(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 October 2001 (11.10.2001)

PCT

(10) International Publication Number
WO 01/75626 A1

(51) International Patent Classification[7]: G06F 15/16

(21) International Application Number: PCT/CA01/00442

(22) International Filing Date: 30 March 2001 (30.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/193,362 31 March 2000 (31.03.2000) US

(71) Applicants *(for all designated States except US)*: **EICON TECHNOLOGY CORPORATION** [CA/CA]; 9800 Cavendish Boulevard, Montreal, Québec H4M 2V9 (CA). **CHABBERT, Martin** [CA/CA]; 93 Bedford, Baie d'Urfé, Québec H9X 2Z7 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MAHER, Tom** [IE/IE]; 4 Glencairn Chase, 18 Dublin (IE). **GADBOIS, Martin** [CA/CA]; Apt. 22, 3597 St-Urbain, Montreal, Québec H2X 2N6 (CA).

(74) Agents: **ANGLEHART, James** et al.; Swabey Ogilvy Renault, Suite 1600, 1981 McGill College Avenue, Montréal, Québec H3A 2Y3 (CA).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/75626 A1

(54) Title: BRIDGE CONFIGURATION OVER IP/WEB

(57) Abstract: A method for locally configuring a bridge is provided. The method is used when the connection to a remote router or gateway is lost or down. The method comprises the steps of : sniffing the LAN traffic, detecting DHCP requests that are not answered to, enabling an on-board DHCP server, detecting the current LAN subnet address, sniffing the LAN traffic, detecting the DNS requests with the Bridge's name, locating an IP address not used on the LAN, sending answers to requests using the new IP address, accessing the bridge with the new IP address, configuring the bridge through the web.

BRIDGE CONFIGURATION OVER IP/WEB

FIELD OF THE INVENTION

The invention relates to the field of bridge devices on networks and more particularly, to locally configuring these bridge devices.

BACKGROUND OF THE INVENTION

When installing new terminal equipment to be connected to a network, such as a local area network (LAN), it is necessary to assign an Internet protocol (IP) network address to the new equipment, and a variety of methods for doing so are used. The most basic form of address management is to manually assign an IP address to the new terminal by directly setting or programming the network address at the new terminal using knowledge (i.e. a list) of IP addresses already used on the network, so as to be able to select a new and available address. Each terminal typically has a Media Access Control address (MAC address), which is a hardware address that uniquely identifies each node of a network. The network manager or administrator is thus the "keeper" of the list of used addresses together with the MAC addresses of each device, and he or she is required to install any new terminal equipment on the network.

It is also common for equipment to have a factory set IP address, and for the network administrator to use the factory address if it is within the range of usable addresses on the network, and it is not already assigned to a different device. If the factory set address is not compatible with the range of addresses used on the LAN, it is necessary to change the IP address of the new equipment.

To change the static IP address of new equipment to be compatible with the LAN requires an input interface. It is known to use a communications interface on the terminal to which a console can be connected to provide the input interface, and it is also known to use Dual In-line Package (DIP) switches on the equipment for setting the static address. These options either require considerable effort and/or extra equipment.

Bridges typically do the following: they listen to all traffic on the network, check source and destination MAC addresses of each packet, learn from

experience to build and maintain routing tables in the bridge's RAM for the nodes on the network based on the source addresses, forward packets to all computers on all segments if the address is not in the routing table, discard the packet if the destination segment is the same as the source segment and forward the packet to the right segment if the address is in the routing table. Bridges work at the data link layer, whereas routers work at the network layer. Bridges are protocol independent; routers are protocol dependent. Bridges are faster than routers because they do not have to read the protocol to glean routing information.

The Address Resolution Protocol (ARP) is the process of mapping a TCP/IP host's IP address to its hardware address on broadcast-based networks. ARP uses a local broadcast of the destination IP address to acquire the hardware address of the destination host or gateway. Once the hardware address is obtained, both the IP address and the hardware address are stored as one entry in the ARP cache. The ARP cache is always checked for an IP address/hardware address mapping before initiating an ARP request broadcast. An ARP request is initiated any time a host tries to communicate with another host. The source host's IP address and hardware address are included in the request. The ARP request is sent as a broadcast so that all local hosts can receive and process it. If a host does not find a match to its own IP address, it ignores the request. The destination host which determines that the IP address in the request matches its own, sends an ARP reply directly to the source host with its hardware address. It then updates the ARP cache.

If the destination IP address is for a host on a remote network, the ARP broadcast is for a router that can forward datagrams to the destination host's network. The source host checks the local routing table for a route to a destination host or network. If no mapping is found, the source host determines the IP address of the default gateway. The source host then checks the ARP cache for the IP address/ hardware address mapping of the specified gateway.

An Ethernet LAN is a grouping of PCs that are directly connected together through an Ethernet link. These PCs all have different MAC addresses (assigned by manufacturing) and IP address (assigned by management, or the DHCP protocol). All PCs on a LAN must be on the same subnet (i.e. the first part of the address is the same, usually the three first bytes).

If a PC wants to reach another PC on the same subnet, it will fill the packet with the real Source and Destination MAC addresses (it will have discovered this address with the ARP protocol), as well as Source and Destination IP addresses.

If a PC wants to reach an IP address that is not on the same subnet, it will send the packet to the configured default Gateway. In this case, the IP part of the packet will be the same as if the machines were on the same subnet (i.e. source and destination IP addresses), but the Destination MAC address will be the one of the Gateway (or Router). Thus, the Router must be on the same subnet as the PCs on the LAN, because they need to be able to reach the router directly.

In the case of a bridging device, the router is on the other side of a WAN link (DSL for example). The bridge's goal is to link the Router to the LAN. For this to work, the Bridge device must be transparent (i.e. it must not modify the contents of the packets); it must only forward the packets on the WAN link. If this is achieved, the Router is virtually on the same LAN as the PCs. The PCs don't know that their Router is on the other side of a DSL link.

Since the Bridge is transparent in this situation, it is not reachable from the PCs, thus, it is not possible to configure it.

