

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Fortinet, Inc.,

Petitioner,

v.

Netskope, Inc.,

Patent Owner.

Case No. 2026-0040

U.S. Patent 8,356,336

PETITION FOR *INTER PARTES* REVIEW

Mail Stop "PATENT BOARD"

Patent Trial and Appeal Board

U.S. Patent Trademark Office

P.O. Box 1450

Alexandria, VA 22313-1450

TABLE OF CONTENTS

	<u>Page</u>
TABLE OF AUTHORITIES	viii
TABLE OF ABBREVIATIONS	ix
EXHIBIT LIST	x
I. INTRODUCTION	1
II. Requirements for inter partes review	3
A. GROUNDS FOR STANDING (37 C.F.R. §42.104(a)).....	3
B. Identification of Challenge.....	3
1. The Specific Art on Which the Challenge is Based.....	4
2. Statutory Grounds on Which the Challenge is Based.....	4
3. How the Challenged Claims are Unpatentable	4
III. THE PATENT AND STATE OF THE ART	5
A. Technology Background	5
B. The '336 Patent.....	7
C. File History.....	11
D. POSITA.....	12
IV. Claim Construction.....	13
A. "anonymous user"	13
B. "pre-authentication capture destination"	14
C. "authentication token"	15
V. Grounds of Unpatentability	17

A.	Grounds 1 and 2: Claims 1--18 Are Anticipated, Or At Least Rendered Obvious By, Subbiah	19
1.	Overview of Subbiah	19
2.	Independent Claim 1	23
3.	Claim 2: " The method according to claim 1, wherein the network resource is at a network location external to the shared network."	37
4.	Claim [3]: " The method according to claim 1, wherein the redirecting further comprises sending from the network access controller to the client device a response containing an identifier identifying the pre-authentication capture destination."	38
5.	Claim [4]: "The method according to claim 1, further comprising: redirecting the browser application running on the client device back to the preauthentication capture destination when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality of server computers in the shared network."	40
6.	Claim 5.....	42
7.	Claim [6]: "The method according to claim 5, wherein the second request does not contain the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network."	45
8.	Claim [7]: "The method according to claim 5, wherein the second request contains the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."	47

9.	Claim [8]: "The method according to claim 7, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network."	48
10.	Claim 9.....	50
11.	Claim [10]: "The computer program product of claim 9, wherein the redirecting further comprises sending from the network access controller to the client device a response containing an identifier identifying the pre-authentication capture destination."	52
12.	Claim [11]: "The computer program product of claim 9, wherein the computer instructions are further translatable by the processor to perform: redirecting the browser application running on the client device back to the preauthentication capture destination when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality of server computers in the shared network."	53
13.	Claim 12.....	53
14.	Claim 13.....	53
15.	Claim 14.....	54
16.	Claim 15.....	54
17.	Claim 16.....	55
18.	Claim [17]: "The apparatus of claim 16, wherein the computer instructions are further translatable by the processor to redirect the browser application running on the client device back to the preauthentication capture destination when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality of server computers in the shared network."	56

19.	Claim [18]: "The apparatus of claim 16, further comprising: a first network interface coupled to the processor, wherein the computer instructions are further translatable by the processor to continuously monitor for network access from client devices on the first network interface."	56
20.	Claim 19.....	57
21.	Claim 20.....	58
B.	Ground 3 – Obviousness in view of Hinton and/or Crandell.....	59
1.	Overview of Hinton and Motivation to Combine with Subbiah	59
2.	Overview of Crandell and Motivation to Combine	61
3.	Claim [5pre]: "The method according to claim 1, further comprising:"	65
4.	Claim [5a]: "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"	65
5.	Claim [5b]: "determining whether the second request contains an authentication token."	66
6.	Claim [6]: "The method according to claim 5, wherein the second request does not contain the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network."	67

7. Claim [7]: "The method according to claim 5, wherein the second request contains the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network." 68
8. Claim [8]: "The method according to claim 7, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network." 68
9. Claim [12a]: "The computer program product of claim 9, wherein the computer instructions are further translatable by the processor to perform:" 68
10. Claim [12b]: "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and" 69
11. Claim [12c]: "determining whether the second request contains an authentication token." 69
12. Claim [13a]: "The computer program product of claim 12, wherein the second request does not contain the authentication token and wherein the computer instructions are further translatable by the processor to perform:" 69
13. Claim [13b]: "redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network." 69
14. Claim [14a]: "The computer program product of claim 12, wherein the second request contains the authentication token and wherein the computer instructions are further translatable by the processor to perform:" 69

15.	Claim [14b]: "redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."	70
16.	Claim [15a]: "The computer program product of claim 14, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network and wherein the computer instructions are further translatable by the processor to perform:"	70
17.	Claim [15b]: " allowing the client device access to the second network resource."	70
18.	Claim [19]: "The apparatus of claim 18, wherein the computer instructions are further translatable by the processor to perform:"	70
19.	Claim [19a]: "intercepting a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"	70
20.	Claim [19b]: "determining whether the second request contains an authentication token."	70
21.	Claim [20pre]: "The apparatus of claim 19, wherein the computer instructions are further translatable by the processor to perform:"	71
22.	Claim [20a]: "if the second request does not contain the authentication token, redirecting the browser application running on the client device associated with the anonymous user back to the preauthentication capture destination hosted on the first server computer in the shared network; and"	71

23.	Claim [20b]: "if the second request contains the authentication token, redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."	71
VI.	MANDATORY Notices Under 37 C.F.R. §42.8(a)(1)	71
A.	37 C.F.R. §42.8(b)(1): Real Parties-In-Interest.....	71
B.	37 C.F.R. §42.8(b)(2): Related Matters	71
C.	37 C.F.R. §42.8(b)(3)-(4): Lead and Back-Up Counsel and Service Information.....	71
VII.	FEES UNDER 37 C.F.R. §42.103	72
VIII.	CONCLUSION	72

TABLE OF AUTHORITIES

Cases

<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	13
--	----

Statutes

35 U.S.C. §102.....	4
35 U.S.C. §103.....	4
35 U.S.C. §311.....	1

Rules

37 C.F.R. §42.100(b), ...	13
37 C.F.R. §42.104(b)	3
37 C.F.R. §42.104(b)(4)	4
37 C.F.R. §42.104(b)(5)	4
37 C.F.R. §42.103	72
37 C.F.R. §42.21	1
37 C.F.R. §42.8(b)(1):	71
37 C.F.R. §42.8(b)(2)	71
37 C.F.R. §42.8(b)(3)	71
37 C.F.R. §42.8(b)(4)	71

TABLE OF ABBREVIATIONS

Abbreviation	Full Name
'336 patent	U.S. Patent No. 8,356,336
Challenged Claims	Claims 1-20 of the '336 patent
Patent Owner, PO	Patent Owner Netskope, Inc.
Petitioner	Petitioner Fortinet, Inc.
POSITA	Person of Ordinary Skill In The Art

EXHIBIT LIST

Exhibit No.	Document
1001	U.S. Patent No. 8,356,336 ("the '336 patent")
1002	File History of the '336 patent
1003	Declaration of Dr. John Black, Jr.
1004	U.K. Patent Application GB2389010A ("Subbiah")
1005	PCT Publication No. WO 2002/039237 ("Hinton")
1006	U.S. Patent Appl. No. US 2004/0177276 ("MacKinnon")
1007	Crandell et al., <i>A Secure and Transparent Firewall Web Proxy</i> ("Crandell")
1008	Bauer et al., <i>Designing and Using DMZ Networks to Protect Internet Servers</i> ("Bauer")

I. INTRODUCTION

Petitioner Fortinet, Inc. ("Petitioner") respectfully petitions, under 35 U.S.C. §311 and 37 C.F.R. §42.21, for *inter partes* review ("IPR") of claims 1-20 ("the Challenged Claims") of U.S. Patent No. 8,356,336 ("the '336 patent") (EX1001) on the grounds below.¹

The '336 patent generally relates to a method of controlling network access for clients within a private and public network. *See* EX1001, 1:25-38. "For example, a shopping mall owner may want to provide any on-site customer possessing a wireless device...with access to the Web server for the mall, plus one or more other Web sites that are associated with the mall" and stored on a local Web server. EX1001, 1:39-44. This "collection of Web servers that the mall owner will allow an anonymous user to visit is referred to as the 'walled garden'." *Id.*, 1:44-47. In addition, the mall owner may grant Internet access to customers who authenticate themselves. *See id.*, 1:48-55. The '336 patent admits that such "walled gardens" and public/private network infrastructures were already known in the art. *E.g.*, EX1001, 3:14-4:37 (incorporating prior art references).

The '336 patent's purported invention is the redirection of unauthenticated network traffic within a shared network to a "Pre-Authentication Capture Destination"—*i.e.*, a pre-defined destination within a closed network (or "walled

¹ Unless otherwise noted, all emphases and annotations have been added.

garden"). EX1001, 1:66-2:19. Properly authenticated users of the shared network have access to external networks, such as the Internet. *See id.*, 5:24-39. In contrast, an unauthenticated user is "free to visit any of the servers that are included in the walled garden without authentication[, but any] attempt to access a web site or location that is outside of the walled garden will cause the client to be re-directed back to the Pre-Authentication Capture Destination." EX1001, 2:14-19; EX1003, ¶¶65-66.

But as discussed herein, it was already well known to redirect network requests by unauthenticated users to a pre-defined set of destinations within a shared network while allowing external Internet access only to authorized users. For example, **Subbiah** (EX1004) discloses a "method for providing communications network access in a public area." EX1004, Abstract. The method includes determining whether the network request is for access to a "local domain" of the communications network (*e.g.*, "a WLAN in an airport or mall") or to an external domain (*e.g.*, the Internet) and, "[i]n response to receiving a request for access to the first area, access is provided.... In response to receiving a request for access to the second area, an authentication process [] is performed." *Id.* As **Subbiah** further discloses, its system "can authenticate which users are paying, authenticated users, and ensure Internet access is provided to those users" while unauthenticated users are provided access to only "the information and services of the first area" (*i.e.*, the

local domain). EX1004, 13:14-22. And like the purported invention of the '336 patent, **Subbiah** discloses redirecting unauthenticated users to a predefined location on the internal domain: "The main Web page 400 is the Web page to which the browser of client 340 is redirected. The Web page 400 typically functions as the 'front page' or 'splash page' of the local network 301." EX1004, 16:1-6.

Thus, as further explained below, **Subbiah** anticipates claims 1-20 and, at minimum, renders obvious these claims.

II. REQUIREMENTS FOR INTER PARTES REVIEW

A. GROUNDS FOR STANDING (37 C.F.R. §42.104(a))

Petitioner certifies that the '336 patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR of the Challenged Claims on the grounds in this petition. The '336 patent issued more than nine months ago, and Petitioner was served with the complaint alleging infringement of the '336 patent less than one year ago.

B. Identification of Challenge

Pursuant to §42.104(b), Petitioner requests IPR of claims 1-20, and that the Board cancel the same as unpatentable. The '336 patent matured from U.S. Application No. 12/619,560 (filed 11/16/2009), and claims priority to U.S. Provisional Application No. 60/551,705 (filed 03/10/2004), and U.S. Provisional Application No. 60/551,702 (filed 03/10/2004). The '336 patent is thus a pre-AIA

patent and any reference to §§102, 103 herein is a reference to the pre-AIA language of that statute under Title 35 of the U.S.C.

1. The Specific Art on Which the Challenge is Based

Name	Exhibit	Patent / Publication	Filed	Issued / Published	Prior art under at least
Subbiah	1004	GB2389010	03/26/2003	11/26/2003	§102(a)
Hinton	1005	WO 2002/039237	10/25/2001	05/16/2002	§102(b)
Crandell	1007	"A Secure and Transparent Firewall Web Proxy"	N/A	Oct. 26-31, 2003	§102(a)

Each of the above references is prior art to the '336 patent based on the purported 03/10/2004 priority dates for the provisional applications to which the '336 patent claims priority.²

2. Statutory Grounds on Which the Challenge is Based

Ground	Claims	Basis	Prior Art
1	1-4, 9-11, 16-18	§102	Subbiah
2	1-4, 9-11, 16-18	§103	Subbiah
3	5-8, 12-15, 19-20	§103	Subbiah in view of Hinton

3. How the Challenged Claims are Unpatentable

Petitioner provides the information required under 37 C.F.R. §§42.104(b)(4)-(5) in §V.

² For purposes of this filing, Petitioner takes no position on whether the '336 patent is entitled to the 03/10/2004 priority date and the unpatentability of the claims over the art cited in this IPR does not require resolution of this issue.

III. THE PATENT AND STATE OF THE ART

A. Technology Background

The '336 patent generally relates to methods for controlling network access within public and private networks and, in particular, with "walled gardens" and "captive portals." EX1001, 1:25-38, 1:66-2:19. Such public and private networks were well known in the art, as were methods of requesting, redirecting, and accessing such networks and network locations. EX1003, ¶¶42-64.

Any networked device can, in theory, connect to any other device on that network, or on a connected network, so long as the device's address (*e.g.*, IP address, such as "23.66.124.110") is known to the other. EX1003, ¶¶44-49. An IP address is theoretically the globally unique address for a given computer or network, but it may be further shared by multiple computers (akin to multiple apartments in a building all sharing the same street address) in order to stretch the number of available addresses. *Id.*, ¶¶48-49. In any event, in order to simplify the Internet browsing process, we often use domain names (demarcated by a URL or URI) rather than an IP address to identify a website. EX1003, ¶50. For example, instead of requiring users to remember "23.66.124.110," browsers instead allow the user to navigate to "www.whitehouse.gov," and a Domain Name Service ("DNS") translation function will match the Domain Name to the IP address and navigate accordingly. *Id.*

In the 2004 timeframe, web-based communications commonly relied on a protocol referred to as "HyperText Transmission Protocol" or "HTTP," which is sent between a computer browser and a web server. EX1003, ¶52. A common HTTP request from a browser is the "GET request"—a plaintext request that starts with the word "GET" followed by a URI naming the requested resource and "HTTP/x.x" indicating the version of HTTP being used. *Id.*, ¶53. The most common version of HTTP in that timeframe was version 1.1. *Id.*, ¶52.

