US006557037B1

(12) **United States Patent**
Provino

(10) **Patent No.: US 6,557,037 B1**
(45) **Date of Patent: *Apr. 29, 2003**

(54) **SYSTEM AND METHOD FOR EASING COMMUNICATIONS BETWEEN DEVICES CONNECTED RESPECTIVELY TO PUBLIC NETWORKS SUCH AS THE INTERNET AND TO PRIVATE NETWORKS BY FACILITATING RESOLUTION OF HUMAN-READABLE ADDRESSES**

(75) Inventor: **Joseph E. Provino**, Cambridge, MA (US)

(73) Assignee: **Sun Microsystems**, Palo Alto, CA (US)

(*) Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/087,823**

(22) Filed: **May 29, 1998**

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/227**; 709/225; 709/228; 709/245; 713/201

(58) **Field of Search** 709/227, 228, 709/250, 245, 225; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,805,803	A	* 9/1998	Birrell et al.	395/187.01
5,826,029	A	* 10/1998	Gore, Jr. et al.	395/200.57
5,898,830	A	* 4/1999	Wesinger, Jr. et al.	395/187.01
5,983,270	A	* 11/1999	Abraham et al.	709/224
6,003,084	A	* 12/1999	Green et al.	709/227
6,006,268	A	* 12/1999	Colie et al.	709/227
6,119,234	A	* 9/2000	Aziz et al.	713/201

FOREIGN PATENT DOCUMENTS

EP	0 825 784 A2	7/1997
EP	0 887 979 A2	6/1998

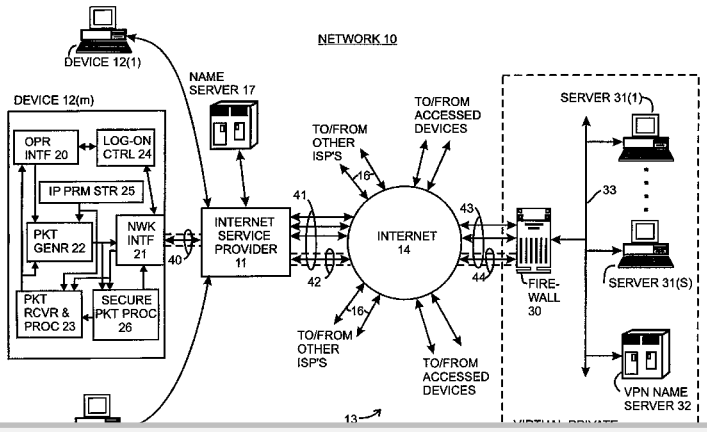
* cited by examiner

Primary Examiner—Dung C. Dinh
Assistant Examiner—Abdullahi E. Salad
(74) *Attorney, Agent, or Firm*—McCormick, Paulding & Huber LLP

(57) **ABSTRACT**

"A system [comprises] includes a virtual private network and an external device interconnected by a digital network. The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection therebetween, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device."