Different methods of configuring terminal devices on a LAN have been proposed. The first solution is to provide configuration/maintenance functions via another channel (e.g. a serial interface) thereby removing the need to use TCP/IP. A configuration terminal would be directly connected to the device to configure using a serial interface and the appropriate changes would be made. The second solution is to manually assign the device an IP address with a matching network address (e.g. via the first solution) using, for example, dip switches. The third solution is to allow the service provider to dynamically assign a host address to the bridge, using for example DHCP. In that case, the ISP assigns an IP address to the bridge which is valid on the subnet as it would for any PC on the subnet. The first and second methods make the product difficult to install because of a requirement for additional equipment and knowledge of the network on which the device is being installed. The third method suffers from a serious limitation: the device uses up an IP address, which the service provider may charge for.

If the PCs were on the same subnet as the Bridge, adding an IP stack in the Bridge that receives all the packets, and answers when packets are destined to it, would be the easiest solution. In this case, the Bridge becomes just another station on the LAN. However, the drawback to this solution is that the IP address of the PCs must be reconfigured manually every time a user wants to configure the Bridge.

When the service provider is not available and the user is therefore not connected to the ISP, the LAN IP address cannot be determined. The bridge's configuration and maintenance settings can therefore not be accessed through the web and with IP requests because the presence of the bridge on the LAN is not confirmed.

Because it is essential to still be able to configure the bridge, it is necessary to have a backup procedure used to communicate with the bridge properly even when the service provider is not available. It would be advantageous for the bridge to be able to fake the DNS and temporarily enable DHCP while the service provider is down.

SUMMARY OF THE INVENTION

Accordingly, an object of the present invention is to provide a DHCP on a bridge which will be activated when the connection to the remote side of the bridge is down.

An object of the present invention is to provide an inspection module for bridges on networks which fakes the DNS and temporarily enables DHCP when the service provider is not available.

Another object of the present invention is to have the bridge sense the IP network address of a LAN and to borrow a valid IP address within that IP network.

Another object of the present invention is to provide a configuration tool for devices on networks which does not require additional equipment or specific knowledge of the addresses of the other devices.

Another object of the present invention is to provide an inspection module with a configuration tool which uses IP and a web browser to configure the bridge.

According to one aspect of the present invention, there is provided a method for locally configuring a bridge wherein a connection to a remote router or gateway is lost. The method comprises the steps of enabling a DHCP server on the bridge; choosing a temporary address for the bridge; receiving at least one DNS request from at least one user; sending at least one corresponding answer to the at least one DNS request using the temporary address; accessing the bridge with a configuration message using the temporary address; configuring the bridge using information contained in the configuration message; wherein local configuration of the bridge is made possible by giving a valid address to the bridge and enabling devices on a LAN to communicate with the bridge.

Preferably, the temporary address is a temporary IP address. Preferably, the choosing step further comprises detecting a current LAN subnet address; detecting a DNS request with a name of the bridge; locating a temporary address not used on the LAN. Preferably, the enabling step comprises detecting that the connection to the remote router or gateway is lost. Preferably, the method further comprises a step of releasing the temporary address for the bridge after a predetermined period of time.

According to another aspect of the present invention, there is provided an apparatus located within a bridge for locally configuring the bridge when a connection to a remote router or gateway is lost. The apparatus comprises a DHCP server enabled on detection that the connection to a remote router or gateway is lost; an address determiner for choosing a temporary address for the bridge; a DNS request interceptor for intercepting at least one DNS request from at least one user; an answer sender for sending at least one corresponding answer to the at least one DNS request using the temporary address; a configuration message receiver for receiving a configuration message sent to the bridge using the temporary address; a configuration manager for configuring the bridge using the configuration message; wherein local configuration of the bridge is made possible by giving a valid address to the bridge and enabling devices on a LAN to communicate with the bridge.

According to another aspect of the present invention, there is provided a method for seamlessly enabling a DHCP on a bridge when the remote side of the bridge is down. The method comprises the steps of detecting that the

remote side of the bridge is down by one of a) sniffing the LAN traffic and noticing that DNS requests and DHCP requests are not being answered to by the remote router or gateway, b) noticing that traffic going through the bridge is not being transmitted to the remote router or gateway, enabling the bridge on-board DHCP server, wherein the DHCP server is ready to be used on the LAN.

According to another aspect of the present invention, there is provided a method for configuring a bridge device locally on a LAN. The method comprises the steps of intercepting DNS request messages sent from stations on the LAN and comprising the name of the bridge device and answering the DNS request messages with the IP address of the bridge device, wherein a remote DNS request is not sent.

For the purpose of the present invention, the following terms are defined below.

The term "datagram" is intended to mean the unit of data, or packet, transmitted in a TCP/IP network. Each datagram contains source and destination addresses and data.

The terms "Ethernet address", "Hardware address" and "MAC address" are used as synonyms in the present disclosure and are intended to mean a unique number assigned to each Ethernet network adapter or device. It is a 48-bit number maintained in part by the IEEE (Institute of Electronics and Electrical Engineers). Hardware vendors obtain blocks of numbers that they can build into their cards.

The term "bridge" is intended to mean a device that connects two LAN segments together, which may be of similar or dissimilar types, such as Ethernet and Token Ring, possibly over a WAN interface.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features, aspects and advantages of the present invention will become better understood with regard to the following description and accompanying drawings wherein:

FIG. 1 illustrates a prior art system;

FIG. 2 illustrates a system according to a preferred embodiment of the present invention;

FIG. 3 illustrates steps of a method according to a preferred embodiment of the

present invention;

FIG. 4 is a flow chart of the steps of an alternate embodiment of the present invention; and

FIG. 5 is a screen shot of the configuration main menu accessible through a web browser connected to the bridge configuration manager.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring now to FIG. 1, the components of the system which can be used with the present invention are illustrated. A bridge 22 is installed on a LAN 24 between a router of an ISP 20 and at least one PC (shown here are computer 26 and computer 28). The bridge's 22 goal is to send Ethernet frames between the PC into the WAN segment of the network. Since a bridge is transparent, it is, by default, not addressable using IP.

When the service provider is not available and the user is therefore not connected to the ISP, the LAN IP address cannot be determined. The bridge's configuration and maintenance settings can therefore not be accessed through the web and with IP requests because the presence of the bridge on the LAN is not confirmed.