After receiving a GET request, the server typically responds with an HTTP response followed by the contents of the requested resource, which is often expressed using HTML code, which the browser then renders for the user's screen. EX1003, ¶54. Another common technique in that timeframe was HTTP redirection, in which the server would redirect the browser from the requested resource to a different resource. *See* EX1006, [0044]; EX1003, ¶¶57, 81.

A GET request can also include parameters—additional pieces of information appended to the URL—that may indicate information relevant to the request. This could include, for example, information about the computer making the request (such as its zip code) that was requested by the server: *e.g.*, GET <http://www.colorado.edu/showmap.html?zipcode=80027>. EX1003, ¶55. In addition to the URL itself, the HTTP request often includes header information (like metadata) as part of the request. *Id.*, ¶57. That metadata can include additional state

information and tokens (such as "cookies") for the server. *Id.*, ¶60. These cookies are sometimes used to track users (*e.g.*, for advertising purposes) or sessions (*e.g.*, notifying the server that the user already logged in and is permitted to continue using the resource so long as the session is not broken). *Id.*

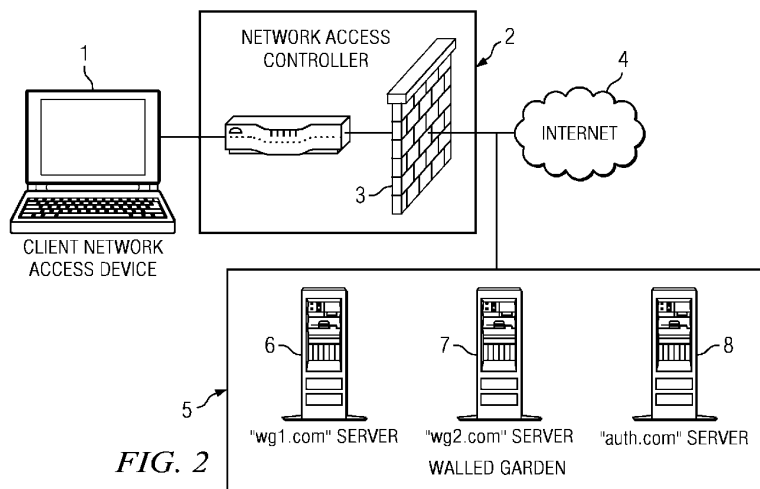
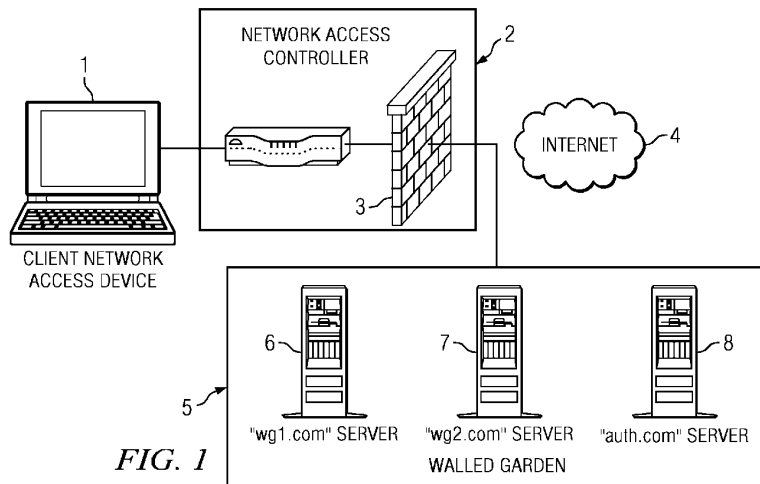
B. The '336 Patent

The '336 patent generally relates to a method of controlling network access for clients within a private and public network. EX1001, 1:25-38. "For example, a shopping mall owner may want to provide any on-site customer possessing a wireless device...with access to the Web server for the mall, plus one or more other Web sites that are associated with the mall" and stored on a local Web server. *Id.*, 1:39-44. This "collection of Web servers that the mall owner will allow an anonymous user to visit is referred to as the 'walled garden'." *Id.*, 1:44-47. In addition, the mall owner may grant Internet access to customers who authenticate themselves. *See id.*, 1:48-55.

The purported invention of the independent claims of the '336 patent is the redirection of unauthenticated network traffic within the shared, or local, network to a "Pre-Authentication Capture Destination"—*i.e.*, a pre-defined destination within the "walled garden," like a welcome screen. EX1001, 1:66-2:19. Properly authenticated users of the shared network have access to external networks, such as the Internet. *See id.*, 5:24-39. In contrast, an unauthenticated (or anonymous) user

is "free to visit any of the servers that are included in the walled garden without authentication[, but any] attempt to access a web site or location that is outside of the walled garden will cause the client to be re-directed back to the Pre-Authentication Capture Destination." *Id.*, 2:14-19. Certain dependent claims include a determination whether the request for network access includes an "authentication token." *E.g., id.*, claims 5, 12, 19; *see* EX1003, ¶67. As the specification explains, this token is "a unique sequence of characters" within the request and, "because of the presence of the Authentication token within the HTTP URL, the Network Access Controller will re-direct the client to [an] authentication screen" instead of the Pre-Authentication Capture Destination. EX1001, 2:31-40.

As depicted in Figures 1 and 2, the '336 patent discloses a system with a client device connected (1) to a series of local servers within a "walled garden" and (2) to the Internet via a Network Access Controller:



As the '336 patent explains, Figure 1 above illustrates the "network access capability afforded to an unauthenticated client" (*i.e.*, the client is restricted to the walled garden), while Figure 2 illustrates the "network access capability afforded to an authenticated client" (*i.e.*, the client can also access the Internet). EX1001, 3:1-6; EX1003, ¶68. Thus, both authenticated and unauthenticated users may access the local servers within the "walled garden," but only authenticated users may access the Internet. EX1003, ¶70.

Figure 3 of the '336 patent discloses the steps of the claimed method. As illustrated in Figure 3, the method includes four determinations used to control and direct access to content:

(1) Is the user authenticated? (Step 20)

(2) Is the destination local (*i.e.*, in the walled garden)? (Step 21)

(3) Is the destination a URL? (Step 22)³

(4) Does URL have a token? (Step 23)

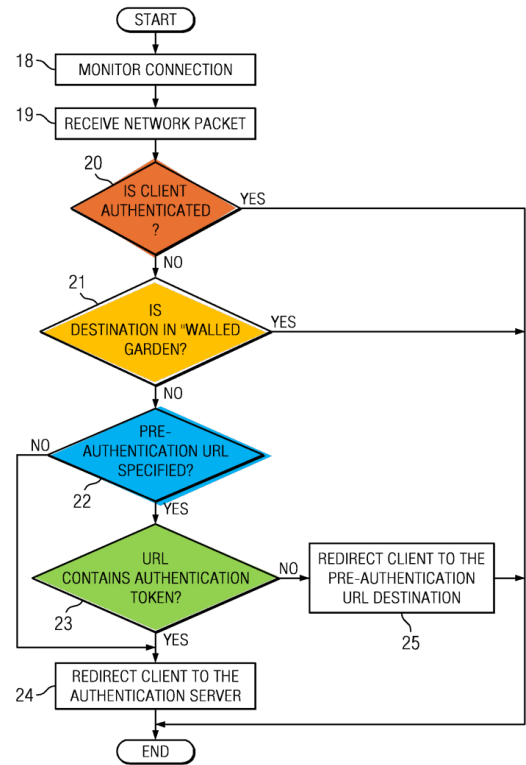


FIG. 3

In this purported invention, an authenticated client is permitted access to whatever resource is requested. EX1001, 5:45-50; *id.*, FIG. 3. Likewise, regardless of authentication, a client is permitted access to any resource within the walled garden. *Id.*, 5:51-58; *id.*, FIG. 3. Unauthenticated users, however, will be redirected either to the "Pre-Authentication Capture Destination" (if no token is included in the

³ While this determination is part of the '336 patent's disclosed process (and already disclosed by **Subbiah**, *infra* § V.A.1), it is not claimed. EX1003, ¶70.

request) or to the authentication server (if a token is included or if the network access request is not using a URL). *Id.*, 5:59-6:11. EX1003, ¶¶69-70.

The '336 patent does not purport to have invented public or private networks, "walled gardens," or Network Access Controllers. Indeed, the '336 patent incorporates by reference at least eight different prior applications (to which the '336 patent does not claim priority) that purport to teach the elements of the claimed system. *See* EX1001, 3:14-4:37. For example, U.S. Patent Appl. Pub. No. 2004/0177276 (EX1006, "MacKinnon"), filed in 2003 based on a provisional application filed in 2002 discloses an "access control device" sitting between a client device on a local network (such as a "public wireless network provided to cafe patrons") and the Internet. EX1006, [0032]; *id.*, FIG. 1. As recognized during prosecution, MacKinnon even "discloses redirecting a client's request to a pre-authorization capture destination." EX1002, 240; *see, e.g.*, EX1006, [0036], [0044]; EX1003, ¶72. Thus, the only purported invention of the '336 patent is the redirection of Internet requests from a client in the local network to a server within that local network. *Infra.*, § III.C; EX1003, ¶66.

C. File History

U.S. Patent Application No. 12/619,560, which matured into the '336 patent, was filed on 11/16/2009. Originally filed claims 1-6, 9-13, and 16-19 were rejected as obvious over two non-patent references, Crandell et al. ("A Secure and

Transparent Firewall Web Proxy") (EX1007) and Bauer ("Designing and Using DMZ Networks to Protect Internet Servers") (EX1008). As the Examiner recognized, intercepting and redirecting unauthenticated requests for access was already well known in the art. *See* EX1002, 165-168. Likewise, the Examiner noted that determining whether a "request contains an authentication token (*i.e.*, determining whether the second request contains a cookie)" and redirecting a browser based on the presence (or absence) of that cookie was well known in the art. *Id.* EX1003, ¶71.

In response, the Applicant amended the claims to specify that the client device accessing the local area network must be "within the shared network." EX1002, 218. Based on this amendment, the Examiner allowed the Challenged Claims, noting that "[t]he closest prior art, MacKinnon et al. (US 2004/0177276), also discloses redirecting a client's request to a pre-authentication capture destination; however, MacKinnon does not disclose that the pre-authentication capture destination is hosted on a first server in the shared network." *Id.*, 240; EX1003, ¶72.

D. POSITA

The relevant art for the '336 patent is the field of computer science generally, and specifically, computer networking and security. A person of ordinary skill in that art ("POSITA"), as of August 2004, would have been an individual with either (1) at least a bachelor's degree in computer science or computer engineering or an

equivalent field plus at least one year of experience working on computer networking or computer security, or (2) at least 3 years of experience working on computer networking or security, even without a formal degree. EX1003, ¶21.

IV. CLAIM CONSTRUCTION

A claim is construed "using the same claim construction standard that would be used to construe the claim in a civil action," 37 C.F.R. § 42.100(b), which is governed by *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005). Under the standard set out in *Phillips*, this petition applies the plain and ordinary meaning to each term in the '336 Patent, which is "the meaning that the term would have to a [POSITA] in question at the time of the invention." *Id.* at 1313.

A. "shared network"

In the context of the '336 patent, a "shared network" is understood to mean "a local network to which an unauthenticated user has access." This is consistent with the patent's stated purpose of facilitating network access control for, *e.g.*, a wireless device at a mall trying to access "the Web server for the mall, plus one or more other Web sites that are associated with the mall (*e.g.*, the ***local Web server*** for a tenant in the mall, such as a department store or movie theater." EX1001, 1:39-47.

B. "anonymous user"

The Board should construe "anonymous" user to encompass a user unknown to the system in the sense that the user is unauthenticated. This is consistent with the specification's dichotomy between an "anonymous user" and an "authenticated

user": "this 'external' access is only granted to the authenticated user. An anonymous user on a different Client would still be restricted to the Walled Garden." EX1001, 5:36-39. Similarly, the specification teaches that an "anonymous user has access to one of the Client network access devices" and, from there, "the anonymous user may access Web locations on any of the three servers that are in the Walled Garden." *Id.*, 4:50-65. This is also consistent with Figure 3, which illustrates that an "authenticated" user may access any desired network, while a client that is *not* authenticated (*i.e.*, is *unauthenticated*) is restricted to the walled garden unless subsequently authenticated. *See id.*, 5:45-6:16; *id.*, FIG. 3.

C. "pre-authentication capture destination"

The '336 patent specification makes clear that the "pre-authentication capture destination" is simply a pre-defined destination (such as a locally hosted Web page) within a closed network (or "walled garden"). In this context, the term "capture" is understood to refer to the "captive portal" which confines pre-authenticated users to the "walled garden" (local network). An exemplary pre-authentication capture destination could be a Web page hosted on a server within the walled garden. EX1003, ¶31.

This understanding is confirmed by the specification, which teaches "[e]mbodiments disclosed herein enable a public/private network service provider to automatically redirect anonymous clients to a pre-defined destination within a

limited set of network destinations." EX1001, 2:47-50. Likewise, the anonymous user does not need to know the URL of any location within the walled garden; rather, "they just have to attempt to access any well-known URL (such as www.yahoo.com), and *they will be redirected to the pre-defined destination.*" *Id.*, 2:53-59. This is exactly how the specification refers to the "pre-authentication capture destination": "Any attempt by an unauthorized client to access a network resource that is not in...the list of servers that make up the 'walled garden'[] will result in the client being *re-directed...to the Pre-Authentication Capture Destination*" and "[a]ny attempt to access a website...that is outside of the walled garden will cause the client to be *re-directed back to the Pre-Authentication Capture Destination.*" *Id.*, 2:7-19. The '336 patent specification further explains that the "Pre-Authentication Capture Destination" can be a Web page hosted on a local server. *E.g., id.*, 4:50-62 (the method can include sending "an HTTP redirect to the Client's browser, specifying the Pre-Authentication Capture URL 'http://wgl.com/welcome.html'. The browser then automatically performs an HTTP Get to retrieve *that Web page* from the wgl.com server.").