18 Claims, 1 Drawing Sheet



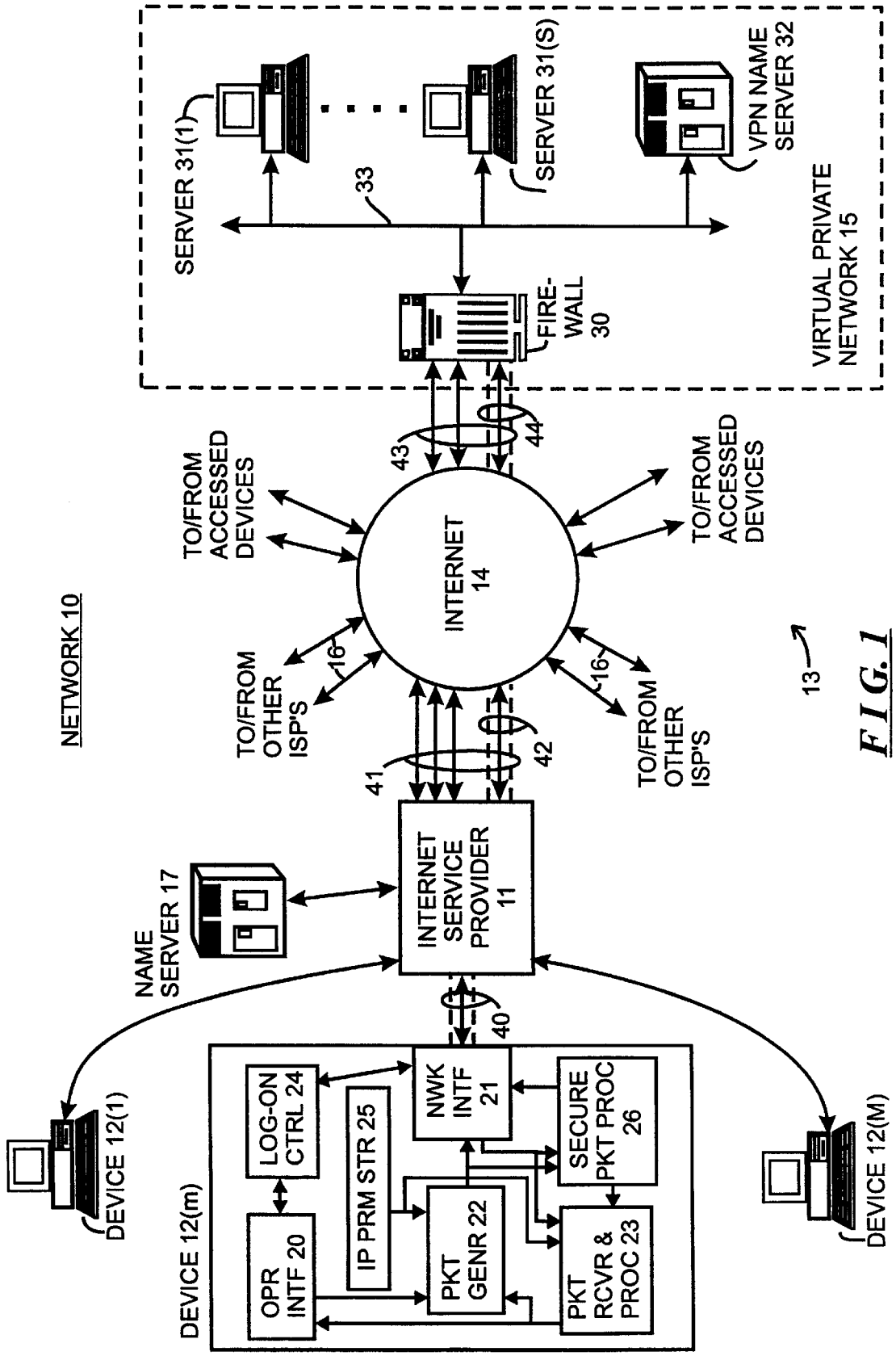


FIG. 1

SYSTEM AND METHOD FOR EASING COMMUNICATIONS BETWEEN DEVICES CONNECTED RESPECTIVELY TO PUBLIC NETWORKS SUCH AS THE INTERNET AND TO PRIVATE NETWORKS BY FACILITATING RESOLUTION OF HUMAN-READABLE ADDRESSES

FIELD OF THE INVENTION

The invention relates generally to the field of digital communications systems and methods, and more particularly to systems and methods for easing communications between devices connected to public networks such as the Internet and devices connected to private networks.

BACKGROUND OF THE INVENTION

Digital networks have been developed to facilitate the transfer of information, including data and programs, among digital computer systems and other digital devices. A variety of types of networks have been developed and implemented, including so-called "wide-area networks" (WAN's) and "local area networks" (LAN's), which transfer information using diverse information transfer methodologies. Generally, LAN's are implemented over relatively small geographical areas, such as within an individual office facility or the like, for transferring information within a particular office, company or similar type of organization. On the other hand, WAN's are generally implemented over relatively large geographical areas, and may be used to transfer information between LAN's as well as between devices that are not connected to LAN's. WAN's also include public networks, such as the Internet, which can carry information for a number of companies.

