US006247054B1

(12) **United States Patent**
Malkin

(10) **Patent No.: US 6,247,054 B1**
(45) **Date of Patent: *Jun. 12, 2001**

(54) **METHOD AND APPARATUS FOR REDIRECTING PACKETS USING ENCAPSULATION**

(75) Inventor: **Gary Malkin**, Lowell, MA (US)

(73) Assignee: **Nortel Networks Limited**, Montreal (CA)

(*) 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.: **08/822,848**

(22) Filed: **Mar. 24, 1997**

(51) **Int. Cl.**[7] **G06F 15/173**; G06F 15/16
(52) **U.S. Cl.** **709/225**; 709/219
(58) **Field of Search** 395/200.31, 200.32, 395/200.33, 200.36, 200.49, 200.55, 200.56; 709/201, 202, 203, 206, 219, 225, 226

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,426,427	*	6/1995	Chinnock et al.	340/827
5,706,427	*	1/1998	Tabuki	395/187.01
5,708,780	*	1/1998	Levergood et al.	395/200.12
5,764,890	*	6/1998	Glasser et al.	395/188.01
5,774,660	*	6/1998	Brendel et al.	395/200.31
5,781,550	*	7/1998	Templin et al.	370/401
5,812,776	*	9/1998	Gifford	395/200.47

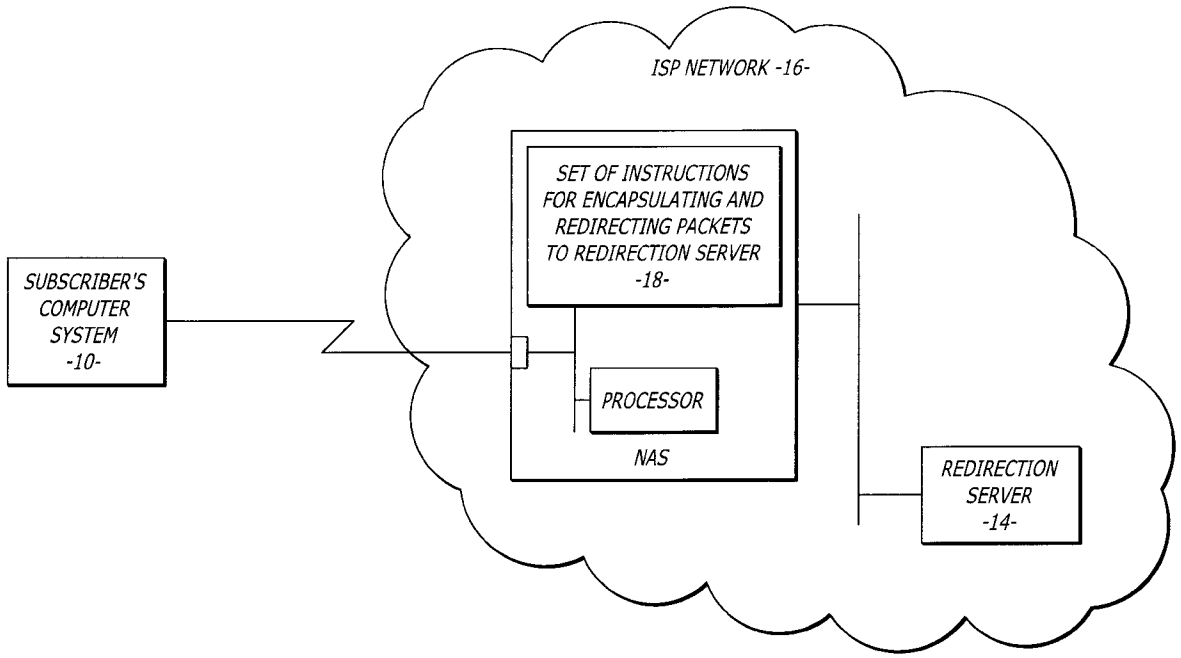
* cited by examiner

Primary Examiner—Glenton B. Burgess
Assistant Examiner—Kenneth W. Fields
(74) *Attorney, Agent, or Firm*—Blakely Sokoloff Taylor & Zafman LLP

(57) **ABSTRACT**

A method and apparatus for redirecting packets using encapsulation techniques. In one embodiment, an Internet subscriber transmits an Internet service request to a Network Access Server (NAS). The service request is transmitted in a first packet. The NAS analyzes the first packet to determine whether the service request exceeds the subscriber's internet subscription. If the request exceeds the subscriber's subscription, the NAS encapsulates the first packet into a second packet and redirects the second to a redirection server. The packet is encapsulated to preserve the address of the original destination of the service request. Upon receipt, the redirection server generates a reply to the internet service request which specifies why the service request was denied. The redirection server also substitutes the address of the original destination as the source of the reply message to allow the reply message to be received as reply from the original destination.