Referring now to FIG. 2, a system according to a preferred embodiment of the present invention is illustrated. A Local Area Network (LAN) 24 connects at least two devices, for example, at least one of computers 26 and 28 and a bridge 22. The devices on the LAN can be clients (such as personal computers, terminals, etc.), servers, etc. The bridge 22 connects the LAN to a router 20 through a Digital Subscriber Line (DSL) or Wide Area Network (WAN) line. In turn, the router 20, which preferably comprises a DHCP server, is connected to the Internet 29. Computer 26 has a specific MAC address assigned by the manufacturer and has been assigned by the remote Dynamic Host Configuration Protocol (DHCP) an IP address on the LAN. The IP address is, for example, 172.30.68.2. Computer 28 also has a personalized MAC address and has been assigned an IP address of 172.30.68.5. It is located on the same subnet as the computer 26 and therefore has a similar IP address (the first, second and third portions of the IP address are typically the same). Bridge 22 however, has been assigned an IP address during manufacturing. This IP address does not necessarily correspond to an IP address valid on the LAN. In

this case, the IP address assigned to the bridge was 192.168.1.1. This IP address is not valid on the example subnet. The router has also been assigned an IP address valid on the subnet. The address is, for example, 172.30.68.1.

A typical bridge device 22 comprises the following items: a Bridge IP Module 16 used to manage IP communications in the bridge, a Bridge's Transparent Forwarding Module 18 used to forward packets, a table of known MAC addresses 19 used to compare the destination MAC addresses to a table identifying to which port the packet is destined (if known) and a Bridge's IP address 21. Configuration Managers 15 can be added but would be accessed using a serial connection.

The bridge 22 according to a preferred embodiment of the present invention comprises Configuration Managers 15 and a Detection Module 17 which are used to, respectively, configure the bridge and detect configuration instructions on the LAN in order to configure and maintain the bridge locally.

A method of configuring the bridge has the following steps, as illustrated in FIG. 3. First, when the bridge is not connected to the ISP, the answers to DHCP requests will be delayed with respect to the typical response time of the answers to the requests. A detection module is introduced which will serve as a spy to detect the LAN IP address and then enable local configuration of the bridge using TCP/IP. When the detection module is sniffing the LAN traffic 32 coming from the user's LAN, DHCP requests from PCs are detected. If those DHCP requests have not been answered 34 because the connection is down, the next time the DHCP client will try to get an IP address, an on-board DHCP server (in bridge mode) should be enabled 36 before forwarding the DHCP request to the bridge. This will allow the DHCP server to provide a correct IP address to the PC requesting it. The length of the DHCP lease should be very short. The detection module will then detect the current LAN subnet address 38.

This detection can be done in many ways, such as 1. Sniffing ARP requests to the router and getting the IP addresses involved in the exchange, 2. Using Inverse ARP to the destination address of all non-broadcast MAC addresses, 3. Sniffing DHCP requests and responses.

Unless specified in the configuration of the detection module, it will typically forward all packets to the bridge after the detection of the current LAN subnet address is completed.

The next step will be to sniff the traffic 40, while searching for a DNS request. Upon the arrival of any DNS request, the bridge checks if the name requested matches its name 42, "myadsl.diva" for example. If it does, the bridge will locate an IP address not in use on the segment 44. In order to do so, the bridge will choose a random IP address on the local network. It will then check with the ARP if it is already taken by a device on the network. If it is not, it will be kept it as the new IP address for the bridge. If the ARP answers to the request, the bridge will choose another address until it finds a free one. The following step is to set the Bridge IP address to the borrowed address.

Then, an answer to the DNS request is sent 46 with the located address for the bridge. This is done by answering the DNS request with the local LAN IP address, therefore saying, for example, to the requesting PC: "Here's the IP address for myadsl.diva: 222.54.7.193.". From now on, the PC will use this IP address to communicate with the bridge 48. Since the bridge is now officially present on the subnet, all IP traffic will be exchanged between the bridge's IP stack and the PC, including any Web (HTTP) traffic. Then, a web configuration tool accessible through a web browser can be used to access the configuration and maintenance settings of the bridge 50.

In order to keep this method and configuration private, the module should answer ARP requests for the MAC address locally, and not let this ARP packet be bridged.

If it is ever detected that another machine on the LAN answers to the same IP address, the bridge should release the IP address that it borrowed. And, after a certain period of time, the borrowed IP address should, preferably, also be released.

If the DNS request does not match the name assigned to the bridge, the request should be bridged.

The user, preferably the network manager, only has to enter the bridge's name into a web browser in order to configure it. For example, http://myadsl.diva would be used to communicate with a bridge called myadsl.diva.

This method can also be used to configure routers using a similar approach.

Since an IP address is borrowed on the subnet, it is possible, although locally, that a PC might want to connect to this IP address. In this case, all that the PC is going to connect to is the bridge. If identification of the user, such as passwords and usernames, is required to manipulate the configuration of the bridge the PC will not be able to modify any of the settings. This possibility is however very remote because the PCs are connecting to the Internet, and not to one another. And, if the user does connect to another machine connected to the same ISP, odds are that this will not be the address borrowed by this method.

Preferably, the ISP should not be aware that this procedure is happening. Anything belonging to this configuration connection should remain private between the detection module and the PC.

FIG. 4 illustrates another method. An on-board DHCP server is enabled on the bridge when traffic is blocked at the remote side of the bridge or when the DHCP requests are not answered to. The on-board DHCP server could also be enabled when DNS requests are not being answered to. The bridge according to a preferred embodiment sniffs the traffic on the LAN 52 and detects 54 that the traffic and requests are not answered to. The on-board DHCP server is then enabled 56. This is useful when the ISP line is down or when the LAN has been cut off the remote network. The on-board DHCP could detect the LAN sub-net address.

Table 1 is a excerpt from a telnet session with a configuration manager of a bridge. The telnet session illustrates possible remote configuration instructions that can be performed on the configuration manager of the bridge.