D. "authentication token"

The Board should construe "authentication token" as used in claims 5-7, 12-14, and 19-20 to mean a "unique sequence of characters that are valid for use within the query portion of a URL to redirect a client to an authentication screen." For

example, as illustrated in Figure 3 and reflected in claims 5-7, the patented method simply looks for the presence of a so-called "authentication token" and makes a yes/no determination if that token is present. *See* EX1001, claim 5 ("method according to claim 1, further comprising: ... determining whether the second request contains an authentication token."); *id.*, FIG. 3 (step 23, "URL contains authentication token?"); *id.*, 6:1-5 ("the Network Access Controller 2 determines if the packet contains the Authentication Token (step 23)."). "If...the packet does not contain the Authentication Token, then the Network Access Controller 2 directs the client to the Pre-Authentication URL (step 25)." *Id.*, 6:6-11. In contrast, if "the packet contains the Authentication Token, then the Network Access Controller 2 directs the client to the Authentication URL (step 24)." *Id.*, 6:12-16. In other words, the presence or absence of the token is all that matters to the invention; the contents of the token are irrelevant. EX1003, ¶32. This is consistent with the specification's description of the token, explaining that the term "authentication token," as used in the patent, simply refers to "a unique sequence of characters that are valid for use in the query portion of a URL." EX1001, 2:30-34. The specification makes clear that "the exact form of this special token need not be predefined; the special token is simply uniquely identifiable." *Id.*, 5:11-16.

Petitioner respectfully submits that no other constructions are required for the purposes of this petition.

V. Grounds of Unpatentability

The '336 patent is directed to a method and system for redirecting network access requests to either a "Pre-Authentication Capture Destination" (all independent claims) or an authentication server (claims 7, 14, 20).

Independent claim 1 recites:

A method for automatic pre-authentication redirection of network traffic, comprising:

providing a network access controller in a shared network, wherein the shared network comprises a plurality of server computers and a set of network destinations hosted on the plurality of server computers;

intercepting at the network access controller a request to access a network resource from a browser application running on a client device within the shared network associated with an anonymous user;

determining whether the network resource referenced in the request is in the set of network destinations hosted on the plurality of server computers in the shared network;

if the network resource is in the set of network destinations hosted on the plurality of server computers in the shared network, directing the browser application running on the client device within the shared network associated with the anonymous user to the network resource; and

if the network resource is not in the set of network destinations hosted on the plurality of server computers in the shared network, redirecting the browser application running on the client device within the shared network associated with the anonymous user to a pre-authentication capture destination hosted on a first server computer, wherein the first server computer is one of the plurality of server computers in the shared network and wherein from the pre-authentication capture destination the anonymous user is free to visit any of the set of network destinations hosted on the plurality of server computers in the shared network without authentication.

At their core, the claims are directed to (1) determining whether a user is already authenticated; (2) determining whether a request is for a local or external resource; (3) providing local access to any requests for local resources (regardless of authentication); and (4) redirecting unauthenticated users to a location within the local network if the requested resource is external to the local network. The claimed features are anticipated and, at minimum, obvious in view of the prior art, as explained below. EX1003, ¶¶34-41.

For example, **Subbiah** discloses a system and method for client devices in a closed network (*e.g.*, at an airport or a shopping mall) to access the Internet when so authorized and to otherwise be redirected to locations within the local network. **Subbiah** discloses all the claimed features of independent claims 1, 9, and 16, including the computing devices providing the very same steps required by the claims of the '336 patent. **Subbiah** also describes or at minimum renders obvious the additional limitations recited in the challenged dependent claims, including that the requested resource is external to the local network (claim 2); that redirecting includes sending an identifier for the site to which the user is redirected (claim 3); and redirecting back to the "Pre-Authentication Capture Destination" (claim 4).

As to claims 5-8, 12-15, and 19-22, **Subbiah** in view of **Hinton** renders these claims obvious. **Hinton** teaches the use of a token, or flag, in the URL that is used to determine how to redirect the user's browser. These teachings would have been

obvious to apply in implementing **Subbiah's** system, which already includes the teaching of redirecting a user to either the "splash" page of the local network or the authentication server based on the user's prior actions. EX1003, ¶¶110-111, 162.

As shown below, the cited prior art renders the Challenged Claims of the '336 patent unpatentable. This Petition is supported by the Declaration of John R. Black, Jr., which describes the scope and content of the prior art at the time of the alleged invention of the '336 patent. *Id.*, Section VIII.

A. Grounds 1 and 2: Claims 1--18 Are Anticipated, Or At Least Rendered Obvious By, Subbiah

As further set forth below, claims 1-4, 9-11, and 16-18 are anticipated by **Subbiah**. However, as further described below for particular limitations, to the extent it is argued that further evidence is required for those limitations, a POSITA would have found the limitations obvious over **Subbiah**. In addition, claims 5-8, 12-15, and 19-20 are rendered obvious by **Subbiah** alone in view of how a POSITA would have understood **Subbiah's** disclosures.

1. Overview of Subbiah

Subbiah teaches a system and method for a wireless access point (*i.e.*, a network access controller) to "provid[e] communications network access (*e.g.*, Web page browsing, instant messaging, e-mail, etc.) in a public area (*e.g.*, a mall, airport, sports arena, etc.)." EX1004, 4:12-15. The network can include a "local domain of the communications network, such as, for example, a local Intranet of a shopping

mall, airport, or the like" and an external domain, "outside the local domain, such as, for example, popular sites or Web pages on the Internet." *Id.*, 4:18-24. EX1003, ¶74.

Similar to the system described in the '336 patent, **Subbiah's** system includes a client device connected to a local domain and an external domain, *i.e.*, the Internet, via a wireless access point. *See* EX1004, FIGs. 1, 3. The "wireless access point 330 is configured to provide different levels of access to services, such as" "local network" access, "web and telnet, full access, etc.," and serves "to authenticate users." *Id.*, 14:17-24. **Subbiah's** "wireless access point" serves as the "network access controller" as it intercepts and redirects network requests from a client. *E.g.*, *id.*, 15:9-12, 16:2-8. EX1003, ¶75.

And like the '336 patent, **Subbiah's** wireless access point controls network access using the same four basic determinations:

(1) Is the user authenticated? (Step 703)

(2) Is the destination local (*i.e.*, in the walled garden)? (Step 704)

(3) Is the destination a URL? (*i.e.*, is the client "using a Web browser"

(EX1004, 17:18-22) (Step 706)

(4) Does the URL have a token? (*i.e.*, is it a "first time request") (Step 707)

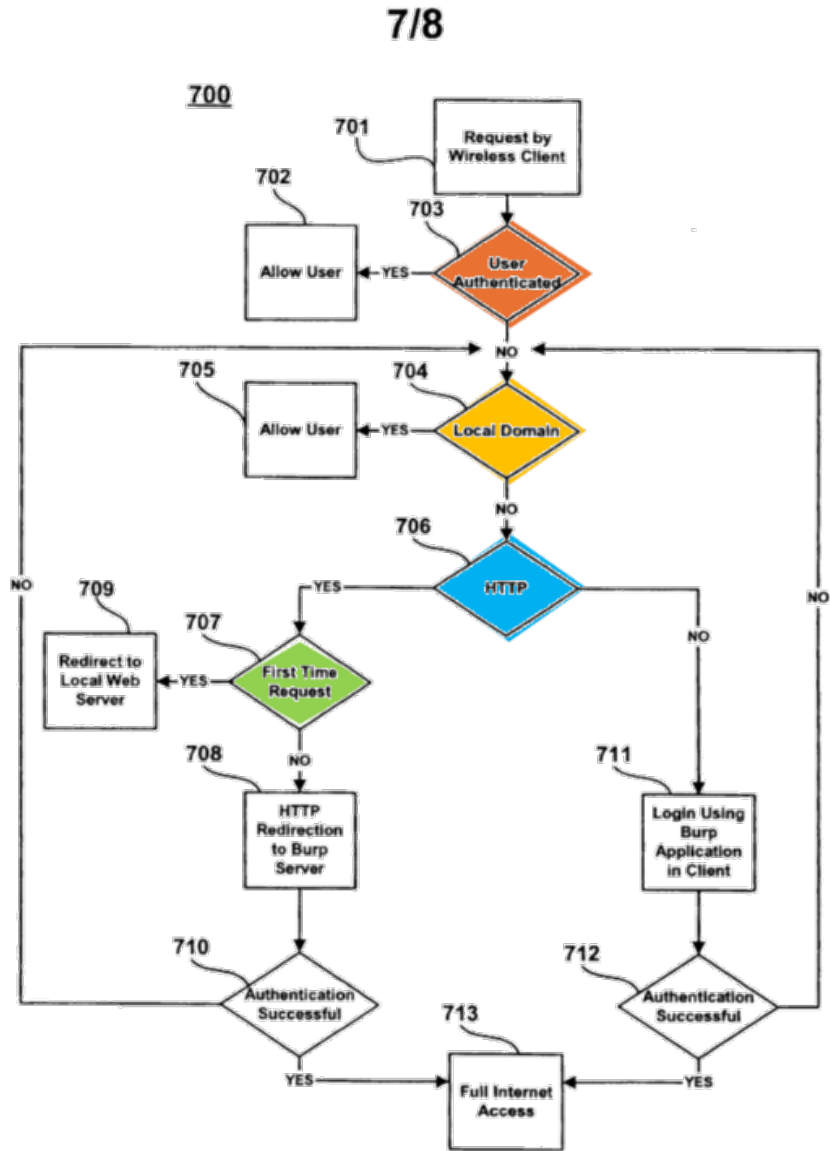


FIG. 7

Like the purported invention of the '336 patent, an authenticated client is permitted access to whatever resource is requested. EX1004, 17:10-14; *id.*, FIG. 7

(steps 702, 703). Likewise, regardless of authentication, a client is permitted access to any resource within the walled garden. *Id.*, 17:16-18; *id.*, FIG. 7 (steps 704, 705). Unauthenticated users, however, will be redirected either to the "Local Web Server," and in particular to a "main, or default, Web page 400," (*i.e.*, the "Pre-Authentication Capture Destination") if the user requested an Internet HTML page (*e.g.*, using an HTTP URL), or to the authentication server (because some flag indicates it is not the user's first visit or the user is not requesting a URL). *Id.*, 15:7-13, 16:2-14, 17:18-18:4; *id.*, FIG. 7 (steps 706-709, 711). Finally, "in the event of an unsuccessful authentication process," the user is "provide[d] access to the information and services of the first area" (*i.e.*, the local domain). *Id.*, 13:14-17; *id.*, FIG. 2. EX1003, ¶¶76-77.

With respect to step 707, checking whether it is a "first time request," a POSITA would have understood, or at minimum found it obvious, that **Subbiah's** wireless access point could track whether the client's request was a first-time request, or a repeat request, for Internet access using tokens (*e.g.*, flags or cookies) in the request. *Supra* §**Error! Reference source not found.** Cookies are well-known tools in HTTP for transmitting and tracking state information, and the use of cookies is a design choice well within the knowledge of a POSITA during that timeframe. EX1003, ¶¶60, 78. Likewise, with respect to step 710, a POSITA would have understood, or at minimum found it obvious, that an unsuccessful authentication

attempt would redirect the user back to the "main, or default, Web page 400" as an unauthenticated user is always permitted free access to the local domain. *See, e.g.*, EX1004, 13:14-17 ("in the event of an unsuccessful authentication process as determined in step 204, process 200 proceeds to step 206 and provides access to the information and services of the first area"). EX1003, ¶77-79.

2. Independent Claim 1

(a) [1.pre] "A method for automatic pre-authentication redirection of network traffic, comprising:"

To the extent the preamble is limiting, **Subbiah** discloses this limitation. **Subbiah** discloses a "communications network access and control system" with a "wireless access point...configured to provide different levels of access to services[,]" including "redirect[ing] the browser of [the] client [] to the local web server." EX1004, 13:26-14:4, 14:15-24, 15:9-12. **Subbiah** further discloses that this redirection takes place before a client is authenticated by the system. *See id.*, 17:16-26; *id.*, FIG. 7; EX1003, ¶98.

Specifically, **Subbiah** discloses "[a] *method for providing communications network access* in a public area" within a network comprised of "a first area" and a "second area" of the communications network. EX1004, Abstract. This "communications network access and control system" is further illustrated in Figure 3 of **Subbiah**:

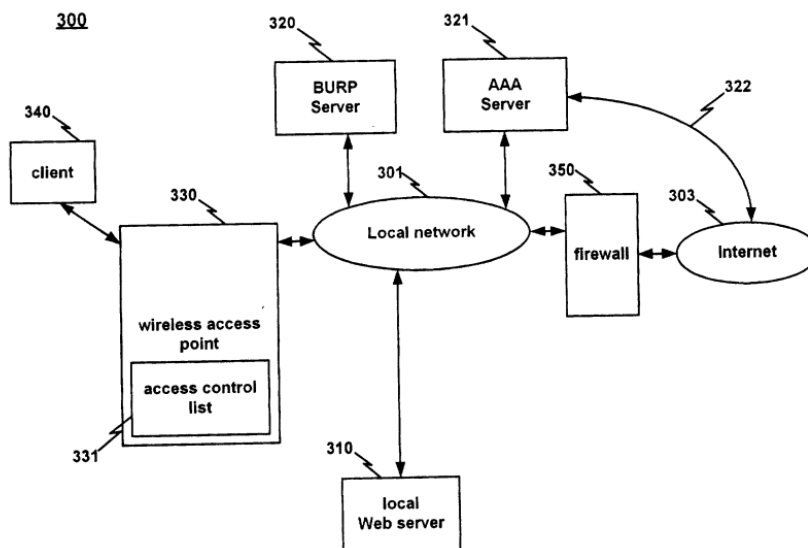
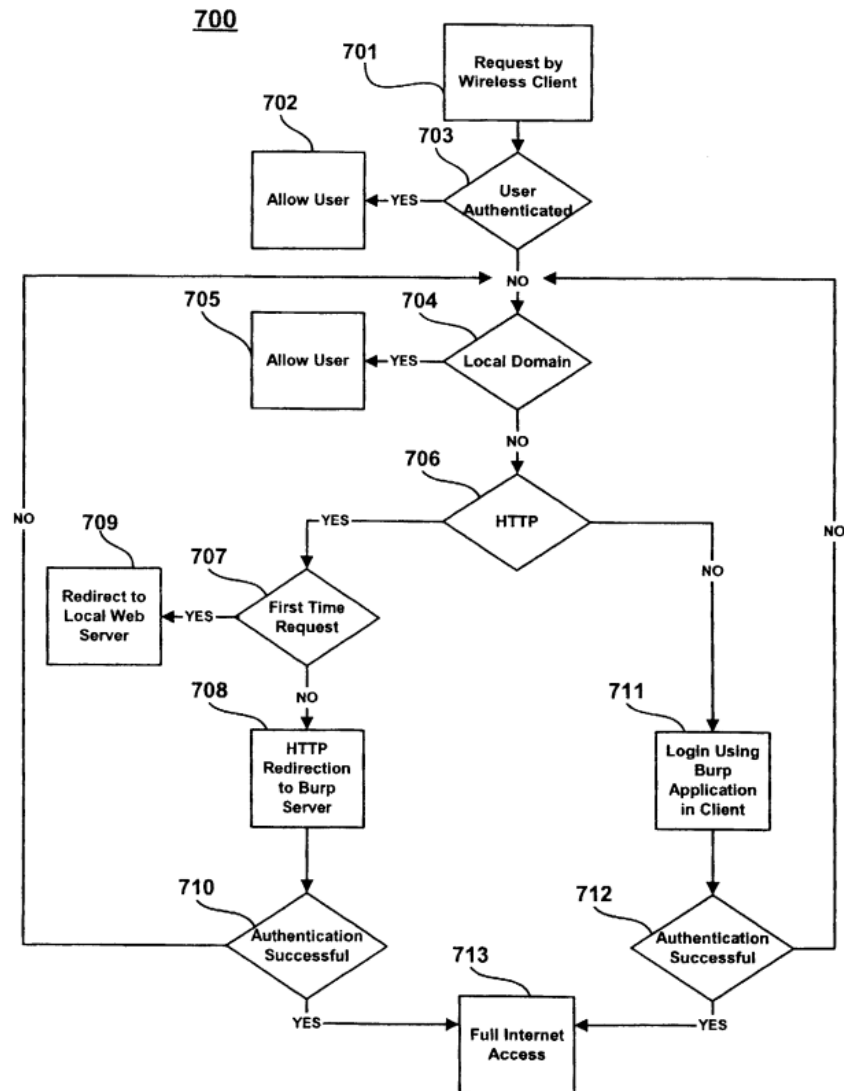