Several problems have arisen in connection with communication over a network, particularly a large public WAN such as the Internet. Generally, information is transferred over a network in message packets, which are transferred from one device, as a source device, to another device as a destination device, through one or more routers or switching nodes (generally, switching nodes) in the network. Each message packet includes a destination address which the switching nodes use to route the respective message packet to the appropriate destination device. Addresses over the Internet are in the form of an "n"-bit integer (where "n" may be thirty two or 128), which are difficult for a person to remember and enter when he or she wishes to enable a message packet to be transmitted. To relieve a user of the necessity of remembering and entering specific integer Internet addresses, the Internet provides second addressing mechanism which is more easily utilized by human operators of the respective devices. In that addressing mechanism, Internet domains, such as LAN's, Internet service providers ("ISP's") and the like which are connected in the Internet, are identified by relatively human-readable names. To accommodate the use of human-readable names, nameservers, also referred to as DNS servers, are provided to resolve the human-readable names to the appropriate Internet addresses. When an operator at one device, wishing to transmit a message packet to another device, enters the other device's human-readable name, the device will initially contact a nameserver. Generally, the nameserver may be part of the ISP itself or it may be a particular device which is accessible through the ISP over the Internet; in any case, the ISP will identify the nameserver to be used by the device. Thereafter, the device will provide the human-readable domain name to the nameserver. If the nameserver has or can obtain an integer Internet address for the human-readable domain name, it (that is, the nameserver) will provide the integer Internet address corresponding to the human-readable domain name to the operator's device. The device, in turn, can thereafter include the integer Internet address returned by the nameserver in the message packet and provide the message packet to the ISP for transmission over the Internet in a conventional manner. The Internet switching nodes use the integer Internet address to route the message packet to the intended destination device.

Other problems arise, in particular, in connection with the transfer of information over a public WAN such as the Internet. One problem is to ensure that information transferred over the WAN that the source device and the destination device wish to maintain confidential, in fact, remains confidential as against possible eavesdroppers which may intercept the information. To maintain confidentiality, various forms of encryption have been developed and are used to encrypt the information prior to transfer by the source device, and to decrypt the information after it has been received by the destination device. If it is desired that, for example, all information transferred between a particular source device and a particular destination device is maintained confidential, the devices can establish a "secure tunnel" therebetween, which essentially ensures that all information to be transferred by the source device to the destination device is encrypted (except for certain protocol information, such as address information, which controls the flow of network packets through the network between the source and destination devices) prior to transfer, and that the encrypted information will be decrypted prior to utilization by the destination device. The source and destination devices may themselves perform the encryption and decryption, respectively, or the encryption and decryption may be performed by other devices prior to the message packets being transferred over the Internet.

A further problem that arises in particular in connection with companies, government agencies, and private organizations whose private networks, which may be LAN's, WAN's or any combination thereof, are connected to public WAN's such as the Internet, is to ensure that their private networks are secure against others whom the companies do not wish to have access thereto, or to regulate and control access by others whom the respective organizations may wish to have limited access. To accommodate that, the organizations typically connect their private networks to the public WAN's through a limited number of gateways sometimes referred to as "firewalls," through which all network traffic between the internal and public networks pass. Typically, network addresses of domains and devices in the private network "behind" the firewall are known to nameservers which are provided in the private network, but are not available to nameservers or other devices outside of the private network, making communication between a device outside of the private network and a device inside of the private network difficult.

SUMMARY OF THE INVENTION

The invention provides a new and improved system and method for easing communications between devices connected to public networks such as the Internet and devices connected to private networks by facilitating resolution of secondary addresses, such as the Internet's human-readable addresses, to network addresses by nameservers or the like connected to the private networks.

interconnected by a digital network. The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection therebetween, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device.

BRIEF DESCRIPTION OF THE DRAWINGS

This invention is pointed out with particularity in the appended claims. The above and further advantages of this invention may be better understood by referring to the following description taken in conjunction with the accompanying drawing, in which:

FIG. **1** is a functional block diagram of a network constructed in accordance with the invention.

DETAILED DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT

FIG. **1** is a functional block diagram of a network **10** constructed in accordance with the invention. The network **10** as depicted in FIG. **1** includes an Internet service provider ("ISP") **11** which facilitates the transfer of message packets among one or more devices **12**(**1**) through **12**(M) (generally identified by reference numeral **12**(*m*)) connected to ISP **11**, and other devices, generally identified by reference numeral **13**, over the Internet **14**, thereby to facilitate the transfer of information in message packets among the devices **12**(*m*) and **13**. The ISP **11** connects to the Internet **14** over one or more logical connections or gateways or the like (generally referred to herein as "connections") generally identified by reference numeral **41**. The ISP **11** may be a public ISP, in which case it connects to devices **12**(*m*) which may be controlled by operators who are members of the general public to provide access by those operators to the Internet. Alternatively, ISP **11** may be a private ISP, in which case the devices **12**(*m*) connected thereto are generally operated by, for example, employees of a particular company or governmental agency, members of a private organization or the like, to provide access by those employees or members to the Internet.