Table 1. Telnet Session with a Configuration Manager

Welcome to Armstrong 1.9.9:000 This version is internal to Eicon Technology development group.
Copyright Eicon Technology 1999

-->SHOW BRIDGE PORTS

port	status	physical addr
B-ether-ATM-(8,35)	DOWN	(null>
WinEth-1	UP	00:00:32:78:98:12

-->SHOW BRIDGE TABLE

Station	Physical addr	Port	Type
000	00:00:32:78:98:12	-> WinEth-1	learned

```
001          00:a0:24:0c:8b:ba  -> WinEth-1     learned
002          00:b0:d8:80:00:ac  -> WinEth-1     learned

-->SHOW BRIDGE STATISTICS
Total Learned Entry Discards: 0

Port Name              IN      OUT  Discards
B-ether-ATM-(8,35)     0       0    0
WinEth-1               79      0    79

-->SHOW BRIDGE CONFIGURATION
Bridge aging time: 300(sec)

-->SHOW PROFILES
Profile                Type          State
-----------------      -------       ---------
B-ether-ATM-(8,35)     UNKNOWN       DISABLED
WinEth-1               UNKNOWN       UP

-->PROFILE B-ether-ATM-(8,35)
B-ether-ATM-(8,35)>SET
SET <keyword(s)>
Keywords valid in this context:
ADSL ATM BRIDGE DATE DHCP ILMI IP LOG PASSWORD PROFILE TIME
TIMEPROTOCOL
B-ether-ATM-(8,35)>SET ATM
SET ATM <keyword(s)>
Keywords valid in this context:
CDUT MBS MODE PCR SCR SERVICE UCI UPI
B-ether-ATM-(8,35)>SET ATM UPI 8
B-ether-ATM-(8,35)>SET ATM UCI 35
B-ether-ATM-(8,35)>1
```

Table 2 is a list of potentially available instructions in a telnet session with the configuration manager of the bridge. It will be understood that this list comprises functions which are not necessary to configure a bridge and which are used to monitor the design and management of its modules. The list could also be completed by adding other functions depending on the options of the bridge.

Table 2. List of Available Instructions

ADD DHCP STATICMAP	adds a new entry to the STATICMAP table.
DELETE DHCP STATICMAP	delete an entry from the STATICMAP table
DELETE IP ROUTE	deletes an IP route
DISABLE ADSL INTERNAL BER TESTER	disables ADSL internal BER tester
DISABLE ADSL TRELLIS CODING	disables trellis coding
DISABLE BRIDGE	disables bridge
DISABLE DHCP STATICMAP	disable support for static address assignment
DISABLE IP FORWARDING	disables IP forwarding option
DISABLE LOG MODULE	disables logging for a module

DISABLE LOG OUTPUT	disables logging to a destination
DISABLE TFTP SERVER	disable internal tftp server
DISABLE TIMEPROTOCOL	disable time protocol
ENABLE ADSL INTERNAL BER TESTER	enables ADSL internal BER tester
ENABLE ADSL TRELLIS CODING	enables trellis coding
ENABLE BRIDGE	enables bridge
ENABLE DHCP STATICMAP	enable support for static address assignment
ENABLE IP FORWARDING	enables IP forwarding option
ENABLE LOG MODULE	enables logging for a module
ENABLE LOG OUTPUT	enables logging to a destination
ENABLE TFTP SERVER	enable internal TFTP server
ENABLE TIMEPROTOCOL	enable time protocol
EXIT	closes current session
GET TFTP FILE	download a file using TFTP
SET ADSL FAST MAX BITRATE DOWN	sets/shows ADSL debug config element
SET ADSL FAST MAX BITRATE UP	sets/shows ADSL debug config element
SET ADSL FAST MIN BITRATE DOWN	sets/shows ADSL debug config element
SET ADSL FAST MIN BITRATE UP	sets/shows ADSL debug config element
SET ADSL FAST PLANNED BITRATE DOWN	sets/shows ADSL debug config element
SET ADSL FAST PLANNED BITRATE UP	sets/shows ADSL debug config element
SET ADSL INTERLEAVED MAX BITRATE DOWN	sets/shows ADSL debug config element
SET ADSL INTERLEAVED MAX BITRATE UP	sets/shows ADSL debug config element
SET ADSL INTERLEAVED MIN BITRATE DOWN	sets/shows ADSL debug config element
SET ADSL INTERLEAVED MIN BITRATE UP	sets/shows ADSL debug config element
SET ADSL INTERLEAVED PLANNED BITRATE DOWN	sets/shows ADSL debug config element
SET ADSL INTERLEAVED PLANNED BITRATE UP	sets/shows ADSL debug config element
SET ADSL MAX ADDITIONAL NOISE MARGIN DOWN	sets/shows ADSL debug config element
SET ADSL MAX ADDITIONAL NOISE MARGIN UP	sets/shows ADSL debug config element
SET ADSL MAX AGGR PWR LEVEL DOWN	sets/shows ADSL debug config element
SET ADSL MAX AGGR PWR LEVEL UP	sets/shows ADSL debug config element
SET ADSL MAX PDS DOWN	sets/shows ADSL debug config element
SET ADSL MIN NOISE MARGIN DOWN	sets/shows ADSL debug config element
SET ADSL MIN NOISE MARGIN UP	sets/shows ADSL debug config element
SET ADSL MODULATION TYPE	sets/shows ADSL modulation type
SET ADSL RADOWNSHIT INTERVAL DOWN	sets/shows ADSL debug config element
SET ADSL RADOWNSHIT INTERVAL UP	sets/shows ADSL debug config element
SET ADSL RADOWNSHIT MARGIN DOWN	sets/shows ADSL debug config element
SET ADSL RADOWNSHIT MARGIN UP	sets/shows ADSL debug config element
SET ADSL RAMODE DOWN	sets/shows ADSL RA Mode downstream
SET ADSL RAMODE UP	sets/shows ADSL RA Mode upstream
SET ADSL RARATIO DOWN	sets/shows ADSL debug config element
SET ADSL RARATIO UP	sets/shows ADSL debug config element
SET ADSL RAUPSHIT INTERVAL DOWN	sets/shows ADSL debug config element
SET ADSL RAUPSHIT INTERVAL UP	sets/shows ADSL debug config element