FIG. 3

Id., FIG. 3. "As depicted in Figure 3, system 300 includes a client 340 coupled to **a local network 301** via a wireless access point 330. A BURP server 320, a AAA server 321, and a local Web server 310 are coupled to the local network 301. The local network 301 is coupled to **the Internet 303** via a firewall 350." *Id.*, 13:26-14:4; EX1003, ¶99.

As explained further below, **Subbiah** Figure 7 shows a flow chart "depict[ing] the operating steps as performed by the components of system 300 of Figure 3" in which, when an unauthenticated user attempts to access the Internet, the wireless access point 330 may automatically "redirect[]" the browser of client 340 to the local web server 310" or "the request is redirected to the BURP server 320." EX1004, 15:9-12, 17:6-8, 17:22-26. The BURP server (which stands for "basic user registration protocols") is used for "[t]he authentication process...and

can be used to provide different levels of Internet access in accordance with different classes of customers." *Id.*, 5:4-16. And as further confirmed by Figure 7, the automatic redirection (*e.g.*, at steps 709 and 708) takes place prior to authentication (at step 710):



Id., FIG. 7; see also, *e.g.*, *id.*, 12:7-13:17; *id.*, FIG. 2; EX1003, ¶¶99-100.

(b) [1.a]: "providing a network access controller in a shared network, wherein the shared network comprises

a plurality of server computers and a set of network destinations hosted on the plurality of server computers;"

Subbiah discloses providing a network access controller (*e.g.*, "wireless access point") **in a shared network** (*e.g.*, "local network" or "local domain"), **wherein the shared network comprises a plurality of server computers** ("local web server," "BURP Server, "AAA Server") **and a set of network destinations hosted on the plurality of server computers** (*e.g.*, "free local services offered...by the local Web server," "Web pages"). EX1003, ¶101.

Subbiah discloses a "wireless access point" connecting a "client" to a "local network" within its "communications network access and control system." EX1004, 14:2-11 ("As depicted in Figure 3, system 300 includes a client 340 coupled to a local network 301 via a wireless access point 330. A BURP server 320, a AAA server 321, and a local Web server 310 are coupled to the local network 301. The local network 301 is coupled to the Internet 303 via a firewall 350.... Access to the local network 301 is provided wirelessly, via a wireless access point 330. Local content is served to the client 340 via the local Web server 310."); EX1003, ¶102.

The "local network" (or "local domain") may be "a local Intranet of a shopping mall, airport, or the like," and itself comprises a plurality of servers (including "local web server" and authentication servers) hosting network destinations, such as "web pages provided by the local server" and "informational Web pages, event

information and the like." EX1004, 4:12-20 ("In one embodiment, the present invention is implemented as a wireless access method for providing communications network access (*e.g.*, Web page browsing, instant messaging, e-mail, etc.) in a public area (*e.g.*, a mall, airport, sports arena, etc.)[] . . . for access to a first area or a second area of the communications network. The first area can be a local domain of the communications network, such as, for example, a local Intranet of a shopping mall, airport, or the like."; *id.*, 5:8-10 ("[U]sers surfing the local, or internal, domain can do so freely (*e.g.*, browsing advertisements, informational Web pages, event information, and the like)..."); *id.*, 10:27-11:11 ("In response to receiving a request for access to the local domain 101, access is provided to the services of the local domain 101 of the communications network. Such services include, for example, Web pages provided by the local server 110."); *see also id.*, 15:7-12; EX1003, ¶102.

(c) **Claim [1.b]: "intercepting at the network access controller a request to access a network resource from a browser application running on a client device within the shared network associated with an anonymous user;"**

Subbiah discloses intercepting at the network access controller ("wireless access point") a request to access a network resource (*e.g.*, "requests for network access", "request from the client") from a browser application running on a client device (*e.g.*, "PDA, laptop, cellphone", "client") within the shared network (*e.g.*,

network at "an airport terminal" or "shopping mall") **associated with an anonymous user** (e.g. "client", "mobile user", "Internet user[]"). EX1003, ¶103.

Subbiah discloses the "wireless access point" is positioned between client devices and network resources—both local domain resources and external resources, such as the Internet. E.g., EX1004, 12:14-17 ("[I]n one embodiment, requests for network access are received wirelessly from clients via a wireless access point (e.g., wireless access point 130) coupled to the network."); *id.*, 17:10-11 ("Process 700 begins in step 701 when a request from the client 340 is received by the access point 330.").

These "client devices" include a "PDA, laptop, cellphone, or the like" and access "web pages" using a "browser." EX1004, 4:15-18 ("The method includes the step of receiving a request to access a communications network from a client, such as a PDA, laptop, cellphone, or the like. A determination is then made as to whether the request is for access to a first area or a second area of the communications network."); *id.*, 2:22-3:3 ("[I]t would be advantageous to provide Internet access to mobile, wireless client equipped passengers (e.g., via wireless PDAs, laptop computers, cellphones, etc.) as they move from place to place within an airport terminal. The Internet access would allow them to, for example, check airline flight times, ground transportation schedules, obtain a list of restaurants, check hotel reservations, or the like. Similarly, wireless Internet access in a shopping mall or in

a downtown business district would allow properly equipped users to obtain information with regard to commercial services, sales, ATM locations, and the like."); *id.*, 15:7-12 ("[W]hen the client 340 tries to access non-local domains such as the Internet 303, the access point 330 will react in the following manner. If the client 340 is using a browser...the wireless access point 330 redirects the browser of client 340 to the local web server 310."); EX1003, ¶104; *see also, e.g.*, EX1004, 14:18-15:2, 19:23-20:12; *id.*, FIGs. 1-3, 7.

(d) Claim [1.c]: "determining whether the network resource referenced in the request is in the set of network destinations hosted on the plurality of server computers in the shared network;"

Subbiah discloses determining whether the network resource referenced in the request is in the set of network destinations (*e.g.*, "Web pages") hosted on the plurality of server computers in the shared network (*e.g.*, "local domain service", "local network"). EX1003, ¶105.

Subbiah discloses that, after receiving a "request [to] access" content, the wireless access point determines "whether the request from the client device is for a local domain service"—*i.e.*, a destination hosted on the plurality of server computers in the shared network—or for an Internet service. *E.g.*, EX1004, 17:16-18 ("In step 704, the wireless access point 330 determines whether the request from the client 340 is for a local domain service. In step 705, if the request is for local domain 301 service, full access to the local service is provided."); *id.*, 10:21-24 ("Upon receiving

request for access from client 140, a determination is made as to whether the request is for access to a first area or a second area of the communications network. In this embodiment, the first area is the local domain 101, which is, for example, a local Internet of a shopping mall, airport, or the like."); *id.*, 12:20-25 ("In step 202, a determination is made as to whether the request is for access to a first area (e.g., local domain 101) or a second area (e.g., external domain 103) of the network. As described above, the local domain of the network can include local servers (e.g., local server 110) configured to provide Web pages and information or services tailored for the characteristics of the local area (e.g., airport, shopping mall, etc.)."); *see also id.*, 20:1-5; EX1003, ¶106.

- (e) **Claim [1.d]: "if the network resource is in the set of network destinations hosted on the plurality of server computers in the shared network, directing the browser application running on the client device within the shared network associated with the anonymous user to the network resource; and"**

Subbiah discloses if the network resource is in the set of network destinations hosted on the plurality of server computers in the shared network (e.g., "Web pages provided by the local server"), **directing the browser application running on the client device within the shared network associated with the anonymous user to the network resource.** EX1003, ¶107.

For example, **Subbiah** discloses that all users, including unauthenticated users, may access the local domain freely, which includes "web pages provided by

the local server" accessed using a browser. *E.g.*, EX1004, 10:27-11:3 ("In response to receiving a request for access to the local domain 101, access is provided to the services of the local domain 101 of the communications network. Such services include, for example, Web pages provided by the local server 110.");*id.*, 11:18-20 ("[U]sers surfing the local domain 101 can do so freely (*e.g.*, browsing mall advertisements, mall informational Web pages, mall shopping event information, and the like)."); EX1003, ¶108.

As further confirmed by **Subbiah**, such access to the local network is provided even prior to the authentication in step 710—*e.g.*, access is provided to the Local Domain (and "Local Web Server") at steps 704-705 of Figure 7 even after confirming, at step 703, that the user is not authenticated:

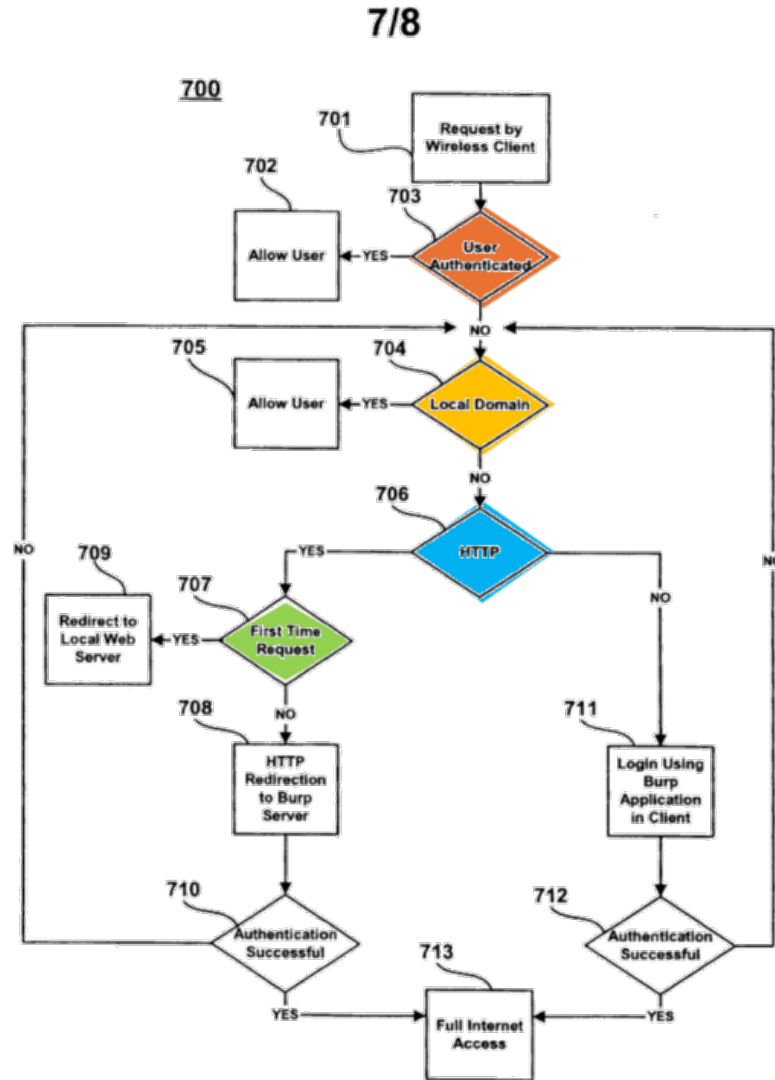


FIG. 7

EX1004, FIG. 7; *see also id.*, 17:17-18 ("In step 705, if the request is for local domain 301 service, full access to the local service is provided."); *id.*, 13:12-14 ("In step 206, when the request for access to the first area is received as determined in step 202, access is freely provided to the information and services of the first area of the communications network."); *id.*, FIG. 2; *see also, e.g., id.*, Abstract, 4:22-5:2, 17:18-21; EX1003, ¶108.

- (f) **Claim [1.e]: "if the network resource is not in the set of network destinations hosted on the plurality of server computers in the shared network, redirecting the browser application running on the client device within the shared network associated with the anonymous user to a pre-authentication capture destination hosted on a first server computer, wherein the first server computer is one of the plurality of server computers in the shared network and wherein from the pre-authentication capture destination the anonymous user is free to visit any of the set of network destinations hosted on the plurality of server computers in the shared network without authentication."**

Subbiah discloses if the network resource is not in the set of network destinations hosted on the plurality of server computers in the shared network (e.g., request for "an Internet [] service", "external domain", "Internet"), **redirecting the browser application running on the client device within the shared network associated with the anonymous user (e.g., "browser" on "client") to a pre-authentication capture destination hosted on a first server computer (e.g., "main, or default, Web page" residing on "local web server", "main Web page 400", "login Web page" residing on "BURP server"), wherein the first server computer is one of the plurality of server computers in the shared network (e.g., "local network", "local web server") and wherein from the pre-authentication capture destination the anonymous (e.g., unauthenticated) user is free to visit any of the set of network destinations hosted on the plurality of server computers in the**

shared network (e.g., "Web pages provided by the local server") **without authentication**. EX1003, ¶109.