As is conventional, the Internet comprises a mesh of switching nodes (not separately shown) which interconnect ISP's **11** and devices **13** to facilitate the transfer of message packets thereamong. The message packets transferred over the Internet **14** conform to that defined by the so-called Internet protocol "IP" and include a header portion, a data portion, and may include a error detection and/or correction including, for example, a destination address that identifies the device that is to receive the message packet as the destination device and a source address that identifies the device which generated the message packet. For each message packet, the destination and source addresses are each in the form of an integer that uniquely identifies the respective destination and source devices. The switching nodes comprising the Internet **14** use at least the destination address of each respective message packet to route it (that is, the respective message packet) to the destination device, if the destination device is connected to the Internet, or to an ISP **11** or other device connected to the Internet **14**, which, in turn, will forward the message packet to the appropriate destination. The data portion of each message packet includes the data to be transferred in the message packet, and the error detection and/or correction portion contains error detection and/or correction information which may be used to verify that the message packet was correctly transferred from the source to the destination device (in the case of error detection information), and correct selected types of errors if the message packet was not correctly transferred (in the case of error correction information).

The devices **12**(*m*) connected to ISP **11** may comprise any of a number of types of devices which communicate over the Internet **14**, including, for example, personal computers, computer workstations, and the like, with other devices **13**. Each device **12**(*m*) communicates with the ISP **11** to transfer message packets thereto for transfer over the Internet **14**, or to receive message packets therefrom received by the ISP **11** over the Internet **14**, using any convenient protocol such as the well-known point-to-point protocol ("PPP") if the device **12**(*m*) is connected to the ISP **11** using a point-to-point link, any conventional multi-drop network protocol if the device **12**(*m*) is connected to the ISP **11** over a multi-drop network such as the Ethernet, or the like. The devices **12**(*m*) are generally constructed according to the conventional stored-program computer architecture, including, for example, a system unit, a video display unit and operator input devices such as a keyboard and mouse. A system unit generally includes processing, memory, mass storage devices such as disk and/or tape storage elements and other elements (not separately shown), including network and/or telephony interface devices for interfacing the respective device to the ISP **11**. The processing devices process programs, including application programs, under control of an operating system, to generate processed data. The video display unit permits the device to display processed data and processing status to the user, and the operator input device enables the user to input data and control processing.

These elements of device **12**(*m*), along with suitable programming, cooperate to provide device **12**(*m*) with a number of functional elements including, for example, an operator interface **20**, a network interface **21**, a message packet generator **22**, a message packet receiver and processor **23**, an ISP log-on control **24**, an Internet parameter store **25** and, in connection with the invention, a secure message packet processor **26**. The operator interface **20** facilitates reception by the device **12**(*m*) of input information from the operator input device(s) of device **12**(*m*) and the display of output information to the operator on the video display device(s) of the device **12**(*m*). The network interface **21** facilitates connection of the device **12**(*m*) to the ISP **11** using the appropriate PPP or network protocol, to transmit message packets to the ISP **11** and receive message packets therefrom. The network interface **21** may facilitate connec-

telephone system. Alternatively or in addition, the network interface **21** may facilitate connection through the ISP **11** over, for example, a conventional LAN such as the Ethernet. The ISP log on control **24**, in response to input provided by the operator interface **20** and/or in response to requests from programs (not shown) being processed by the device **12**(*m*), communicates through the network interface **21** to facilitate the initialization ("log-on") of a communications session between the device **12**(*m*) and the ISP **11**, during which communications session the device **12**(*m*) will be able to transfer information, in the form of, message packets with other devices over the Internet **14**, as well as other devices **12**(*m'*) (m'≈m) connected to the ISP **11** or to other ISP's. During a log-on operation, the ISP log-on control **24** receives the Internet protocol ("IP") parameters which will be used in connection with message packet generation during the communications session.

During a communications session, the message packet generator **22**, in response to input provided by the operator through the operator interface **20**, and/or in response to requests from programs (not separately shown) being processed by the device **12**(*m*), generates message packets for transmission through the network interface **21**. The network interface **21** also receives message packets from the ISP **11** and provides them to message packet receiver and processor **23** for processing and provision to the operator interface **20** and/or other programs (not shown) being processed by the device **12**(*m*). If the received message packets contain information, such as Web pages or the like, which is to be displayed to the operator, the information can be provided to the operator interface **20** to enable the information to be displayed on the device's video display unit. In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device **12**(*m*) for processing.

