time or some other condition. For example, the user will first be redirected to a location regardless of what location the user attempts to reach, then permitted to access other locations, but every ten minutes the user is automatically redirected to the first location. The redirection server 208 accomplishes such a rule set by setting an initial temporary rule set to redirect all traffic; after the user accesses the redirected location, the redirection server then either replaces the temporary rule set with the user's standard rule set or removes the rule set altogether from the redirection server 208. After a certain or variable time period, such as ten minutes, the redirection server 208 reinstates the rule set again.

The following steps describe details of a typical user session:

A user connects to the dial-up network server 102 through computer 100.

The user inputs user ID and password to the dial-up network server 102 using computer 100 which forwards the information to the authentication accounting server 204

The authentication accounting server 204 queries database 206 and performs validation check of user ID and password.

Upon a successful user authentication, the dial-up network server 102 completes the negotiation and assigns an IP address to the user. Typically, the authentication accounting server 204 logs the connection in the database 206.

The Auto-Navi component of the authentication accounting server 204 then sends both the user's rule set (contained in database 206) and the user's IP address (assigned by the dial-up network server 102) in real time to the redirection server 208 so that it can filter the user's IP packets.

6

The redirection server 208 programs the rule set and IP address so as to control (filter, block, redirect, and the like) the user's data as a function of the rule set.

The following is an example of a typical user's rule set, attendant logic and operation:

If the rule set for a particular user (i.e., user UserID-2) was such as to only allow that user to access the web site www.us.com, and permit Telnet services, and redirect all web access from any server at xyz.com to www.us.com, then the logic would be as follows:

The database 206 would contain the following record for user UserID-2:

ID	UserID-2	
Password:	secret	
#####		
### Rule Sets ###		
#####		
#service	rule	expire
http	www.us.com	0
http	*.xyz.com=>www.us.com	0

the user initiates a session, and sends the correct user ID and password (UserID-2 and secret) to the dial-up network server 102. As both the user ID and password are correct, the authentication accounting server 204 authorizes the dial-up network server 102 to establish a session. The dial-up network server 102 assigns UserID-2 an IP address (for example, 10.0.0.1) to the user and passes the IP address to the authentication accounting server 204.

The Auto-Navi component of the authentication accounting server 204 sends both the user's rule set and the user's IP address (10.0.0.1) to the redirection server 208.

The redirection server 208 programs the rule set and IP address so as to filter and redirect the user's packets according to the rule set. The logic employed by the redirection server 208 to implement the rule set is as follows:

```
IF source IP-address=10.0.0.1 AND
  ( ((request type=HTTP) AND (destination address=
    www.us.com) ) OR (request type=Telnet)
  ) THEN ok.
IF source IP-address=10.0.0.1 AND
  ( (request type=HTTP) AND (destination address=
    *.xyz.com)
  ) THEN (redirect=www.us.com)
```

The redirection server 208 monitors all the IP packets, checking each against the rule set. In this situation, if IP address 10.0.0.1 (the address assigned to user ID UserID-2) attempts to send a packet containing HTTP data (i.e., attempts to connect to port 80 on any machine within the xyz.com domain) the traffic is redirected by the redirection server 208 to www.us.com. Similarly, if the user attempts to connect to any service other than HTTP at www.us.com or Telnet anywhere, the packet will simply be blocked by the redirection server 208.

When the user logs out or disconnects from the system, the redirection server will remove all remaining rule sets.

The following is another example of a typical user's rule set, attendant logic and operation:

If the rule set for a particular user (i.e., user UserID-3) was to force the user to visit the web site www.widgetsell.com, first, then to have unfettered access to other web sites, then the logic would be as follows:

The database 206 would contain the following record for user UserID-3;

ID	UserID-3	
Password:	top-secret	
#####		
### Rule Sets ###		
#####		
#service	rule	expire
http	*=>www.widgetsell.com	1x

the user initiates a session, and sends the correct user ID and password (UserID-3 and top-secret) to the dial-up network server 102. As both the user ID and password are correct, the authentication accounting server 204 authorizes the dial-up network server 102 to establish a session. The dial-up network server 102 assigns user ID 3 an IP address (for example, 10.0.0.1) to the user and passes the IP address to the authentication accounting server 204.