For example, **Subbiah** discloses its access point redirecting network traffic for unauthenticated users trying to access the Internet to a "main Web page" on the local web server or a "login Web page" hosted on the "BURP server" within the "local network." See, e.g., EX1004, 16:1-6. Specifically, "when the request is for an Internet 303 service, ...[and] a Web browser is being used, process 700 proceeds to step 707.... In step 707, if the request is a first-time request, process 700 proceeds to step 709 where the request is redirected to the local web server 310. Otherwise, process 700 proceeds to step 708, where the request is redirected to the BURP server 320." *Id.*, 17:18-26; see also *id.*, 15:7-13 ("[W]hen the client 340 tries to access non-local domains such as the Internet 303,..., the wireless access point 330 redirects the browser of client 340 to the local web server 310. The web server 310 then pushes the main, or default, Web page to the client's browser, an example of which is shown in Figure 4 below"); *id.*, 12:20-26; EX1003, ¶111.

The "main Web page" is described as the "front page" or "splash page" of the local network and, from there, unauthenticated users may "freely" surf the local domain, including visiting "informational Web pages" hosted on the local domain. E.g., EX1004, 16:1-6 ("Figure 4 shows a diagram depicting a main, or default, Web page 400 in accordance with one embodiment of the present invention. The main

Web page 400 is the Web page to which the browser of client 340 is redirected. The Web page 400 typically functions as the 'front page' or 'splash page' of the local network 301."); *id.*, 5:8-10 ("[U]sers surfing the local, or internal, domain can do so freely (e.g., browsing advertisements, informational Web pages, event information, and the like)..."); *id.*, 13:12-17 ("In step 206, when the request for access to the first area is received as determined in step 202, access is freely provided to the information and services of the first area of the communications network. Alternatively, in the event of an unsuccessful authentication process as determined in step 204, process 200 proceeds to step 206 and provides access to the information and services of the first area."); EX1003, ¶110.

In addition, **Subbiah** discloses redirecting users to a "login Web page" hosted on the BURP server within the local network, from which users can also access the "home page" of the local network. *E.g.*, EX1004, 16:10-14 ("[I]f the client 340 is using a browser and is attempting to access the Internet 303 for the second time, the access point 330 redirects the browser of client 340 to the BURP server 320. The BURP server 320 will then try to authenticate the client 340 through a login Web page, an example of which is shown in Figure 5 below.").

Figures 4 and 5 depict the "main Web page" and the "login Web page" on the "local Web server" and "BURP server," respectively:

400

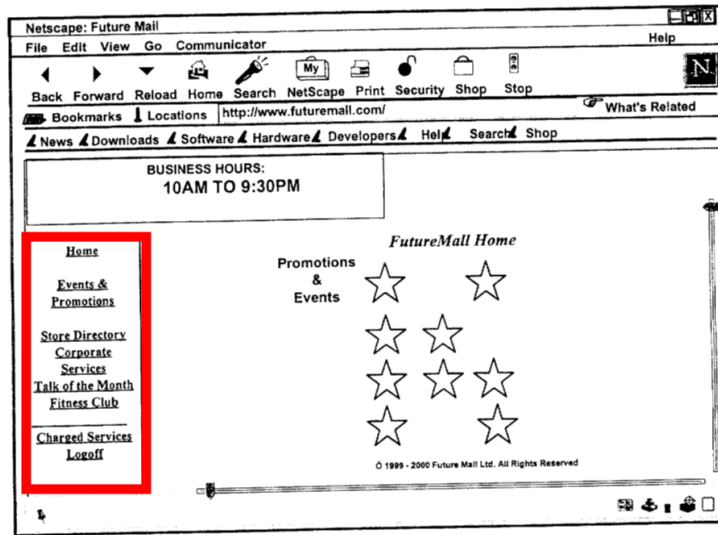


FIG. 4

E.g., EX1004, FIG. 4 (annotated).

500

A screenshot of a Netscape browser window displaying a 'Login Form'. The form is titled 'Login Form' and includes the text 'For access of privileged services, Please fill out this form and submit it. Thank you'. It contains several input fields: 'LOGIN:', 'PASSWORD:', 'CREDIT CARD:', 'ISP NAME:', and 'LOGIN CODE:'. Below the 'PASSWORD:' field are 'Sign In' and 'Reset' buttons. At the bottom, there is a link that reads 'If you came here by accident click here to go to our home page: HOME', where the text 'click here to go to our home page: HOME' is highlighted with a red rectangular box.

FIG. 5

E.g., EX1004, FIG. 5 (annotated). As illustrated in exemplary Figure 5, the login Web page includes links to access the "home page," and the exemplary home page

of Figure 4 includes links to visit other pages hosted on the local domain (e.g., "Events & Promotions"; "Store Directory"; etc.). See EX1003, ¶110.

3. Claim 2: " The method according to claim 1, wherein the network resource is at a network location external to the shared network."

See [1]. Subbiah discloses wherein the network resource (e.g., "site[]", "Web page[]") is at a network location external to the shared network (e.g., "external domain", "Internet"). EX1003, ¶112.

As set forth above in claim 1, Subbiah discloses that "system 100 includes a local domain of a communications network 101 coupled to a gateway 102 to an external communications network, shown as external domain 103." EX1004, 10:4-6. This "part of the communications network outside the local domain 101, in this case external domain 103, compris[es], for example, popular sites or Web pages on the Internet." *Id.*, 10:25-27. Further, Subbiah expressly discloses "receiving a request for access to the external domain 103 (e.g., Web pages and/or sites on the Internet)." *Id.*, 11:3-5; see also *id.*, 12:20-26. Finally, Subbiah expressly discloses redirecting to the local server "when the client 340 tries to access non-local domains such as the Internet 303, the access point 330 will react in the following manner. If the client 340 is using a browser and is downloading a default homepage (e.g., assuming that the Web page resides somewhere in the Internet 303), the wireless

access point 330 redirects the browser of client 340...) *Id.*, 15:7-13; *see id.*, 17:18-20; EX1003, ¶113.

4. **Claim [3]: " The method according to claim 1, wherein the redirecting further comprises sending from the network access controller to the client device a response containing an identifier identifying the pre-authentication capture destination."**

See [1]. Subbiah discloses wherein the redirecting further comprises sending from the network access controller to the client device a response containing an identifier identifying the pre-authentication capture destination (e.g., "http://www.futuremall.com/"). EX1003, ¶114.

Subbiah discloses redirecting HTTP requests from a browser to a "splash page" or "home page" of the local network, for example, as pictured in Figure 4. E.g., EX1004, 15:7-13 ("[W]hen the client 340 tries to access non-local domains such as the Internet 303", the access point 330 will react in the following manner. If the client 340 is using a browser and is downloading a default homepage (e.g., assuming that the Web page resides somewhere in the Internet 303), the wireless access point 330 redirects the browser of client 340 to the local web server 310. The web server 310 then pushes the main, or default, Web page to the client's browser, an example of which is shown in Figure 4 below."); *id.*, 16:1-6 ("Figure 4 shows a diagram depicting a main, or default, Web page 400 in accordance with one embodiment of the present invention. The main Web page 400 is the Web page to

which the browser of client 340 is redirected. The Web page 400 typically functions as the 'front page' or 'splash page' of the local network 301."). Figure 4 provides an exemplary page with the address "http://www.futuremall.com/":

400

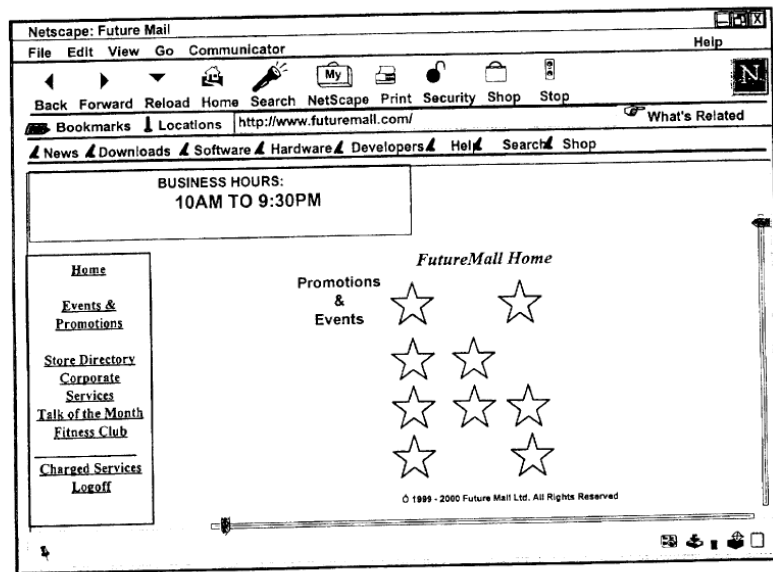


FIG. 4

EX1004, FIG. 4. A POSITA would have understood that such redirection necessarily requires sending the URL of the target Web page (e.g., "http://www.futuremall.com/") for the browser to access and load the Web page. At minimum, a POSITA would have found it obvious to do so for the same reason. See EX1003, ¶115.

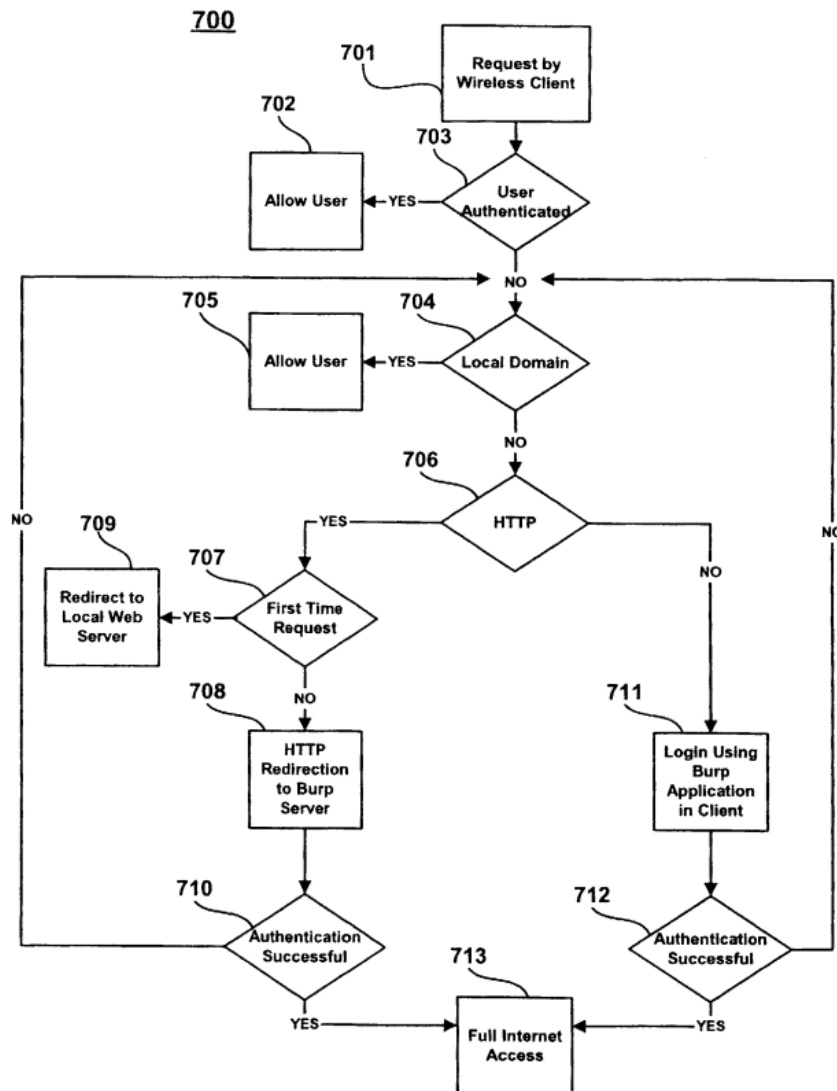
5. **Claim [4]: "The method according to claim 1, further comprising: redirecting the browser application running on the client device back to the preauthentication capture destination when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality of server computers in the shared network."**

See [1]. Subbiah discloses redirecting the browser application running on the client device back to the preauthentication capture destination (e.g., "login Web page" on "BURP server") when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality of server computers in the shared network. EX1003, ¶116.

Subbiah discloses that unauthenticated users are provided free access to the information and services of the first area, *i.e.*, the web sites hosted on the local domain servers. *E.g.*, EX1004, 13:14-17 ("Alternatively, in the event of an unsuccessful authentication process as determined in step 204, process 200 proceeds to step 206 and provides access to the information and services of the first area."); *id.*, 5:8-10 ("[U]sers surfing the local, or internal, domain can do so freely (e.g., browsing advertisements, informational Web pages, event information, and the like)...").

As demonstrated in the flow charts of Fig. 7, to the extent a user attempts to access external resources (such as the Internet) after the first such attempt, the process returns to step 704 and cycles through step 708 in which the user is redirected

back to the login Web page of Fig. 5, hosted on the BURP server, and is provided access to the pages on the local domain, including the "splash page" of the local network:



EX1004, FIG. 7; see also *id.*, 16:10-14 ("If the client 340 is using a browser and is attempting to access the Internet 303 for the second time, the access point 330 redirects the browser of client 340 to the BURP server 320. The BURP server 320

will then try to authenticate the client 340 *through a login Web page*, an example of which is shown in Figure 5 below."); EX1003, ¶117.