Generally, elements such as the operator interface **20**, message packet generator **22**, message packet receiver and processor **23**, ISP log-on control **24** and Internet parameter store **25** may comprise elements of a conventional Internet browser, such as Mosaic, Netscape Navigator and Microsoft Internet Explorer.

In connection with the invention, as noted above the device **12**(*m*) also includes a secure message packet processor **26**. The secure message packet processor **26** facilitates the establishment and use of a "secure tunnel," which will be described below, between the device **12**(*m*) and another device **12** (*m'*) (m'≈m) or **13**. Generally, in a secure tunnel, information in at least the data portion of message packets transferred between device **12**(*m*) and a specific other device **12**(*m'*) (m'≈m) or **13** is maintained in secret by, for example, encrypting the data portion prior to transmission by the source device. Information in other portions of such message packets may also be maintained in secret, except for the information that is required to facilitate the transfer of the respective message packet between the devices, including, for example, at least the destination information, so as to allow the Internet's switching nodes and ISP's to identify the device that is to receive the message packet.

In addition to ISP **11**, a number of other ISP's may connect to the Internet, as represented by arrows **16**, facilitating communications between devices which are connected to those other ISP's with other devices over the Internet, which may include the devices **12**(*n*) connected to ISP **11**.

including personal computers, computer workstations, and the like, and also including mini-and mainframe computers, mass storage systems, compute servers, local area networks ("LAN's") and wide area networks ("WAN's") including such devices and numerous other types of devices which may be connected directly or indirectly to the networks. In connection with the invention, at least one of the devices will include at least one private network, identified as virtual private network **15**, which may be in the form of a LAN or WAN. The virtual private network **15** may comprise any of the devices **12**(*m'*) (m'≈m) (thereby connecting to the Internet **14** through an ISP) or **13** (thereby connecting directly to the Internet **14**); in the illustrative embodiment described herein, the virtual private network **15** will be assumed to comprise a device **13**. The virtual private network **15** itself includes a plurality of devices, identified herein as a firewall **30**, a plurality of servers **31**(**1**) through **31**(S) (generally identified by reference numeral **31**(*s*)) and a nameserver **32**, all interconnected by a communication link **33**. The firewall **30** and servers **31**(*s*) maybe similar to any of the various types of devices **12**(*m*) and **13** described herein, and thus may include, for example, personal computers, computer workstations, and the like, and also including mini-and mainframe computers, mass storage systems, compute servers, local area networks ("LAN's") and wide area networks ("WAN's") including such devices and numerous other types of devices which may be connected directly or indirectly to the networks.

As noted above, the devices, including devices **12**(*m*) and devices **13**, communicate by transferring message packets over the Internet. The devices **12**(*m*) and **13** can transfer information in a "peer-to-peer" manner, in a "client-server" manner, or both. Generally, in a "peer-to-peer" message packet transfer, a device merely transfers information in one or more message packets to another device. On the other hand, in a "client-server" manner, a device, operating as a client, can transfer a message packet to another device, operating as a server to for example, initiate service by the other device. A number of types of such services will be appreciated by those skilled in the art, including, for example, the retrieval of information from the other device, to enable the other device to perform processing operations, and the like. If the server is to provide information to the client, it (that is, the server) may generally be referred to as a storage server. On the other hand, if the server is to perform processing operations at the request of the client, it (that is, the server) may generally be referred to as a compute server. Other types of servers, for performing other types of services and operations at the request of clients, will be appreciated by those skilled in the art.

In a client/server arrangement, device **12**(*m*) requiring service by, for example, a device **13**, generates one or more request message packets requesting the required service, for transfer to the device **13**. The request message packet includes the Internet address of the device **13** that is, as the destination device, to receive the message packet and perform the service. The device **12**(*m*) transfers the request message packet(s) to the ISP **11**. The ISP **11**, in turn, will transfer the message packet over the Internet to the device **13**. If the device **13** is in the form of a WAN or LAN, the WAN or LAN will receive the message packet(s) and direct it (them) to a specific device connected therein which is to provide the requested service.

In any case, after the device **13** which is to provide the requested service receives the request message packet(s), it

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.