46 Claims, 3 Drawing Sheets



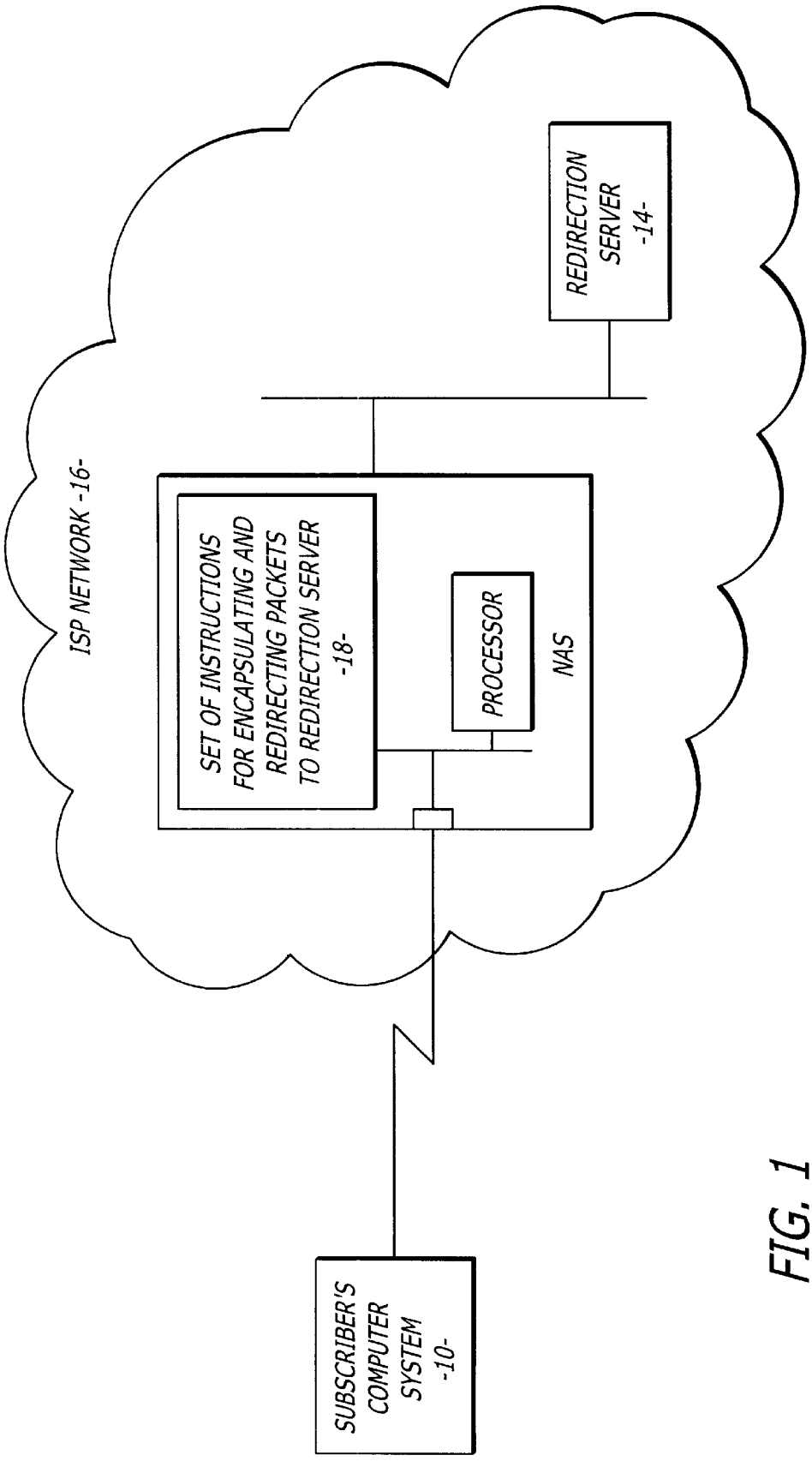
