Field	Meaning
Primary Domain Name Server	IP address of **BinGO!**'s first Domain Name Server (DNS).
Secondary Domain Name Server	IP address of another Domain Name Server.
Primary WINS	IP address of **BinGO!**'s first WINS (Windows Internet Name Server) or NBNS (NetBIOS Name Server).
Secondary WINS	IP address of another WINS or NBNS.

Table 7-15: ***IP ➧ STATIC SETTINGS***

Field	Meaning
Dynamic Name Server Negotiation	Defines whether **BinGO!** receives IP addresses for *Primary Domain Name Server*, *Secondary Domain Name Server*, *Primary WINS* and *Secondary WINS* from the WAN partner or sends them to the WAN partner.

Table 7-16: ***WAN PARTNER ➧ EDIT ➧ IP ➧ ADVANCED SETTINGS***

Then, on page 201, BinGO UG shows that a WAN partner (e.g., a secure corporate network) can be sent DNS requests received by the BinGO! router for resolution and handling:

The *Dynamic Name Server Negotiation* field contains the following selection options:

Possible Values	Meaning
off	**BinGO!** does not send or answer requests for WINS or DNS IP addresses.
yes	The response is linked to the mode for issuing / receiving an IP address (setting under *IP Transit Network* in ***WAN PARTNER ➧ EDIT ➧ IP***): ■ **BinGO!** sends requests for WINS and DNS IP addresses to the WAN partner, if *dynamic client* is selected. ■ **BinGO!** answers requests for WINS and DNS IP addresses from the WAN partner, if *dynamic server* is selected. ■ **BinGO!** does not send or answer requests for WINS and DNS IP addresses, if *yes* or *no* is selected.
client (receive)	**BinGO!** sends requests for WINS and DNS IP addresses to the WAN partner.
server (send)	**BinGO!** answers requests for WINS and DNS IP addresses from the WAN partner.

Table 7-17: *Dynamic Name Server Negotiation*

Thus, in this second configuration (*i.e.*, where the BinGO! router was configured to connect to a router for the corporate network as a WAN Partner, and the BinGO! router has the Dynamic Name Server Negotiation variable set to be active), all DNS and WINS requests would be sent to the WAN Partner for resolution. *See also* BinGO at 202 ("Proceed as follows if you want

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

BinGO! to report the DNS or WINS entered to the WAN partner (Server Mode) or if DNS/WINS addresses other than those in the LAN are to be used for connections to the WAN partner (Client Mode, e.g. for dialing into an Internet Service Provider).").

BinGO thus shows two configurations in which a determination is made by a data processing device that intercepts DNS requests sent by a client in which it is determined whether the intercepted DNS request corresponds to a secure server.

Step (ii) of claim 1 specifies: "when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer."

As described above, BinGO shows two different configurations in which DNS requests from a client computer are sent to a router and evaluated. In each configuration, a determination is made whether the DNS request specifies a secure destination, or a non-secure destination (e.g., a non-secure website on the Internet).

In the first configuration (i.e., where the BinGO! router sends the request to a DNS server on the LAN on which the router is located), a determination is made whether the hostname in the DNS request matches a hostname in the local secure DNS server. If it does not, then the BinGO! router will send the request to a secondary DNS server as designated in its configuration. BinGO shows that ordinarily a BinGO! router will be configured to have an internet service provider (ISP) as a default WAN partner. *See, e.g.,* BinGO UG at 90 ("Generally, the route to the Internet provider is used as the default route, because most unknown packets are bound for the Internet anyway (e.g. www.bintec.de)."). In this configuration, if a DNS request specifying a non-secure destination (i.e., one that does not match a name on the local DNS server storing IP addresses of secure computers), then that DNS request would be sent to the ISP designated as a WAN partner, and the DNS server of this ISP would resolve the non-secure destination and return the IP address. *See, e.g.,* BinGO UG at 88 ("If you have configured Internet access with the Wizard and you do not have your own DNS server, you can obtain the IP address of your provider's DNS server. The router is known as the DNS proxy by the PCs in the LAN. When a request is made for a name resolution (e. g. for www.bintec.de), the PC asks the router, and the router in turn refers to the provider's DNS server. Translation of the address can then take place there.").