The Auto-Navi component of the authentication accounting server 204 sends both the user's rule set and the user's IP address (10.0.0.1) to the redirection server 208.

The redirection server 208 programs the rule set and IP address so as to filter and redirect the user's packets according to the rule set. The logic employed by the redirection server 208 to implement the rule set is as follows:

```
IF source IP-address=10.0.0.1 AND
  (request type=HTTP) THEN (redirect=
  www.widgetsell.com)
THEN SET NEW RULE
IF source IP-address=10.0.0.1 AND
  (request type=HTTP) THEN ok.
```

The redirection server 208 monitors all the IP packets, checking each against the rule set. In this situation, if IP address 10.0.0.1 (the address assigned to user ID UserID-3) attempts to send a packet containing HTTP data (i.e., attempts to connect to port 80 on any machine) the traffic is redirected by the redirection server 208 to www.widgetsell.com. Once this is done, the redirection server 208 will remove the rule set and the user is free to use the web unmolested.

When the user logs out or disconnects from the system, the redirection server will remove all remaining rule sets.

In an alternate embodiment a user may be periodically redirected to a location, based on the number of other factors, such as the number of locations accessed, the time spent at a location, the types of locations accessed, and other such factors.

A user's account can also be disabled after the user has exceeded a length of time. The authentication accounting server 204 keeps track of user's time online. Prepaid use subscriptions can thus be easily managed by the authentication accounting Server 204.

In yet another embodiment, signals from the Internet 110 side of redirection server 208 can be used to modify rule sets being used by the redirection server. Preferably, encryption and/or authentication are used to verify that the server or other computer on the Internet 110 side of redirection server 208 is authorized to modify the rule set or rule sets that are being attempted to be modified. An example of this embodiment is where it is desired that a user be redirected to a particular web site until the fill out a questionnaire or satisfy some other requirement on such a web site. In this example,

the redirection server redirects a user to a particular web site that includes a questionnaire. After this web site receives acceptable data in all required fields, the web site then sends an authorization to the redirection server that deletes the redirection to the questionnaire web site from the rule set for the user who successfully completed the questionnaire. Of course, the type of modification an outside server can make to a rule set on the redirection server is not limited to deleting a redirection rule, but can include any other type of modification to the rule set that is supported by the redirection server as discussed above.

It will be clear to one skilled in the art that the invention may be implemented to control (block, allow and redirect) any type of service, such as Telnet, FTP, WWW and the like. The invention is easily programmed to accommodate new services or networks and is not limited to those services and networks (e.g., the Internet) now known in the art.

It will also be clear that the invention may be implemented on a non-IP based networks which implement other addressing schemes, such as IPX, MAC addresses and the like. While the operational environment detailed in the preferred embodiment is that of an ISP connecting users to the Internet, it will be clear to one skilled in the art that the invention may be implemented in any application where control over users' access to a network or network resources is needed, such as a local area network, wide area network and the like. Accordingly, neither the environment nor the communications protocols are limited to those discussed.

What is claimed is:

1. A system comprising:

- a database with entries correlating each of a plurality of user IDs with an individualized rule set;
- a dial-up network server that receives user IDs from users' computers;
- a redirection server connected to the dial-up network server and a public network, and
- an authentication accounting server connected to the database, the dial-up network server and the redirection server;
- wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;
- wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and
- wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

2. The system of claim 1, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.

3. The system of claim 1, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.

4. The system of claim 1, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.

5. The system of claim 1, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.

6. The system of claim 1, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.

9

7. The system of claim 1, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.

8. In a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected to the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server, the method comprising the steps of:

communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;

communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server;

and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.