6. Claim 5

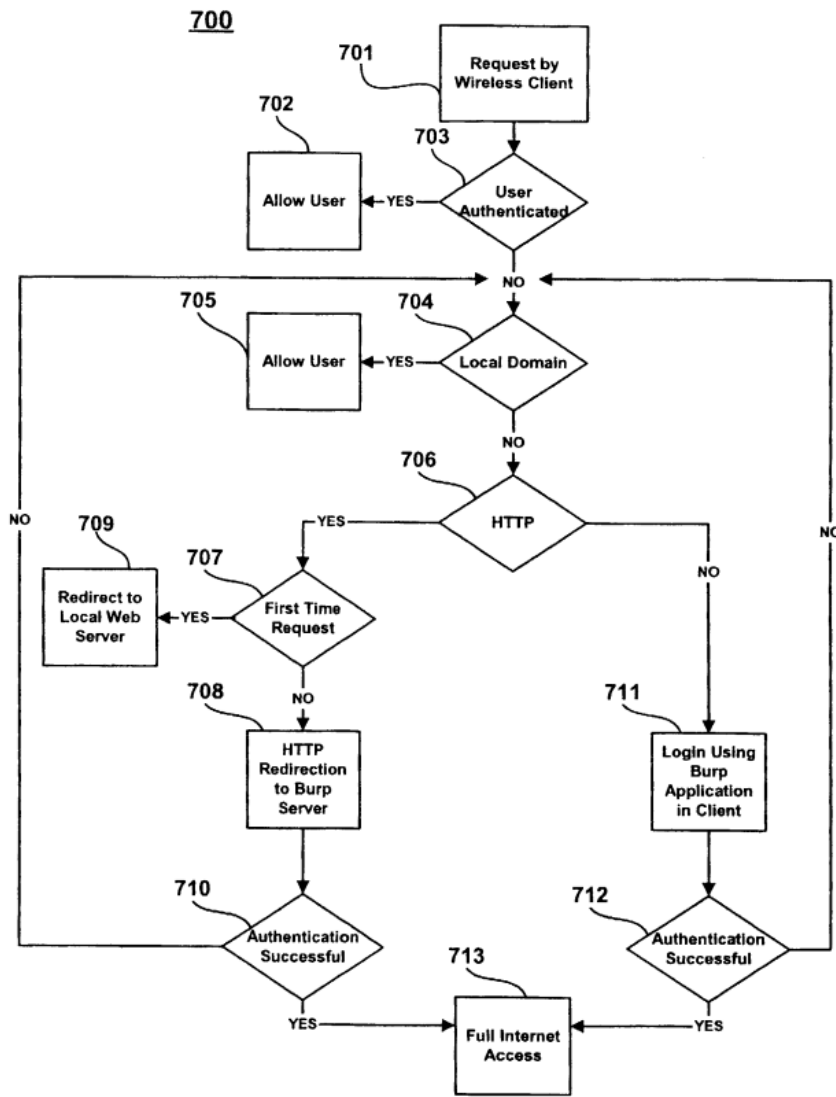
- (a) **Claim [5pre]: "The method according to claim 1, further comprising:"**

See [1]. EX1003, ¶118.

- (b) **Claim [5a]: "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"**

***See* [1.b]. Subbiah discloses intercepting at the network access controller ("wireless access point") a second request from the browser application running on the client device associated with the anonymous (*e.g.*, "unauthenticated") user to access a second network resource (*e.g.*, "Web page") that is not in the set of network destinations (*e.g.*, "external domain", "Internet"). EX1003, ¶119.**

Subbiah further discloses that its wireless access point can detect and intercept multiple attempts (including an "attempt[] ... for the second time") by the same user to access Internet Web pages hosted external to the local domain. *E.g.*, EX1004, 16:10-14 ("[I]f the client 340 is using a browser and is attempting to access the Internet 303 for the second time..."); EX1003, ¶120.



E.g., EX1004, Fig. 7.

(c) **Claim [5b]: "determining whether the second request contains an authentication token."**

Subbiah discloses, and/or renders obvious, determining whether the second request contains an authentication token (*e.g.*, flag or cookie tracking "first time request[s]"). EX1003, ¶121.

Subbiah discloses the wireless access point intercepting a request to access a non-local resource, such as an Internet Web page and "redirect[ing] the browser" to a login Web page on the BURP server. *E.g.*, EX1004, 16:10-14 ("[I]f the client 340 is using a browser and is attempting to access the Internet 303 for the second time, the access point 330 redirects the browser..."). This redirection takes place after determinations that the user is trying to access an Internet Web page (*i.e.*, using a browser and "HTTP" protocol) and that it is not the first such attempt:

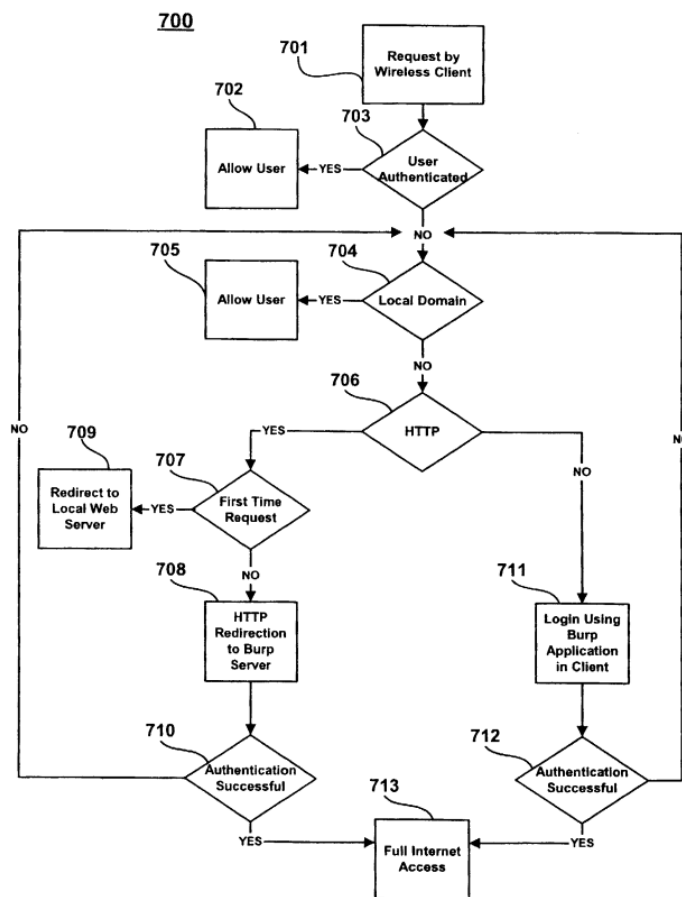


Fig. 7 (steps 706, 707, 708). A POSITA would have understood that a common way of determining whether this is an Internet browser's first or second attempt at

accessing the Internet would include the use of cookies inserted into the HTTP requests and responses. The wireless access point could insert a cookie into its HTTP response after the first attempt and each subsequent attempt by the browser would therefore include that cookie until the user is authenticated and permitted to access the Internet. At minimum, it would have been obvious to use cookies to do so in order to ensure that browsers are directed to the correct location on the local domain. A cookie is a unique sequence of characters that may be used in the query portion of a URL and can be used to redirect a client to an authentication screen accordingly. EX1003, ¶122. The use of a cookie to transmit and track state information (such as a "first time request" or "second attempt", authentication status, etc.) was a well-known mechanism in early versions of HTTP available as of the priority date of the '336 patent and the use of cookies would have been an obvious design choice yielding predictable results. EX1003, ¶122.

7. **Claim [6]: "The method according to claim 5, wherein the second request does not contain the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network."**

***See* [5]. Subbiah discloses wherein the second request does not contain the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user**

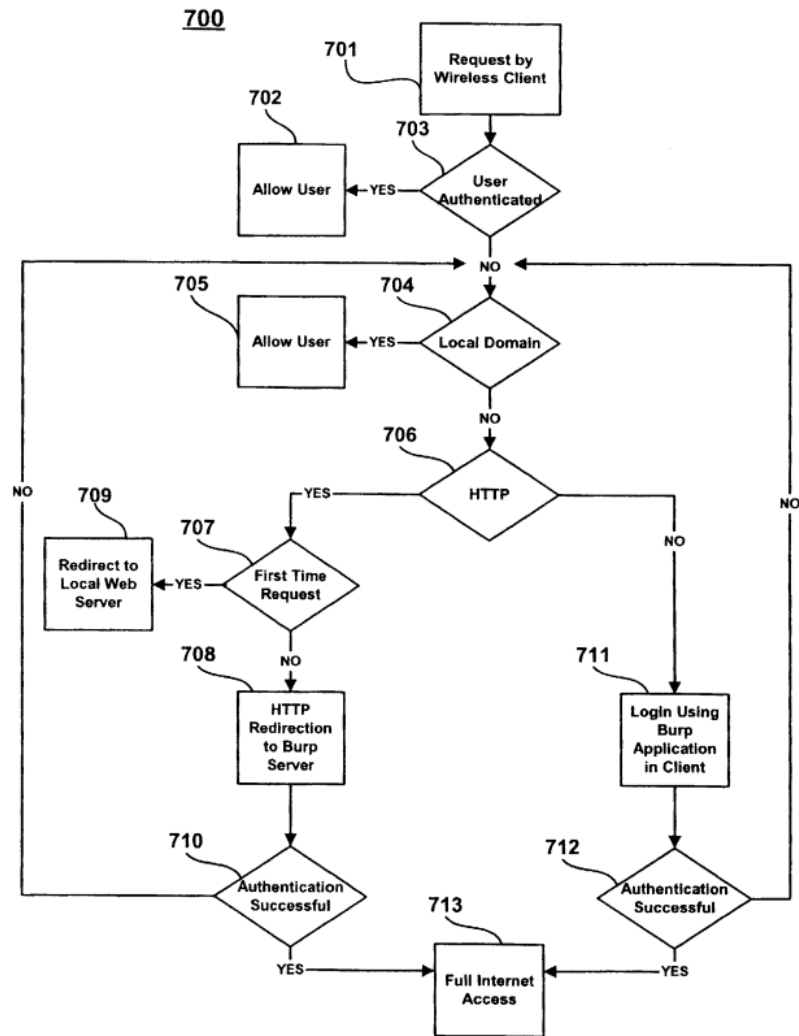
back to the pre-authentication capture destination hosted on the first server computer in the shared network. EX1003, ¶123.

Subbiah discloses that, for first time requests—*i.e.*, requests without the authentication token (*see* [5b])—the unauthenticated user's browser is redirected to the "front page" on a first server—*i.e.*, "local web server 310." *E.g.*, EX1004, 15:7-13 ("[W]hen the client 340 tries to access non-local domains such as the Internet 303, the access point 330 will react in the following manner. If the client 340 is using a browser...the wireless access point 330 redirects the browser of client 340 to the local web server 310."); *id.*, 16:1-6 ("Figure 4 shows a diagram depicting a main, or default, Web page 400 in accordance with one embodiment of the present invention. The main Web page 400 is the Web page to which the browser of client 340 is redirected. The Web page 400 typically functions as the 'front page' or 'splash page' of the local network 301."). A POSITA would have further understood that, for subsequent requests where the authentication token is nonetheless missing, *e.g.*, the user cleared its cache of cookies, started a new session, etc., the server would react as though it were a first time request (because it determines the token is missing) and would therefore redirect the user back to the "front page" on the local network. *See* EX1003, ¶124.

8. **Claim [7]: "The method according to claim 5, wherein the second request contains the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."**

See [5]. Subbiah discloses wherein the second request contains the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user to an authentication page (e.g., "login Web page") hosted on a second server computer in the shared network (e.g., "BURP server"). EX1003, ¶125.

Subbiah discloses that, for subsequent requests—*i.e.*, requests having the authentication token (*see [5b]*)—the unauthenticated user's browser is redirected to a "login web page" on a second server, the "BURP server," where the user can then be authenticated. *E.g.*, EX1004, 16:10-14 ("If the client 340 is using a browser and is attempting to access the Internet 303 for the second time, the access point 330 redirects the browser of client 340 to the BURP server 320. The BURP server 320 will then try to authenticate the client 340 through a login Web page, an example of which is shown in Figure 5 below."); EX1003, ¶126.



EX1004, FIG. 7.

9. Claim [8]: "The method according to claim 7, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network."

See [7]. Subbiah discloses wherein the anonymous user is authenticated by the second server computer (e.g., "BURP server") for network access external to the shared network. EX1003, ¶127.

Subbiah discloses that the BURP server authenticates the user to permit access to the external network, such as the Internet. *E.g.*, EX1004, 16:10-14 ("If the client 340 is using a browser and is attempting to access the Internet 303 for the second time, the access point 330 redirects the browser of client 340 to the BURP server 320. The BURP server 320 will then try to authenticate the client...."); *id.*, 17:22-26 ("[T]he request is redirected to the BURP server 320. In step 710, if the authentication is successful, full Internet access is provided in step 713."); *id.*, 14:11-13 ("Authentication is performed in accordance with...BURP protocols using BURP server 320..."). FIG. 3 illustrates the system with multiple local servers including BURP server 320:

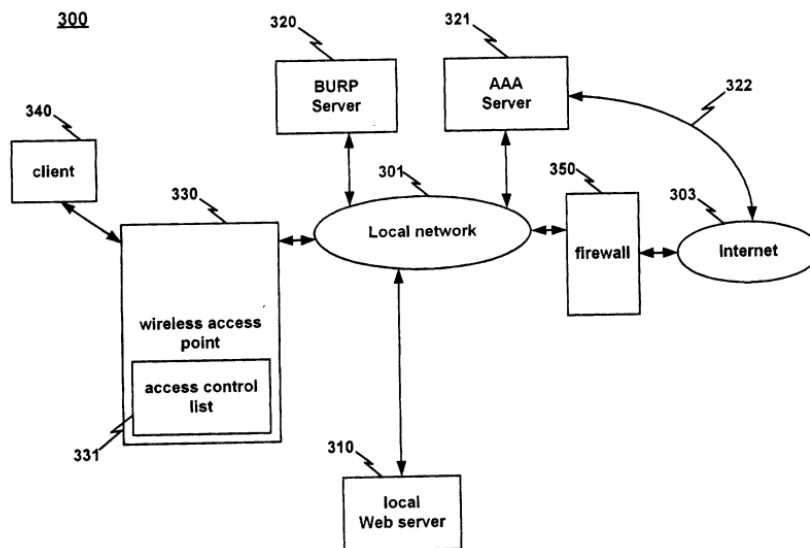


FIG. 3

E.g., EX1004, FIG. 3; *see also id.*, FIG. 7; EX1003, ¶128.

10. Claim 9

- (a) **[9.pre]: "A computer program product comprising a non-transitory computer readable storage medium storing computer instructions translatable by a processor to perform:"**

See [1.pre]. In addition, Subbiah discloses a computer program product comprising a non-transitory computer readable storage medium storing computer instructions translatable by a processor. EX1003, ¶129.