SET ADSL RAUPSHIT MARGIN DOWN	sets/shows ADSL debug config element
SET ADSL RAUPSHIT MARGIN UP	sets/shows ADSL debug config element
SET ADSL TARGET NOISE MARGIN DOWN	sets/shows ADSL debug config element
SET ADSL TARGET NOISE MARGIN UP	sets/shows ADSL debug config element
SET ADSL TRANSCEIVER TYPE	sets/shows ADSL transceiver type
SET ATM MODE	sets ATM mode, UNI version, ILMI version
SET BRIDGE AGINGTIME	sets bridge aging time
SET DATE	sets the internal system date
SET DHCP DNS	defines DNS addresses for DHCP serer use
SET DHCP DOMAIN	defines domain name for DHCP server use
SET DHCP IPRANGE	defines the pool of addresses for DHCP serer
SET DHCP LEASEDURATION	set the duration of DHCP leases
SET DHCP SERVERADDR	specifies main DHCP serer address
SET DHCP STATICMAP	modifies an existing entry in the STATICMAP table
SET DHCP TYPE	selects type of DHCP services provided
SET BRIDGE AGINGTIME	sets bridge aging time
SET DATE	sets the internal system date
SET DHCP DNS	defines DNS addresses for DHCP serer use
SET DHCP DOMAIN	defines domain name for DHCP server use
SET DHCP IPRANGE	defines the pool of addresses for DHCP server
SET DHCP LEASEDURATION	set the duration of DHCP leases
SET DHCP SERUERADDR	specifies main DHCP server address
SET DHCP STATICMAP	modifies an existing entry in the STATICMAP table
SET DHCP TYPE	selects type of DHCP services provided
SET DHCP WINS	defines WINS addresses for DHCP server use
SET ILMI DEVICE TYPE	sets ILMI device type
SET ILMI UNI TYPE	sets ILMI UNI type
SET ILMI UNI VERSION	sets ILMI UNI version
SET ILMI VERSION	sets ILMI version
SET LOG FILTER	sets the level of logging
SET PASSWORD	sets the password
SET TIME	sets the internal system clock
SET TIMEPROTOCOL SERVER	set address of a time server
SET TIMEPROTOCOL ZONE	set time zone difference
SHOW ADSL CONFIGURATION	shows ADSL line configuration
SHOW ADSL STATISTICS	shows current statistics for ADSL line
SHOW BRIDGE CONFIGURATION	shows bridge configuration
SHOW BRIDGE PORTS	shows ports the bridge is binded to
SHOW BRIDGE STATISTICS	shows bridge statistics
SHOW BRIDGE STATUS	shows bridge status
SHOW BRIDGE TABLE	show bridge table
SHOW DATE	displays the current system date and time
SHOW DHCP CONFIGURATION	displays the DHCP server configuration
SHOW DHCP STATICMAP	display the list of defined static DHCP addresses
SHOW DHCP STATUS	displays DHCP server status
SHOW ILMI CONFIG	shows ILMI config
SHOW IP ADDRESS	displays current IP address(es)
SHOW IP ROUTE	displays routing table contents
SHOW IP STATISTICS	Displays statistics for the IP protocol.
SHOW LOG	show recorded log messages
SHOW LOG PLUS	show recorded log and trace for specified module(s)
SHOW PROFILES	displays the settings for all profiles.
SHOW TCP STATISTICS	displays TCP statistics
SHOW TIME	displays the system date and time

SHOW TIMEPROTOCOL CONFIGURATION	display time protocol settings
SHOW TRACE	show recorded traces for specified module(s)
SHOW UDP STATISTICS	displays UDP statistics.
START TRACE	start tracing a module
STOP TRACE	stop tracing a module

In order to communicate with the configuration manager of the bridge, a web browser interface 57 is preferably used. FIG. 5 illustrates a screen shot of an example of a Configuration Main Menu 58 of such a web browser interface 57. It comprises an Overview 59 and an Administration 60 section. The Overview section 59 allows quick verification of the status 61 of the bridge (in this example, the status is "ready"). Also, the current firmware version 62 is displayed.

In the Administration section 60, links to the different aspects of the managers are listed, the aspects being accessible by clicking on the title of the aspect. In this example, the aspects are : the ATM connections 63, the System 64, the Security 65, the ADSL Connections 66, the Maintenance 68 and the Support Information 70. A "Reset" button 72 and a "Log Out" button 74 are also provided.

The ATM Configuration Menu 63, preferably allows to define the following parameters : the VCC number, the VPI, the VCI, whether the bridge is enabled and the encapsulation.

The System Parameters Menu 64 allows to define the LAN IP address, the time and date and whether spanning trees are enabled.

The Security Parameters Menu 65 allows to define the System name, the login password, whether inbound access is disabled and whether only IP traffic is allowed.

The ADSL parameters Menu 66 preferably allows to define the mode and the data path type.

The Firmware Maintenance Menu preferably allows to download the most updated version of the firmware, to save an image of the currently installed firmware to a file on the administrator's computer and to load in a firmware image onto the configuration managers.

Finally, the Configuration Maintenance Menu allows to save an image of the current configuration to a file on the administrator's computer, to restore a saved configuration and to reset the configuration to a factory default.

While the invention has been described in connection with specific embodiments thereof, it will be understood that it is capable of further modifications and this applications intended to cover any variations, uses, or adaptations of the invention following, in general, the principles of the invention and including such departures form the present disclosure as come within known or customary practice within the art to which the invention pertains and as may be applied to the essential features hereinbefore set forth, and as follows in the scope of the appended claims.

CLAIMS

1. A method for locally configuring a bridge wherein a connection to a remote router or gateway having an on-board DHCP server is lost, comprising the steps of:

enabling a DHCP server on said bridge;

choosing a temporary address for said bridge;

receiving a DNS request from a user requesting an address for said bridge using said bridge's name;

sending an answer to said DNS request using said temporary address, said answer having said temporary address for said bridge;

accessing said bridge with a configuration message using said temporary address;

configuring said bridge using information contained in said configuration message;

wherein local configuration of the bridge is made possible by giving a valid address to the bridge and enabling devices on a LAN to communicate with the bridge.

2. A method as claimed in claim 1, wherein said temporary address is a temporary IP address.

3. A method as claimed in any one of claims 1 and 2, wherein said steps of choosing further comprise:

detecting a current LAN subnet address; and

locating a temporary address not used on said LAN.

4. A method as claimed in any one of claims 1 to 3, wherein said enabling comprises detecting that said connection to said remote router or gateway is lost.

5. A method as claimed in any one of claims 1 to 4, further comprising a step of releasing said temporary address for said bridge after a predetermined period of time.

6. An apparatus located within a bridge for locally configuring said bridge when a connection to a remote router or gateway having an on-board DHCP server is lost, comprising :

a DHCP server enabled on detection that said connection to a remote router or gateway is lost;

an address determiner for choosing a temporary address for said bridge;

a DNS request interceptor for intercepting a DNS request from a user, said DNS request requesting an address for said bridge using said bridge's name;

an answer sender for sending an answer to said DNS request using said temporary address, said answer having said temporary address for said bridge;

a configuration message receiver for receiving a configuration message sent to said bridge using said temporary address;

a configuration manager for configuring said bridge using said configuration message;

wherein local configuration of the bridge is made possible by giving a valid address to the bridge and enabling devices on a LAN to communicate with the bridge.