In the second configuration (i.e., where DNS requests are forwarded to a router at the secure corporate network), a determination is made whether the DNS specifies a secure or non-secure destination. In the latter case, the router at the corporate network will take steps to resolve the DNS request and return the IP address of the non-secure destination. *See, e.g.,* BinGO UG at 90 ("If you have not configured Internet access, but your head office has an Internet Service Provider, you can access the Internet via the provider of your WAN partner. … Due to the fact that your default route leads all unknown packets to your head office, and there another default route in turn sends all unknown packets to its Internet provider, you can access the Internet via your partner's network.")

BinGO thus shows that when an intercepted DNS request does not correspond to a secure server, a DNS function returns the IP address of the non-secure computer.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Step (iii) of claim 1 specifies: "(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer."

As explained above, BinGO shows processes whereby a BinGO! router automatically establishes an encrypted ISDN connection after authentication between client computers on a LAN with the BinGO! router and destination computers inside a secure corporate network. Also as explained above, this occurs after a DNS request generated on a client computer is evaluated and determined to be identifying as the destination a secure computer on the corporate network. BinGO further shows that it could also be configured to establish these connection using a variety of types of VPNs. *See, e.g.,* BinGO EFR at 73-98. In particular, BinGO EFR shows configurations in which the BinGO! router would establish encrypted tunnels between the client computer and the secure destination computer. *See, e.g.*, BinGO EFR at 82-84.

BinGO thus shows that in response to determining that a DNS request is requesting access to a secure target web site, automatically initiating an encrypted channel between the client computer and the target computer.

Accordingly, BinGO anticipates claim 1 of the '151 under 35 U.S.C. § 102(a).

2. Claim 2

Claim 2 of the '151 patent depends from claim 1, and specifies that "step (iii) comprises the steps of: (a) determining whether the client is authorized to access the secure server; and (b) when the client is authorized to access the secure server, sending a request to the secure server to establish an encrypted channel between the secure server and the client. "

BinGO explains that a BinGO! router could be configured to require authentication from client computers attempting to use the BinGO! router to gain access to a secure destination. For example, BinGO UG explains that all users must have authentication credentials (*i.e.*, user account and password) and that this is checked each time a user attempts to use the BinGO! router. For example, BinGO UG at 243 explains:

> You can log in to BinGO! in several different ways as described in chapter 5, page 97, but **logging in is always protected by a password**. Every failed attempt is logged by a syslog message indicating the source and creates a relevant SNMP trap. Pauses are introduced after several failed attempts in order to make automatic attempts to log in more difficult.

BinGO further explains that it uses conventional authentication techniques. *See, e.g.*, BinGO UG at 242 ("PAP, CHAP and MS-CHAP are the common procedures used for authentication of PPP connections. These use a standard procedure to exchange a user ID and a password for checking the identity of the far end.") BinGO also explains that it provides additional mechanisms to authenticate users, such as call-back functionality in which a remote user accessing a BinGO! router is called back to establish the connection. *See, e.g.*, BinGO UG at 242 (§ 8.2.4). *See also* BinGO UG at 40 ("Before every connection, BinGO! and the router at HQ check the incoming data to see if they should take the call. In order to protect the network against unauthorized

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

access, acceptance of the call only takes place after correct authentication. This authentication is based on a common password and two codes that you and your partner use for the connection."); *Id.* at 175-176 (authentication required for access to corporate network); BinGO EFR at 84-85 ("Both the ISP and the VPN Server will typically want to verify the initiating partner during connection establishment. Authentication is performed inband using PAP, CHAP, or MS-CHAP.").