9. The method of claim 8, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.

10. The method of claim 8, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.

11. The method of claim 8, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.

12. The method of claim 8, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.

13. The method of claim 8, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.

14. The method of claim 8, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.

15. A system comprising:

a redirection server programed with a user's rule set correlated to a temporarily assigned network address;

wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user access.

16. The system of claim 15, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

17. The system of claim 15, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

10

18. The system of claim 15, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user access.

19. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

20. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

21. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user access.

22. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user access.

23. The system of claim 15, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

24. The system of claim 23 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.

25. In a system comprising a redirection server containing a user's rule set correlated to a temporarily assigned network address wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network; the method comprising the step of:

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.

26. The method of claim 25, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user access.

27. The method of claim 25, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and the location or locations the user access.

\* \* \* \* \*



US006779118C1

(12) **EX PARTE REEXAMINATION CERTIFICATE** (8926th)  
**United States Patent**

**Ikudome et al.**

(10) **Number:** **US 6,779,118 C1**

(45) **Certificate Issued:** **Mar. 27, 2012**

(54) **USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM**

(75) Inventors: **Koichiro Ikudome**, Arcadia, CA (US);  
**Moon Tai Yeung**, Alhambra, CA (US)

(73) Assignee: **Linksmart Wireless Technology, LLC**,  
Pasadena, CA (US)

**Reexamination Request:**

No. 90/009,301, Dec. 17, 2008

**Reexamination Certificate for:**

Patent No.: **6,779,118**  
Issued: **Aug. 17, 2004**  
Appl. No.: **09/295,966**  
Filed: **Apr. 21, 1999**

**Related U.S. Application Data**

(60) Provisional application No. 60/084,014, filed on May 4, 1998.

(51) **Int. Cl.**

**H04L 29/06** (2006.01)  
**H04L 29/00** (2006.01)

(52) **U.S. Cl.** ..... **726/7; 726/14**

(58) **Field of Classification Search** ..... **726/8**  
See application file for complete search history.

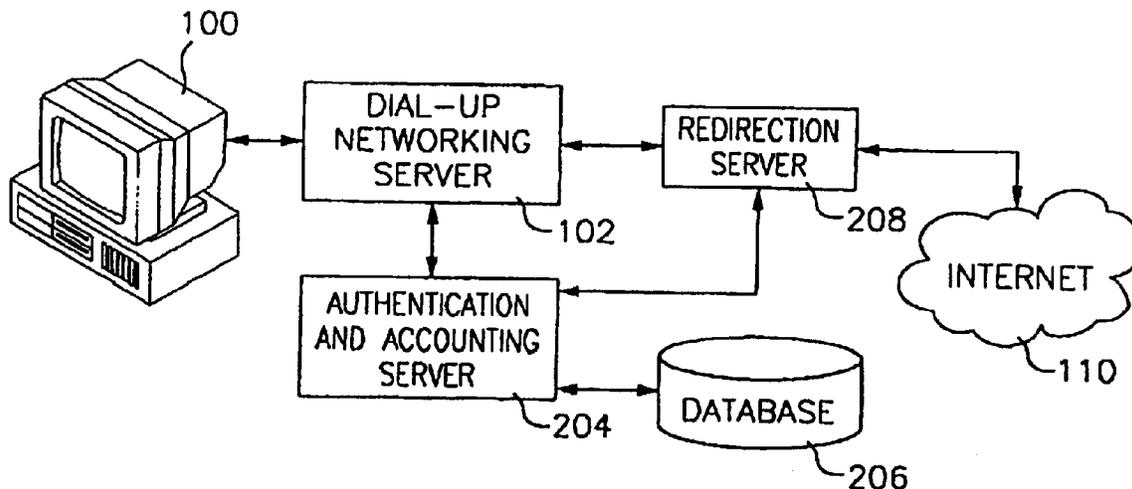
(56) **References Cited**

To view the complete listing of prior art documents cited during the proceeding for Reexamination Control Number 90/009,301, please refer to the USPTO's public Patent Application Information Retrieval (PAIR) system under the Display References tab.