7. An apparatus as claimed in claim 6, wherein said temporary address is a temporary IP address.

8. An apparatus as claimed in any one of claims 6 to 7, wherein said address determiner detects a current LAN subnet address and locates a temporary address not used on said LAN.

9. An apparatus as claimed in any one of claims 6 to 8, further comprising a lost connection detector for detecting that said connection to said remote router or gateway is lost.

10. An apparatus as claimed in any one of claims 6 to 9, further comprising an address releaser for releasing said temporary address for said bridge after a predetermined period of time.

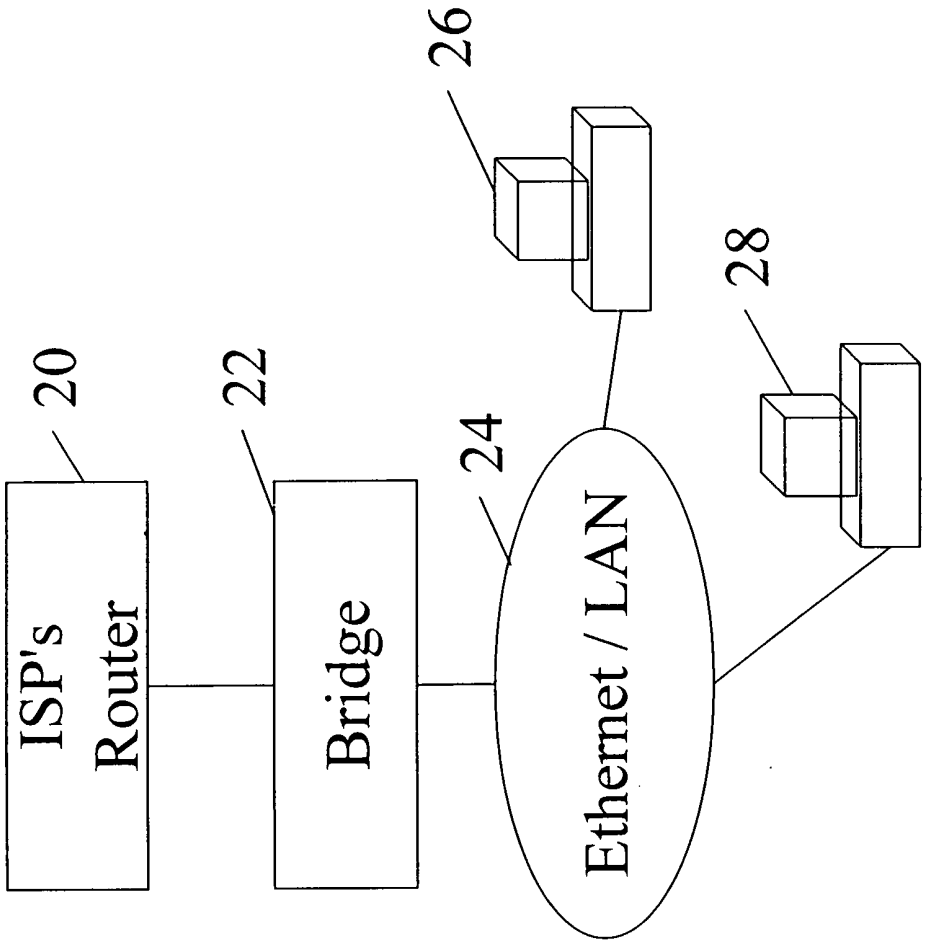

Fig. 1 (Prior Art)

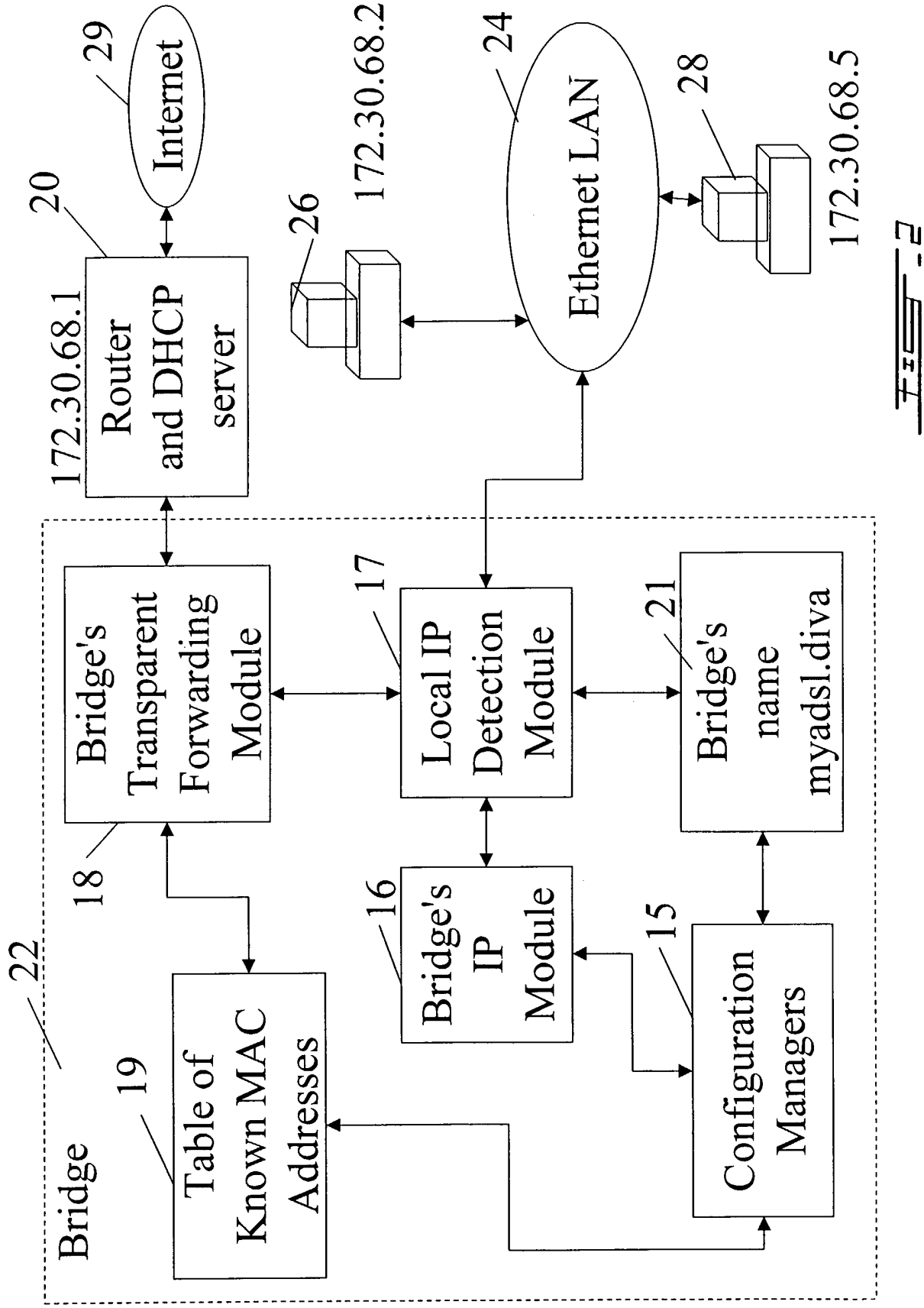
Internet
29
20
172.30.68.1
Router and DHCP server
26
172.30.68.2
24
Ethernet LAN
28
172.30.68.5
Bridge
22
Bridge's Transparent Forwarding Module
18
Local IP Detection Module
17
Bridge's name myadsl.diva
21
Table of Known MAC Addresses
19
Bridge's IP Module
16
Configuration Managers
15