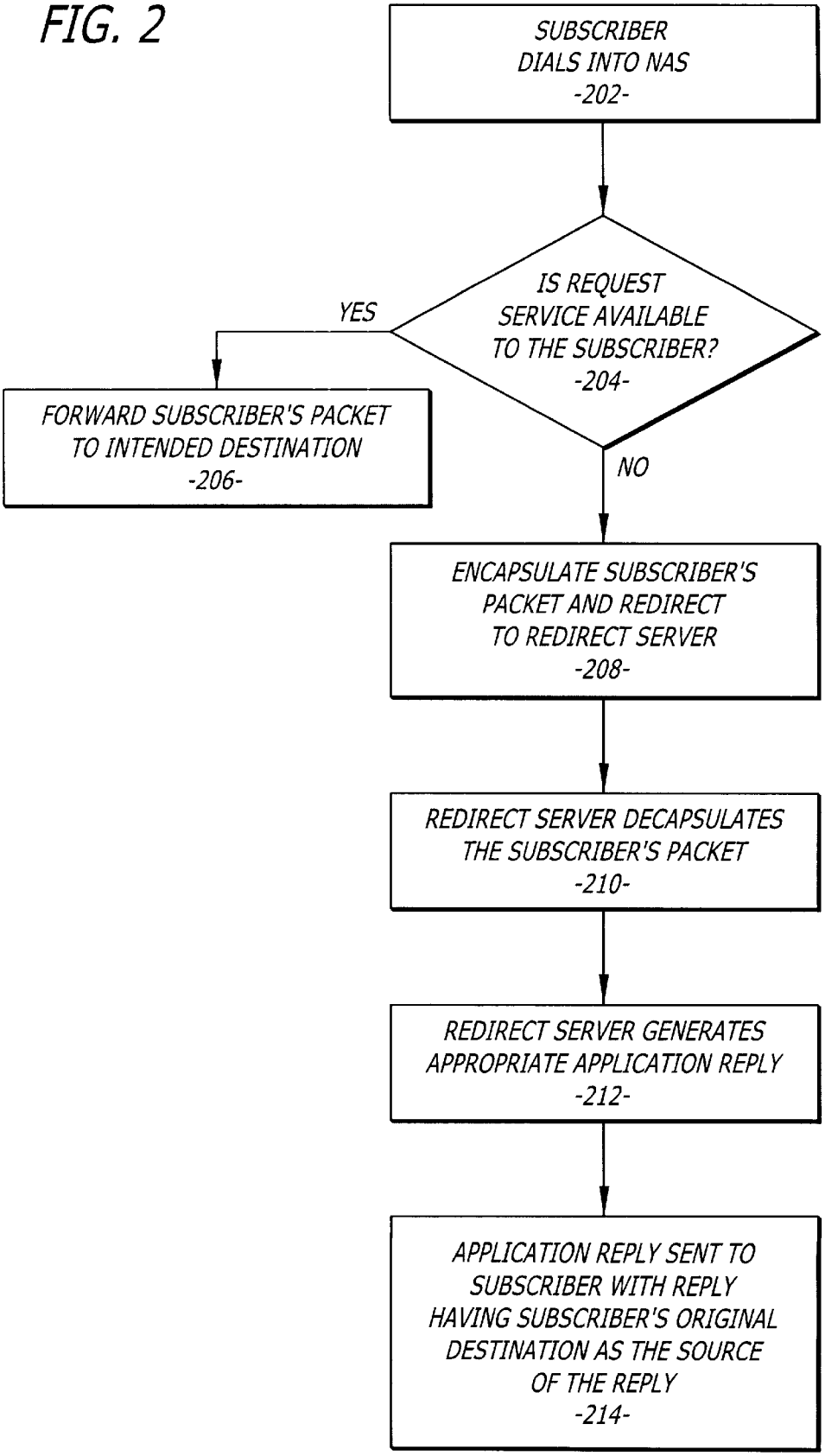