Subbiah discloses the method is performed by a "computer system platform," which "implement[s] certain software based functionality of the present invention." *E.g.*, EX1004, 18:6-17 ("Computer System Platform: With reference now to Figure 8, a computer system 812...shows the components of a computer system...for implementing certain software based functionality of the present invention. As described above [in Subbiah], certain processes and steps of the present invention are realized, in one embodiment, as a series of instructions (*e.g.*, software program) that reside within computer readable memory units of a computer system (*e.g.*, system 812) and are executed by the processor(s) of system 812. When executed, the instructions cause the computer system 812 to implement the functionality of the present invention as described above."). The disclosed "computer system" includes "an embedded computer system as implemented within a wireless access point, firewall, or gateway" comprising "one or more central processors 801...for processing information and instructions, a computer readable volatile memory unit

802 (e.g., random access memory, static RAM, dynamic, [*sic*] RAM, etc.)...for storing information and instructions for the central processor(s) 801, a computer readable non-volatile memory unit (e.g., read only memory, programmable ROM, flash memory, EPROM, EEPROM, etc.)...for storing static information and instructions for the processor(s) 801...[and] a mass storage computer readable data storage device 804 such as a magnetic or optical disk and disk drive...for storing information and instructions." *Id.*, 18:19-19:14.

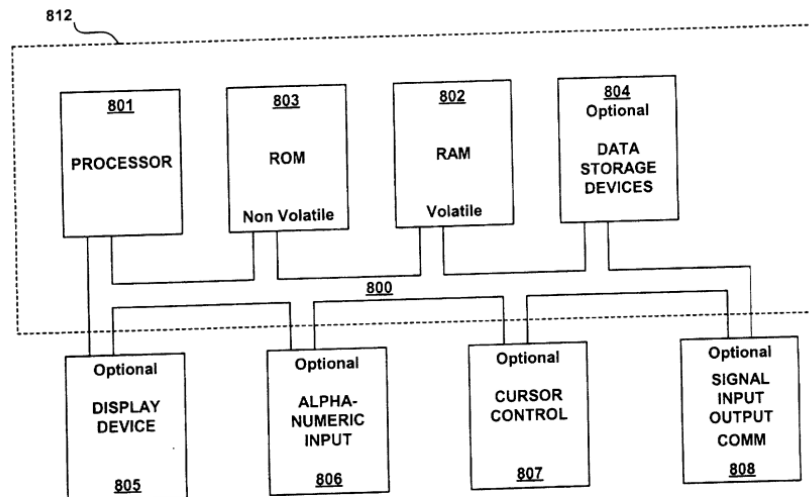


FIG. 8

E.g., EX1004, FIG. 8; see EX1003, ¶130.

- (b) **Claim [9a]: "intercepting at a network access controller a request to access a network resource from a browser application running on a client device within the shared network associated with an anonymous user;"**

See [1.a]. EX1003, ¶131.

- (c) **Claim [9b]: "determining whether the network resource referenced in the request is in a set of network"**

**destinations hosted on a plurality of server computers
in a shared network;"**

See [1.b]. EX1003, ¶132.

- (d) **Claim [9c]: "if the network resource is in the set of
network destinations hosted on the plurality of server
computers in the shared network, directing the browser
application running on the client device within the
shared network associated with the anonymous user to
the network resource; and"**

See [1.c]. EX1003, ¶133.

- (e) **Claim [9d]: "if the network resource is not in the set of
network destinations hosted on the plurality of server
computers in the shared network, redirecting the
browser application running on the client device within
the shared network associated with the anonymous
user to a pre-authentication capture destination hosted
on a first server computer, wherein the first server
computer is one of the plurality of server computers in
the shared network and wherein from the pre-
authentication capture destination the anonymous user
is free to visit any of the set of network destinations
hosted on the plurality of server computers in the
shared network without authentication."**

See [1.d]. EX1003, ¶134.

11. **Claim [10]: "The computer program product of claim 9,
wherein the redirecting further comprises sending from the
network access controller to the client device a response
containing an identifier identifying the pre-authentication
capture destination."**

See [3], [9]. EX1003, ¶135.

12. **Claim [11]: "The computer program product of claim 9, wherein the computer instructions are further translatable by the processor to perform: redirecting the browser application running on the client device back to the preauthentication capture destination when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality of server computers in the shared network."**

See [4], [9]. EX1003, ¶136.

13. **Claim 12**

- (a) **[12a]: "The computer program product of claim 9, wherein the computer instructions are further translatable by the processor to perform:"**

See [9]. EX1003, ¶137.

- (b) **[12b]: "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"**

See [9], [5a]. EX1003, ¶138.

- (c) **[12c]: " determining whether the second request contains an authentication token."**

See [9], [5b]. EX1003, ¶139.

14. **Claim 13**

- (a) **[13a]: "The computer program product of claim 12, wherein the second request does not contain the authentication token and wherein the computer instructions are further translatable by the processor to perform:"**

See [12], [6]. EX1003, ¶140.

- (b) [13b]: "redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network."

See [12], [6]. EX1003, ¶141.

15. Claim 14

- (a) Claim [14a]: "The computer program product of claim 12, wherein the second request contains the authentication token and wherein the computer instructions are further translatable by the processor to perform:"

See [12], [7]. EX1003, ¶142.

- (b) Claim [14b]: "redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."

See [12], [7]. EX1003, ¶143.

16. Claim 15

- (a) Claim [15a]: "The computer program product of claim 14, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network and wherein the computer instructions are further translatable by the processor to perform:"

See [12], [8]. EX1003, ¶144.

- (b) Claim [15b]: "allowing the client device access to the second network resource."

See [12], [8]. EX1003, ¶145.

17. Claim 16

- (a) Claim [16pre]: "An apparatus for controlling network access, comprising:"

See [1.pre], [9.pre]. EX1003, ¶146.

- (b) Claim [16a]: "a processor within a shared network; and"

See [9.pre]. EX1003, ¶147.

- (c) Claim [16b]: "a computer readable storage medium storing computer instructions translatable by the processor to perform:"

See [9.pre]. EX1003, ¶148.

- (d) Claim [16c]: "intercepting a request to access a network resource from a browser application running on a client device within the shared network coupled to the apparatus, wherein the client device is associated with an anonymous user;"

See [1.a]. EX1003, ¶149.

- (e) Claim [16d]: "determining whether the network resource referenced in the request is in a set of network destinations hosted on a plurality of server computers coupled to the apparatus, wherein the plurality of server computers resides on the shared network;"

See [1.b]. EX1003, ¶150.

- (f) Claim [16e]: "if the network resource is in the set of network destinations hosted on the plurality of server computers in the shared network, directing the browser application running on the client device within the shared network associated with the anonymous user to the network resource; and"

See [1.c]. EX1003, ¶151.

- (g) **Claim [16f]: " if the network resource is not in the set of network destinations hosted on the plurality of server computers in the shared network, redirecting the browser application running on the client device within the shared network associated with the anonymous user to a pre-authentication capture destination hosted on a first server computer, wherein the first server computer is one of the plurality of server computers in the shared network and wherein from the pre-authentication capture destination the anonymous user is free to visit any of the set of network destinations hosted on the plurality of server computers in the shared network without authentication."**

See [1.d]. EX1003, ¶152.

18. **Claim [17]: "The apparatus of claim 16, wherein the computer instructions are further translatable by the processor to redirect the browser application running on the client device back to the preauthentication capture destination when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality of server computers in the shared network."**

See [16], [4]. EX1003, ¶153.

19. **Claim [18]: "The apparatus of claim 16, further comprising: a first network interface coupled to the processor, wherein the computer instructions are further translatable by the processor to continuously monitor for network access from client devices on the first network interface."**

See [16]. Subbiah discloses a first network interface coupled to the processor, wherein the computer instructions are further translatable by the processor to continuously monitor for network access from client devices on the first network interface. EX1003, ¶154.

Subbiah discloses that communications networks access is handled via the wireless access point. For example, **Subbiah** discloses that "requests for network access are received wirelessly from clients via a wireless access point (*e.g.*, wireless access point 130) coupled to the network." EX1004, 12:14-17; *see also id.*, 17:10-11 ("a request from the client 340 is received by the access point 330"); *id.*, 4:15-18 ("method includes the step of receiving a request to access..."); *id.*, 2:22-3:3 ("advantageous to provide Internet access to mobile, wireless client equipped passengers" or "properly equipped users"); *id.*, 14:15-21 (wireless access point is configured to provide different levels of access to different clients). In order to provide such communication services, "wireless access point 330 waits for a wireless client (*e.g.*, client 340) to connect to the wired local network 301." *Id.*, 14:27-15:1. Thus, a POSITA would have understood, or at minimum found it obvious based on these disclosures, that the wireless access point would need to continuously monitor connection requests by client devices—and wireless client devices in particular—in order to facilitate such network access. *See* EX1003, ¶155.

20. Claim 19

- (a) [19.pre]: "The apparatus of claim 18, wherein the computer instructions are further translatable by the processor to perform:"

See [18]. EX1003, ¶156.

- (b) [19a]: "intercepting a second request from the browser application running on the client device associated with

the anonymous user to access a second network resource that is not in the set of network destinations; and"

See [18], [5a]. EX1003, ¶157.

- (c) **[19b]: "determining whether the second request contains an authentication token."**

See [18], [5b]. EX1003, ¶158.

21. Claim 20

- (a) **[20.pre]: " The apparatus of claim 19, wherein the computer instructions are further translatable by the processor to perform:"**

See [19]. EX1003, ¶159.

- (b) **Claim [20a]: "if the second request does not contain the authentication token, redirecting the browser application running on the client device associated with the anonymous user back to the preauthentication capture destination hosted on the first server computer in the shared network; and"**

See [19], [6]. EX1003, ¶160.

- (c) **Claim [20b]: "if the second request contains the authentication token, redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."**

See [19], [7]. EX1003, ¶161.

B. Ground 3 – Obviousness in View of Hinton and/or Crandell

1. Overview of Hinton and Motivation to Combine with Subbiah

Hinton teaches a system for "cross-domain, single-sign-on, authentication functionality," using an "authentication token" passed from one domain to another using "HTTP-redirection." EX1005, Abstract. As **Hinton** teaches, "HTTP Redirects are well known in the art. An HTTP Redirect allows a server to respond to a client request with instructions to load a resource at a different location, and in response, most browsers will automatically request the new resource in response to a redirect. When the browser receives the HTTP Redirect, the browser issues a new HTTP Request using the redirected URI provided in the HTTP Redirect." EX1005, p. 24. As part of this HTTP redirect process, and in the event a client is trying to access a "protected resource," the server "generates an introductory authentication token (step 410), preferably appends the token to the redirection URI, places the redirection URI in the HTTP Redirect message, and then sends the HTTP Redirect to the client (step 412)." *Id.*, pp. 23-24. **Hinton** further teaches appending the authentication token to the redirect URI as an ASCII-encoded string, and that the browser is not even aware that it is processing the token when copying from the URI redirect to the new URI request. *Id.*, pp. 25-26. In addition, **Hinton** teaches checking an HTTP request for an authentication token and, if no token is found, requiring the user to undergo an authentication process. *Id.*, p. 16 ("the server

determines whether the client's HTTP Request contains an introductory authentication token, preferably appended to the URI (step 212).... If the HTTP message does not have an introductory authentication token, then the server forces the user at the client to complete a manual authentication process"). EX1003, ¶¶81-83.

Thus, as **Hinton** teaches, it was well known in the art to use authentication tokens to track whether a user is, or needs to be, authenticated. EX1003, ¶¶84, 168. More generally, it was well known in the art to use tokens in a URI to track authentication state information about a client or client device. *Id.*, ¶84. A POSITA would have been motivated, and would have found it advantageous and obvious to apply **Hinton's** teachings of using an authentication token in a URI for an HTTP redirect in implementing **Subbiah's** access control system. *Id.* Like **Subbiah**, **Hinton** is in the same field and is analogous art to the '336 patent, namely controlling access to resources across communications networks and, more particularly, to controlling access to network resources in multi-domain networks. *E.g.*, EX1005, Abstract; EX1003, ¶85. **Hinton** is also pertinent to the alleged problem(s) identified in the '336 patent of the alleged need for controlled access to network resources. *E.g.*, EX1001, 1:34-38; EX1005, p. 2.

A POSITA would have recognized that **Hinton's** teachings of appending an authentication token to a URI would have improved, or at least have been an obvious

implementation of, **Subbiah's** access control system. For example, **Subbiah's** access control system already makes a determination at step 707 whether the network resource request is a "first time request" and redirects the user accordingly based on a simple yes/no to that determination. EX1004, FIG. 7. A POSITA thus would have found it advantageous to implement this determination using an authentication token in the URI, which would allow the server to simply look for the presence or absence of this token in determining whether to redirect the user to the local domain home page or to the authentication login page. EX1003, ¶86. A POSITA would have understood **Hinton's** teachings to provide known implementation details for the redirection functionality already present in **Subbiah**. *Id.*, ¶87.

In light of the foregoing, a POSITA would have found it obvious and straightforward to apply **Hinton's** teachings in implementing **Subbiah's** system and would have known that such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality. *Id.*, ¶84.