Fig. 2

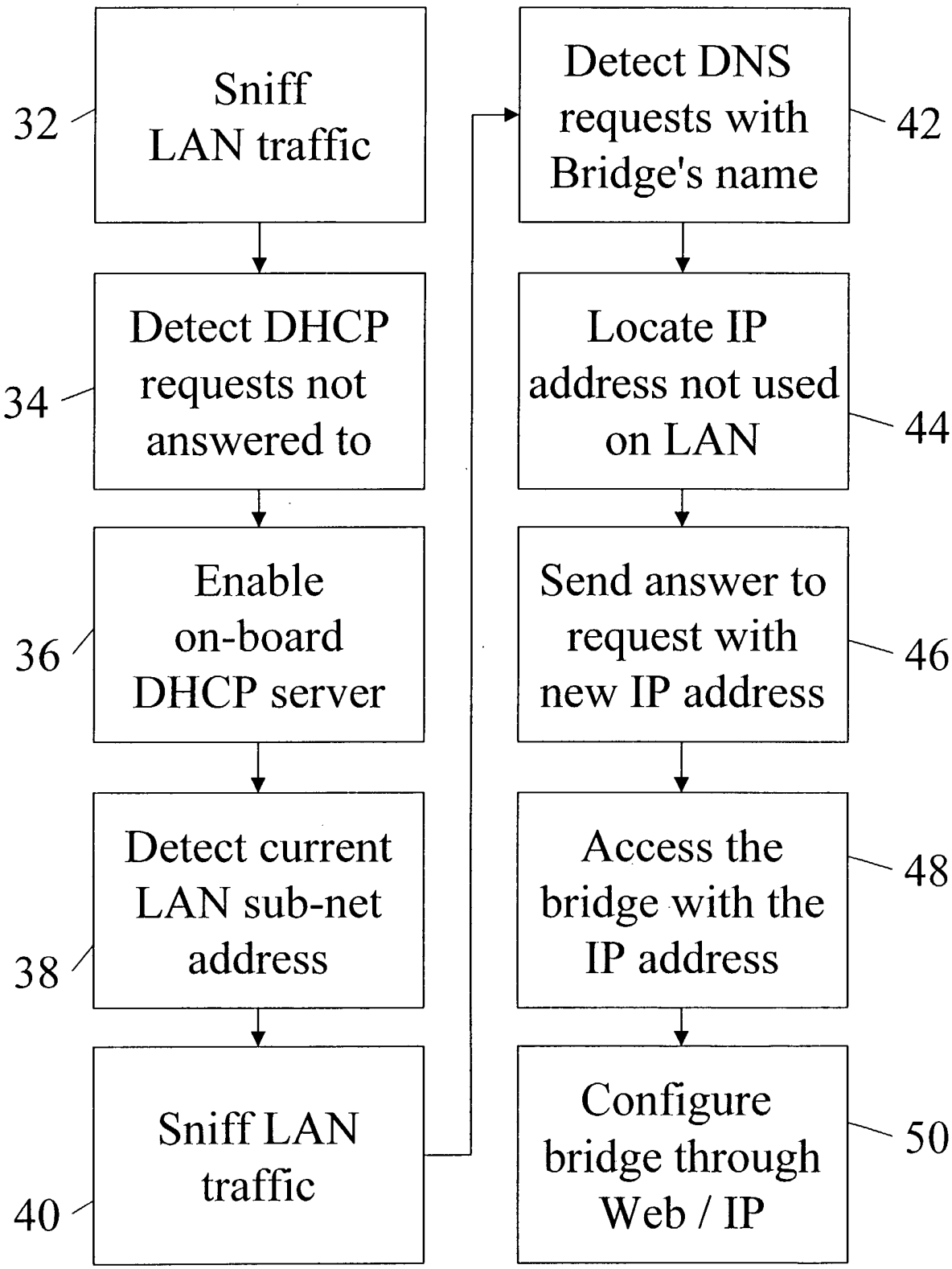
Sniff LAN traffic
32
Detect DHCP requests not answered to
34
Enable on-board DHCP server
36
Detect current LAN sub-net address
38
Sniff LAN traffic
40
Detect DNS requests with Bridge's name
42
Locate IP address not used on LAN
44
Send answer to request with new IP address
46
Access the bridge with the IP address
48
Configure bridge through Web / IP
50