*Primary Examiner*—Samuel Rimell

(57) **ABSTRACT**

A data redirection system for redirecting user's data based on a stored rule set. The redirection of data is performed by a redirection server, which receives the redirection rule sets for each user from an authentication and accounting server, and a database. Prior to using the system, users authenticate with the authentication and accounting server, and receive a network address. The authentication and accounting server retrieves the proper rule set for the user, and communicates the rule set and the user's address to the redirection server. The redirection server then implements the redirection rule set for the user's address. Rule sets are removed from the redirection server either when the user disconnects, or based on some predetermined event. New rule sets are added to the redirection server either when a user connects, or based on some predetermined event.



**1**  
**EX PARTE**  
**REEXAMINATION CERTIFICATE**  
**ISSUED UNDER 35 U.S.C. 307**

THE PATENT IS HEREBY AMENDED AS  
INDICATED BELOW.

**Matter enclosed in heavy brackets [ ] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.**

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims 2-7 and 9-14 is confirmed.

Claims 1, 8, 15 and 25 are cancelled.

Claims 16-23 and 26-27 are determined to be patentable as amended.

Claim 24, dependent on an amended claim, is determined to be patentable.

New claims 28-90 are added and determined to be patentable.

16. [The system of claim 15.] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and*

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

17. [The system of claim 15.] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and*

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

**2**

18. [The system of claim 15.] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and*

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user [access] accesses.

19. [The system of claim 15.] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and*

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

20. [The system of claim 15.] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and*

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

21. [The system of claim 15.] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*

*wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;*

3

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user [access] accesses.

22. [The system of claim 15.] A system comprising:  
a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user [access] accesses.

23. [The system of claim 15.] A system comprising:  
a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

26. The method of claim 25, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user [access] accesses.

27. The method of claim 25, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and [the] a location or locations the user [access] accesses.

28. The system of claim 1, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

29. The system of claim 1, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

4

30. The system of claim 1, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

31. The system of claim 1, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

32. The method of claim 8, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

33. The method of claim 8, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

34. The method of claim 8, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

35. The method of claim 8, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

36. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

37. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

38. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

5

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

39. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

40. The method of claim 25, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

41. The method of claim 25, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

42. The method of claim 25, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

43. The method of claim 25, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

44. A system comprising:

a database with entries correlating each of a plurality of user IDs with an individualized rule set;

a dial-up network server that receives user IDs from users' computers;

a redirection server connected between the dial-up network server and a public network, and

an authentication accounting server connected to the database, the dial-up network server and the redirection server;

wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;

wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and

wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

45. The system of claim 44, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.

6

46. The system of claim 44, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.

47. The system of claim 44, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.

48. The system of claim 44, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.

49. The system of claim 44, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.

50. The system of claim 44, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.

51. The system of claim 44, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

52. The system of claim 44, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

53. The system of claim 44, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

54. The system of claim 44, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

55. The system of claim 44, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

56. In a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected between the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection servers, a method comprising the steps of:

communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;

communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server;

and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.

57. The method of claim 56, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.

58. The method of claim 56, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.

59. The method of claim 56, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.

60. The method of claim 56, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.

61. The method of claim 56, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.

7

62. The method of claim 56, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.

63. The method of claim 56, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

64. The method of claim 56, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

65. The method of claim 56, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

66. The method of claim 56, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

67. The method of claim 56, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

68. A system comprising:

a redirection server connected between a user computer and a public network, the redirection server programmed with a users' rule set correlated to a temporarily assigned network address;

wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses.

69. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

70. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

71. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.

72. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

73. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

74. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.

75. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.

8

76. The system of claim 68, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

77. The system of claim 68 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.

78. The system of claim 68, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

79. The system of claim 68, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

80. The system of claim 68, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

81. The system of claim 68, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

82. The system of claim 68, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the modified rule set.

83. In a system comprising a redirection server connected between a user computer and a public network, the redirection server containing a user's rule set correlated to a temporarily assigned network address wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network; a method comprising the step of:

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.