BinGO also discloses that a remote computer (e.g., in a WAN partner such as a corporate headquarters network) may access a BinGO! router to perform remote configuration and administration functions. *See* BinGO UG at 130 ("The "isdnlogin service allows incoming data calls access to the SNMP shell of your BinGO!. This is how BinGO! can, for example, be remotely configured and administrated.") The BinGO! router inherently is a secure computer destination, requiring authentication to access and employing encryption for communications. *See* BinGO UG at 101-103 (describing process where BinGO! router receives ISDN call from remote computer and requires authentication to gain access to server administration functions); BinGO UG at 265 ("BinGO! supports the encryption of PPP connections to WAN partners. Encryption is based on the MPPE (Microsoft Point to Point Encryption) procedure with code lengths of 40 bits and 128 bits."). The BinGO! router also will host web pages that are accessible for administration purposes to authenticated users. *See, e.g.*, BinGO UG at 236 ("Every BinTec router has a homepage, the so-called HTTP status page. You can use this with the aid of an Internet browser (e.g. Netscape Navigator, Internet Explorer) to display the status of BinGO!. All users of the BinGO! LAN can then view the router status, provided they know the password for the user name ht-tp."); *see also generally*, *Id.* at 236-239. Thus, if a remote user fails to authenticate to the BinGO! router, that user will not be able to access any of the remote administration or status web page functions of the BinGO! router, and instead will be returned an error.

Accordingly, BinGO anticipates claim 2 of the '151 patent under § 102(a).

3. Claim 3

Claim 3 depends from claim 2, and specifies that "step (iii) further comprises the step of: (c) when the client is not authorized to access the secure server, returning a host unknown error message to the client.

As described above in connection with claims 1 and 2, BinGO shows systems and processes in which a BinGO! router serves as a DNS proxy server, and will establish encrypted channels with a secure server. BinGO! also explains that it employs conventional DNS procedures. *See, e.g.*, BinGO UG at page 358 (definition of domain name service/domain name server). BinGO further explains that it employs various conventional authentication techniques, including CHAP. *See, e.g.*, BinGO UG at 156; BinGO EFR at 82 (explaining that one VPN tunneling technique is PPTP according to RFC 1171). BinGO thus shows that BinGO! routers follow well-known and standardized industry protocols governing communications (e.g., PPTP (RFC 1171), DNS handling and resolution (RFC1034, 1035).

A client computer that fails to authenticate in any of the configurations specified in BinGO which employ standardized authentication procedures (e.g., CHAP pursuant to

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

RFC1171) will return an error that terminates the connection. For example, it was known in the art under the CHAP authentication protocol, a failure of authentication returns an error and should prompts termination of the connection. *See, e.g,* RFC 1994 at 9 ("If the Value received in a Response is not equal to the expected value, then the implementation MUST transmit a CHAP packet with the Code field set to 4 (Failure), and SHOULD take action to terminate the link."). Once terminated, the TCP/IP response will return an error as well, which commonly is the host unknown error message.

Accordingly, BinGO anticipates claim 3 of the '151 patent under 35 U.S.C. § 102(a).

4. Claim 4

Claim 4 depends from claim 3, and specifies that "the client comprises a web browser into which a user enters a URL resulting in the DNS request."

BinGO shows that web browsers on client computers were the typical type of application that would generate DNS requests. *See, e.g.,* BinGO UG at 15 ("Thus, via your router, as shown above, you can connect with the network of your Internet provider and thus avail of the usual services of the Internet, **such as the World Wide Web (WWW) or** e-mail."); *Id.* at 87 ("What about if you want to communicate or access data by simply using the name and not the number (IP address), for example, if you want to talk with the PC BossPC or **you want to see the Internet pages www.bintec.de**? BossPC and www.bin- tec.de are clearly not IP addresses, but names. As computers only understand IP addresses and not names, it is necessary for the names to be translated (resolved) into their corresponding IP addresses.")

Accordingly, BinGO anticipates claim 4 of the '151 patent under 35 U.S.C. § 102(a).

5. Claim 5

Claim 5 of the '151 patent depends from claim 1, and specifies "automatically initiating the encrypted channel between the client and the secure sewer comprises establishing an IF address hopping scheme between the client and the secure server."

Solely for the purposes of this request, Requestor observes that "secure sewer" and "IF address" may be determined by the Office to be typographical errors, such that the Office may consider a "secure sewer" to be referring to a "secure server" and an "IF address" to be referring to an "IP address."

BinGO shows several processes in which a VPN is established by creating an IP hopping scheme between the client and destination computers. For example, on pages 244-246, BinGO UG shows a protocol called Network Address Translation (NAT) which is used to route IP packets between client and destination computers. As explained on pages 244-246:

8.2.7 NAT (Network Address Translation)

NAT is a simple-to-operate procedure that can be used for four purposes in the BinTec implementation:

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.