FIG. 1

FIG. 2



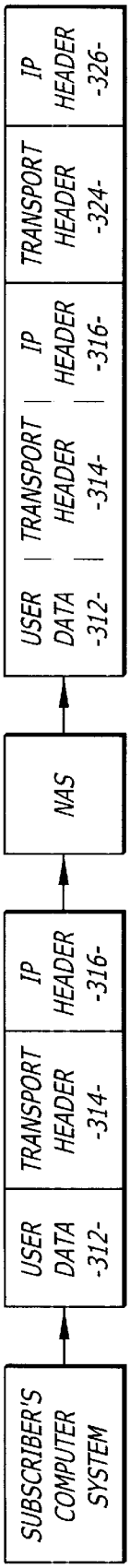


FIG. 3

METHOD AND APPARATUS FOR REDIRECTING PACKETS USING ENCAPSULATION

FIELD OF THE INVENTION

The present invention relates to computer networking systems, and in particular, the invention relates to redirecting packets using encapsulation.

BACKGROUND OF THE INVENTION

Many Internet Service Providers (ISPs) offer multiple levels of service, charging a different fee for each service level. For example, a subscriber of an ISP may subscribe to e-mail only, connection access (i.e., Telnet and FTP), or full access which would allow access to the World Wide Web (WWW).

Typically, the ISPs are configured so that a subscriber cannot use a service which is not included in the subscriber's subscription. The Network Access Servers (NAS), which provide point-of-presence dial-in access for the ISPs, may provide filtering to prohibit a subscriber from accessing services not included in the subscriber's subscription. When a NAS detects a subscriber attempting to exceed their allowed service level, the NAS typically discards the subscriber's packet (which contains a request for the service), and returns a simple "cannot connect" type message to the subscriber.

As a result, the subscriber is uninformed as to why they are unable to connect or receive their requested service. As such, it would be desirable to return an appropriate application level message to the subscriber providing a more detailed explanation why the requested service is unavailable to the subscriber.

SUMMARY OF THE INVENTION

The present invention provides a method and apparatus for redirecting packets using encapsulation techniques. In one embodiment, an Internet subscriber transmits an Internet service request to a Network Access Server (NAS). The service request is transmitted in a first packet. The NAS analyzes the first packet to determine whether the service request exceeds the subscriber's internet subscription. If the request exceeds the subscriber's subscription, the NAS encapsulates the first packet into a second packet and redirects the second to a redirection server. The packet is encapsulated to preserve the address of the original destination of the service request.

Upon receipt, the redirection server generates a reply to the internet service request which specifies why the service request was denied. The redirection server also substitutes the address of the original destination as the source of the reply message to allow the reply message to be received as reply from the original destination.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings, and in which:

FIG. **1** illustrates a network configuration implementing one embodiment of the present invention.

FIG. **2** illustrates a flow diagram describing the steps of the invention according to one embodiment.

FIG. **3** illustrates an encapsulation technique performed according to one embodiment of the present invention.

DETAILED DESCRIPTION

A method and apparatus are described for redirecting application packets using encapsulation techniques. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well-known standards, structures, and techniques have not been shown in order not to unnecessarily obscure the present invention.

As discussed above, in the prior art background section, there is a need to provide computer users/ISP subscribers with a more informative message explaining why they are unable to receive their requested Internet service. One approach is to return an appropriate application level message to the subscriber specifying in more detail why the service is unavailable to the subscriber. For example, the application message could indicate to the subscriber that they are attempting to access the WWW, but their subscription to the ISP does not include access to the WWW.

In order to return such a message, the NAS **12** of the present invention, as shown in FIG. **1**, is configured to detect when a service request exceeds a computer operator's subscription. In such a case, the NAS **12** may redirect the subscriber's request (in the form of a packet) to a Redirection Server **14** included the ISP network **16**. The Redirection Server will respond to the packet by generating and sending an appropriate application level reply message to the subscriber indicating why the request has been denied.

The message from the Redirection Server will be sent as a "reply" to the subscriber's original service request. The subscriber's computer system, however, will typically expect the reply message to have been sent from the original destination of the subscriber's original service request (e.g., a WWW site).

The reply message from the redirection server will be transferred via packets. The packets typically include data and a header. The header typically specifies the source of the packet (i.e., the redirection server) and the destination of the packet (i.e., the subscriber's computer).

When the subscriber's computer system receives the reply message from the Redirection Server, their computer will typically execute an algorithm to check the integrity of the data in the reply message to determine whether some of the data may have been lost while being transmitted. The algorithm is commonly referred to as a checksum.

The checksum will typically analyze the source and destination addresses provided in the header of the packets. Considering the reply packets sent from the redirection server are being sent as a reply to the subscriber's original service request, the checksum performed by subscriber's computer system will expect the source address of the reply packet to match the destination address of the subscriber's original service request.

As a result, the reply message from the redirection server will most likely fail the checksum because it has been sent from the redirection server, rather than being sent from the destination of the original service request. Therefore, the subscriber's computer system will assume the data of the reply message is faulty and dispose of the reply message. As a result, the subscriber will not receive the message explaining why the original service request was denied.

One solution to the problem is to have the Redirection Server perform a "spoofing" technique. Using the spoofing technique, the Redirection Server will substitute the desti-

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.