FIG. 3

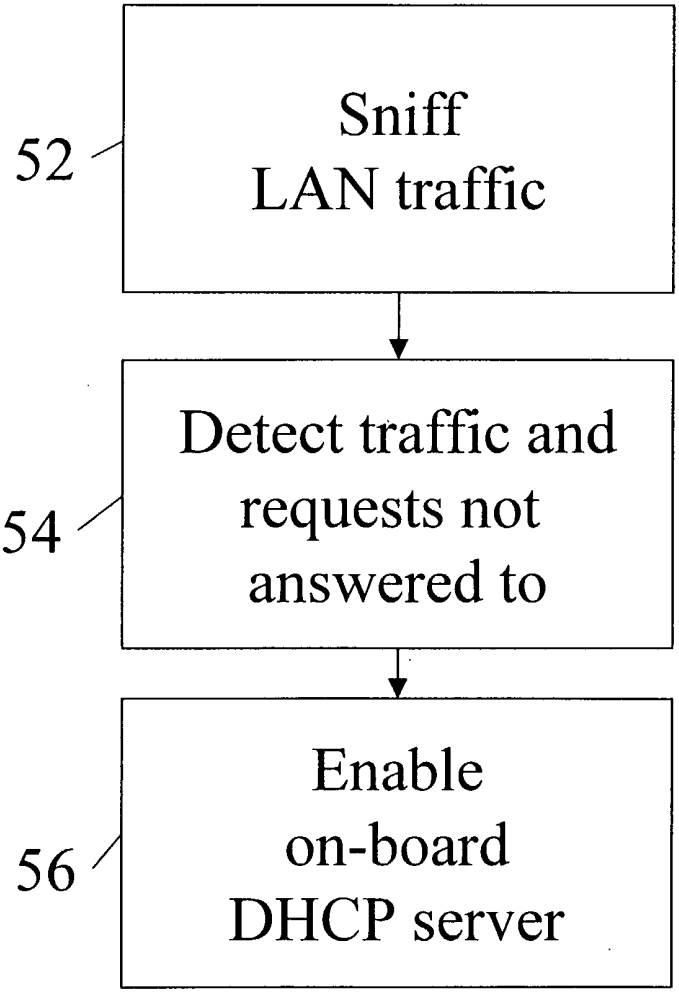
52
Sniff
LAN traffic
54
Detect traffic and
requests not
answered to
56
Enable
on-board
DHCP server

Fig. 4

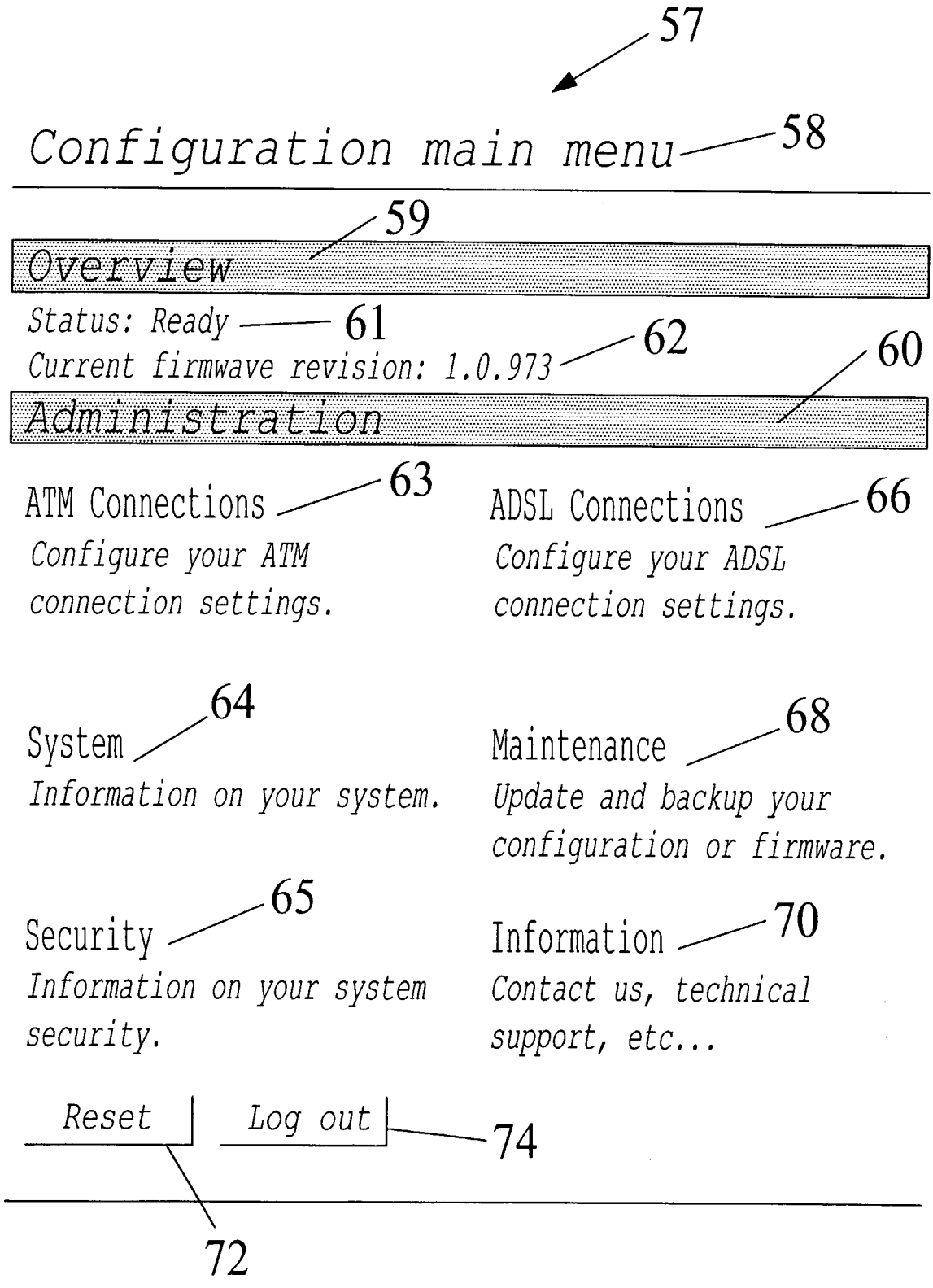
57
Configuration main menu
58
59
Overview
Status: Ready
61
Current firmwave revision: 1.0.973
62
60
Administration
ATM Connections
63
Configure your ATM connection settings.
ADSL Connections
66
Configure your ADSL connection settings.
System
64
Information on your system.
Maintenance
68
Update and backup your configuration or firmware.
Security
65
Information on your system security.
Information
70
Contact us, technical support, etc...
Reset
Log out
74
72

Fig. 5