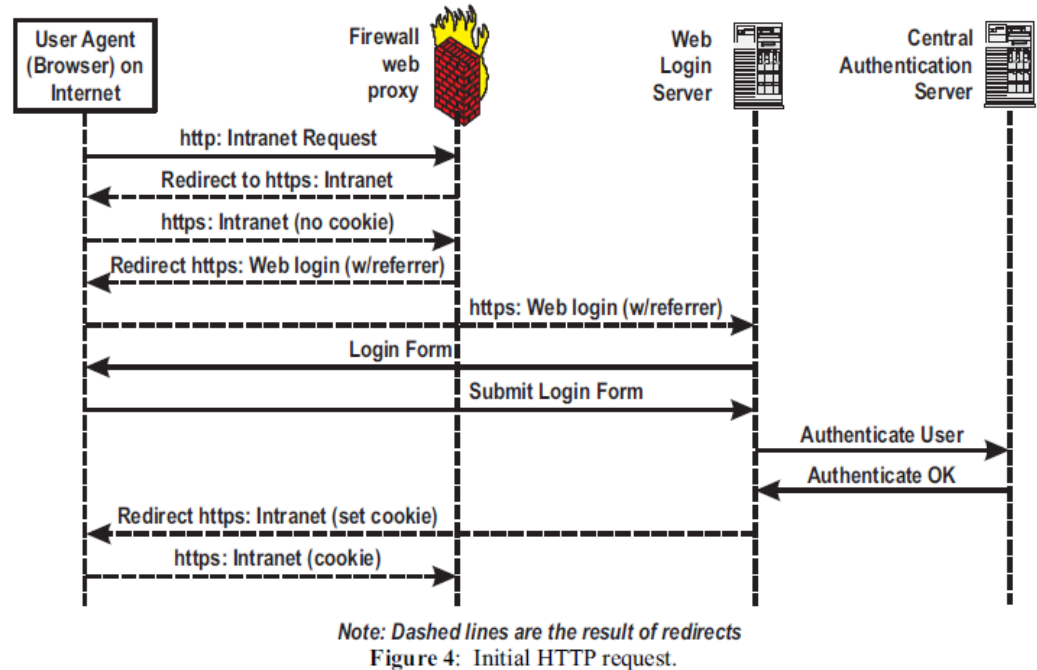
2. Overview of Crandell and Motivation to Combine

Crandell is a publication entitled "A Secure and Transparent Firewall Web Proxy," by Roger Crandell, James Clifford, and Alexander Kent, of Los Alamos National Laboratory. As stated on the face of **Crandell**, it was published as part of The USENIX Association's Proceedings of the 17th Large Installation Systems

Administration Conference. EX1007, Cover. **Crandell** is cited on the face of the '336 patent and was cited as prior art during prosecution. EX1002, 38, 165. EX1003, ¶88.

Crandell discloses a system and method "to provide a transparent firewall web proxy...allowing authorized and secure access to the many firewall-protected intranet web servers at Los Alamos National Laboratory (LANL)." EX1007, p. 23. The purported goal of **Crandell** was to provide "[c]ontrolled access to intranet web servers from the Internet." *Id.* In doing so, **Crandell** discloses "a web authentication system to tell whether or not to forward the user's HTTPS requests," and the service, "at minimum, must provide the following capabilities. First the proxy must be able to tell if an HTTPS request comes from an authenticated user session. Second, if the HTTPS request does not include valid authentication credentials, the proxy needs the URL of a web site that handles an initial, interactive user login." *Id.*, p. 25. **Crandell** recognizes that a "popular method[]" for keeping track of authenticated web sessions" uses "cookies." *Id.* (citing RFC 2965). In implementing this cookie-based scheme, **Crandell** discloses that "[t]he cookie string...contains no intrinsic value or information beyond being reasonably unique..." and "[e]very new HTTPS request causes the cookie to be re-verified." *Id.* **Crandell** further discloses using these cookies in an implementation scheme relying on "iptables redirect" rules. *Id.*, p. 26.

Figure 4 of **Crandell** discloses such an implementation with cookies being transferred back and forth as part of the HTTPS requests.



Id. EX1003, ¶¶89-90.

During prosecution, the Examiner expressly noted that **Crandell** teaches the use of "authentication token[s]" and pointed to **Crandell's** disclosure of cookies. In particular, the Examiner recognized that "Crandell further discloses intercepting at the network access controller a second request from the browser...; determining whether the second request contains an authentication token (*i.e.*, determining whether the second request contains a cookie); and redirecting the browser application" accordingly. EX1002, 167-168. The Applicant did not distinguish or

dispute this aspect of **Crandell** during prosecution but instead amended the independent claims only to secure allowance. *Supra*, §III.C; EX1003, ¶91.

Thus, as **Crandell** teaches, it was well known in the art to use cookies to track whether a user is, or needs to be, authenticated. EX1003, ¶92. More generally, it was well known in the art to use cookies in HTTP request to track state information about a client or client device. *Id.* A POSITA would have been motivated, and would have found it advantageous and obvious, to apply **Crandell's** teachings of using cookies in an HTTP redirect in implementing **Subbiah's** access control system. Like **Subbiah**, **Crandell** is in the same field and is analogous art to the '336 patent, namely controlling access to resources across communications networks and, more particularly, controlling access to network resources in multi-domain networks. *See, e.g.*, EX1007, p. 23; EX1003, ¶92. **Crandell** is also pertinent to the alleged problem(s) identified in the '336 patent of the alleged need for controlled access to network resources. *See, e.g.*, EX1001, 1:34-38; EX1007, p. 23. EX1003, ¶93

A POSITA would have recognized that **Crandell's** teachings of appending a cookie as part of an HTTP message would have improved, or at least have been an obvious implementation of, **Subbiah's** access control system. For example, **Subbiah's** access control system already makes a determination at step 707 whether the network resource request is a "first time request" and redirects the user

accordingly based on a simple yes/no to that determination. EX1004, FIG. 7. A POSITA thus would have found it advantageous to implement this determination using cookies, as taught by **Crandell**, which would allow the server to simply look for the presence or absence of this cookie in determining whether to redirect the user to the local domain home page or to the authentication login page. EX1003, ¶94. A POSITA would have understood **Crandell's** teachings to provide known implementation details for the redirection functionality already present in **Subbiah**. *Id.*

In light of the foregoing, a POSITA would have found it obvious and straightforward to apply **Crandell's** teachings in implementing **Subbiah's** system and would have known that such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality. EX1003, ¶95.

3. Claim [5pre]: "The method according to claim 1, further comprising:"

See §Error! Reference source not found., [5pre]. EX1003, ¶163.

4. Claim [5a]: "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"

See §Error! Reference source not found., [5a]. EX1003, ¶164.

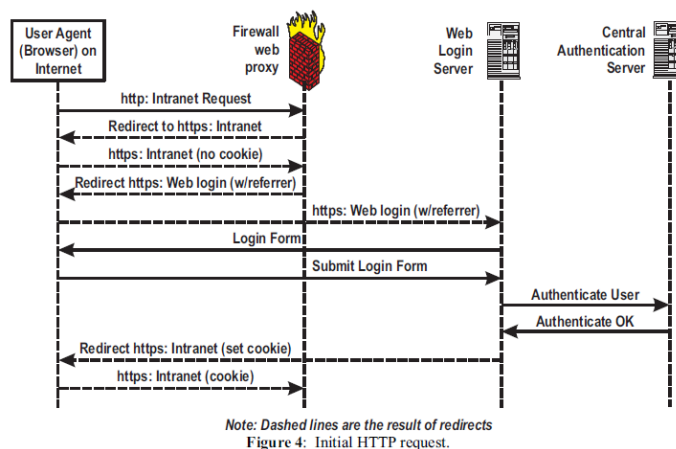
5. Claim [5b]: "determining whether the second request contains an authentication token."

Subbiah in view of Hinton and/or Crandell renders obvious determining whether the second request contains an authentication token. EX1003, ¶165.

See §Error! Reference source not found., [5b].

To the extent further disclosure is required, **Hinton** teaches appending an authentication token to a URI when a client requests a protected resource and using the presence or absence of that token to determine whether authentication is required. **Hinton** explains that the "server [] generates an introductory authentication token...appends the token to the redirection URI...places the redirection URI in the HTTP Redirect message, and then sends the HTTP Redirect to the client," and that "the server determines whether the client's HTTP Request contains an introductory authentication token...[and] [i]f the HTTP message does not have an introductory authentication token, then the server forces the user...to complete a manual authentication process." EX1005, pp. 16, 23-24. **Hinton** further teaches that an "HTTP Redirect allows a server to respond to a client request with instructions to load a resource at a different location," and that by "appending the token to the URI, the browser is not aware that it is processing the token when it copies the token from the HTTP Redirect to the new HTTP Request." *Id.*, pp. 24-26. EX1003, ¶166.

Similarly, **Crandell** discloses determining whether a request includes a cookie to control redirection, describing an "existing cookie based central web authentication service" in which "[e]very new HTTPS request causes the cookie to be re-verified," and showing that an "initial connection without a valid authentication cookie" triggers one sequence (Fig. 4), while a "connection request that has a valid cookie" follows another (Fig. 5). EX1007, pp. 25-26. EX1003, ¶167.



As discussed in §§V.B.1–V.B.2, a POSITA would have been motivated to apply Hinton's teachings of using a URI-appended authentication token, or Crandell's teachings of using cookies, in implementing **Subbiah's** access control system—*e.g.*, at step 707—to distinguish between first-time requests (requiring redirection to the Local Web Server) and repeat requests (redirected to the Burp Server). EX1003, ¶¶ 84-87, 92-95, 168.

6. **Claim [6]: "The method according to claim 5, wherein the second request does not contain the authentication token,**

further comprising redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network."

See §Error! Reference source not found., [6]. For the same reasons as explained in Grounds 1-2, above, a POSITA would have understood that implementing Subbiah with an authentication token (as discussed in claim 5) would have resulted in this limitation. EX1003, ¶¶169-170.

7. **Claim [7]: " The method according to claim 5, wherein the second request contains the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."**

See §Error! Reference source not found., [7]. For the same reasons as explained in Grounds 1-2, above, a POSITA would have understood that implementing Subbiah with an authentication token (as discussed in claim 5) would have resulted in this limitation. EX1003, ¶171.

8. **Claim [8]: "The method according to claim 7, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network."**

See §Error! Reference source not found., [8]. EX1007, ¶172.

9. **Claim [12a]: "The computer program product of claim 9, wherein the computer instructions are further translatable by the processor to perform:"**

See §Error! Reference source not found., [12a]. EX1007, ¶173.

10. **Claim [12b]: "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"**

See §Error! Reference source not found., [12a] [9], [5a]. EX1007, ¶174.

11. **Claim [12c]: "determining whether the second request contains an authentication token."**

See §Error! Reference source not found., [9], [5b]; §V.B.3, [5b]. EX1007, ¶175.

12. **Claim [13a]: "The computer program product of claim 12, wherein the second request does not contain the authentication token and wherein the computer instructions are further translatable by the processor to perform:"**

See §Error! Reference source not found., [13a]. EX1007, ¶176.

13. **Claim [13b]: "redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network."**

See §Error! Reference source not found., [13b]. EX1007, ¶177.

14. **Claim [14a]: "The computer program product of claim 12, wherein the second request contains the authentication token and wherein the computer instructions are further translatable by the processor to perform:"**

See §Error! Reference source not found., [14a]. EX1007, ¶178.

- 15. Claim [14b]: "redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."**

See §Error! Reference source not found., [14b]. EX1007, ¶179.

- 16. Claim [15a]: "The computer program product of claim 14, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network and wherein the computer instructions are further translatable by the processor to perform:"**

See §Error! Reference source not found., [15a]. EX1007, ¶180.

- 17. Claim [15b]: " allowing the client device access to the second network resource."**

See §Error! Reference source not found., [15b]. EX1007, ¶181.

- 18. Claim [19]: "The apparatus of claim 18, wherein the computer instructions are further translatable by the processor to perform:"**

See §Error! Reference source not found., [19]. EX1007, ¶182.

- 19. Claim [19a]: "intercepting a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"**

See §Error! Reference source not found., [19a]. EX1007, ¶183.

- 20. Claim [19b]: "determining whether the second request contains an authentication token."**

See §Error! Reference source not found., [19b], [18], [5b]; § V.B.3, [5b].

EX1007, ¶184.

- 21. Claim [20pre]: "The apparatus of claim 19, wherein the computer instructions are further translatable by the processor to perform:"**

See §Error! Reference source not found., [20pre]. EX1007, ¶185.

- 22. Claim [20a]: "if the second request does not contain the authentication token, redirecting the browser application running on the client device associated with the anonymous user back to the preauthentication capture destination hosted on the first server computer in the shared network; and"**

See §Error! Reference source not found., [20a]. EX1007, ¶186.

- 23. Claim [20b]: "if the second request contains the authentication token, redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."**

See §Error! Reference source not found., [20b]. EX1007, ¶187.

VI. MANDATORY NOTICES UNDER 37 C.F.R. §42.8(a)(1)

A. 37 C.F.R. §42.8(b)(1): Real Parties-In-Interest

Petitioner is the real party-in-interest.

B. 37 C.F.R. §42.8(b)(2): Related Matters

The '336 patent is asserted against Petitioner in *Netskope, Inc. v. Fortinet, Inc.*,

No. 4:25-cv-2360 (N.D. Cal. filed Mar. 7, 2025).

C. 37 C.F.R. §42.8(b)(3)-(4): Lead and Back-Up Counsel and Service Information

Designated Counsel for Petitioner and service information is below:

Lead Counsel	Back-Up Counsel
Andrew D. Gish (Reg. # 67,562) GISH PLLC 41 Madison Avenue New York, New York 10010 Telephone: (212) 518-7380 andrew@gishpllc.com	Ryan Iwahashi (Reg. # 63,378) GISH PLLC 50 California Street, Suite 1500 San Francisco, CA 94111 Telephone: (415) 630-8960 ryan@gishpllc.com Josef B. Schenker (<i>pro hac forthcoming</i>) 41 Madison Avenue New York, New York 10010 Telephone: (212) 518-7380 Josef.schenker@gishpllc.com

Petitioner consents to service by email at the addresses above.

VII. FEES UNDER 37 C.F.R. §42.103

Petition and Post-Institution fees totaling \$51,875.00 have been paid by electronic funds transfer.

VIII. CONCLUSION

Petitioner requests the Board institute IPR of the Challenged Claims and cancel them.

Respectfully Submitted,

Dated: October 10, 2025

/s/Andrew Gish

Andrew Gish (Reg. #67,562)

ATTORNEY FOR PETITIONER

CERTIFICATE OF WORD COUNT UNDER 37 C.F.R. §42.24(a)

I, the undersigned, do hereby certify that the attached petition contains 13,721 words, as measured by the Word Count function of Microsoft Word. This is less than the limit of 14,000 words as specified by 37 C.F.R. §42.24(a)(i).

Dated: October 10, 2025

/s/ Andrew Gish

Andrew Gish (Reg. # 67,562)

ATTORNEY FOR PETITIONER

CERTIFICATION OF SERVICE

The undersigned certifies service pursuant to 37 C.F.R. §§42.6(e) and 42.105 on the Patent Owner of a copy of this Petition for *Inter Partes* Review and supporting materials via FedEx at the following correspondence address of record:

25883 - MUNCK WILSON MANDALA L.L.P
2000 McKinney Ave Ste 1900
Dallas, TX
UNITED STATES

Dated: October 10, 2025

/s/ Andrew Gish

Andrew Gish (Reg. # 67,562)

ATTORNEY FOR PETITIONER