84. The method of claim 83, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.

85. The method of claim 83, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.

86. The method of claim 83, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

87. The method of claim 83, wherein the modified rule set includes an initial temporary rule set and a standard rule

9

set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

88. The method of claim 83, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

89. The method of claim 83, wherein the modified rule set includes at least one rule redirecting the data to a new desti-

10

nation address based on a request type and an attempted destination address.

90. The method of claim 83, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet Protocol) packet header by a second destination address as a function of the individualized rule set.

\* \* \* \* \*

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		
	First Named Inventor	Koichiro Ikudome	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	MIPIKU.002RE	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	5889958		1990-03-30	Willens	
	2	6088451		2000-07-11	He et al.	
	3	6233686		2011-05-15	Zenchelsky et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup>	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
	1							<input type="checkbox"/>

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		
	First Named Inventor	Koichiro Ikudome	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	MIPIKU.002RE	

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>
	1	"The ChoiceNet(TM) Administrator's Guide," Livingston Enterprises, 88 pages, January 1997	<input type="checkbox"/>
	2	Ex parte Linksmart Wireless Technology, LLC, No. 2011-009566 (B.P.A.I., August 23, 2011)	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

**EXAMINER SIGNATURE**

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		
Filing Date		
First Named Inventor	Koichiro Ikudome	
Art Unit		
Examiner Name		
Attorney Docket Number	MIPIKU.002RE	

**CERTIFICATION STATEMENT**

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- See attached certification statement.
- The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- A certification statement is not submitted herewith.

**SIGNATURE**

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Donald D. Min/	Date (YYYY-MM-DD)	2012-06-28
Name/Print	Donald D. Min	Registration Number	47796

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	
<b>Filing Date:</b>	
<b>Title of Invention:</b>	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
<b>First Named Inventor/Applicant Name:</b>	KOICHIRO IKUDOME
<b>Filer:</b>	Donald Dongwhan Min
<b>Attorney Docket Number:</b>	MIPIKU.002RE

Filed as Large Entity

### ex parte reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
Request for ex parte reexamination	1812	1	2520	2520

**Pages:**

**Claims:**

**Miscellaneous-Filing:**

**Petition:**

**Patent-Appeals-and-Interference:**

**Post-Allowance-and-Post-Issuance:**

**Extension-of-Time:**

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>2520</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	13134300
<b>Application Number:</b>	90012378
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	2926
<b>Title of Invention:</b>	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
<b>First Named Inventor/Applicant Name:</b>	KOICHIRO IKUDOME
<b>Customer Number:</b>	90934
<b>Filer:</b>	Donald Dongwhan Min
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	MIPIKU.002RE
<b>Receipt Date:</b>	28-JUN-2012
<b>Filing Date:</b>	
<b>Time Stamp:</b>	16:36:29
<b>Application Type:</b>	Reexam (Third Party)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$2520
RAM confirmation Number	4255
Deposit Account	
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part (if appl.)	Pages (if appl.)

1	Transmittal Letter	2012-06-28_Reexamination_Transmittal_Form-MIPIKU-002RE.PDF	776151 7577836a349ee87162915d4a7672f32cb8e521f5	no	3
<b>Warnings:</b>					
<b>Information:</b>					
2	Receipt of Orig. Ex Parte Request by Third Party	FINAL-Request_for_ex_parte_Reexamination-MIPIKU-002RE.pdf	25838021 1a467fd489655f00467fd9a91ef01c06353c182c	no	428
<b>Warnings:</b>					
<b>Information:</b>					
3	Reexam - Info Disclosure Statement Filed by 3rd Party	2012-06-28_IDS_List-MIPIKU-002RE.pdf	260477 b74a31fa1f1e7cd4931d2ab3809805f1b3478e47	no	4
<b>Warnings:</b>					
<b>Information:</b>					
4	Fee Worksheet (SB06)	fee-info.pdf	29565 8b9f33077aaec9084777dc96e6ea9eb7d05fc203	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>				26904214	

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

