OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

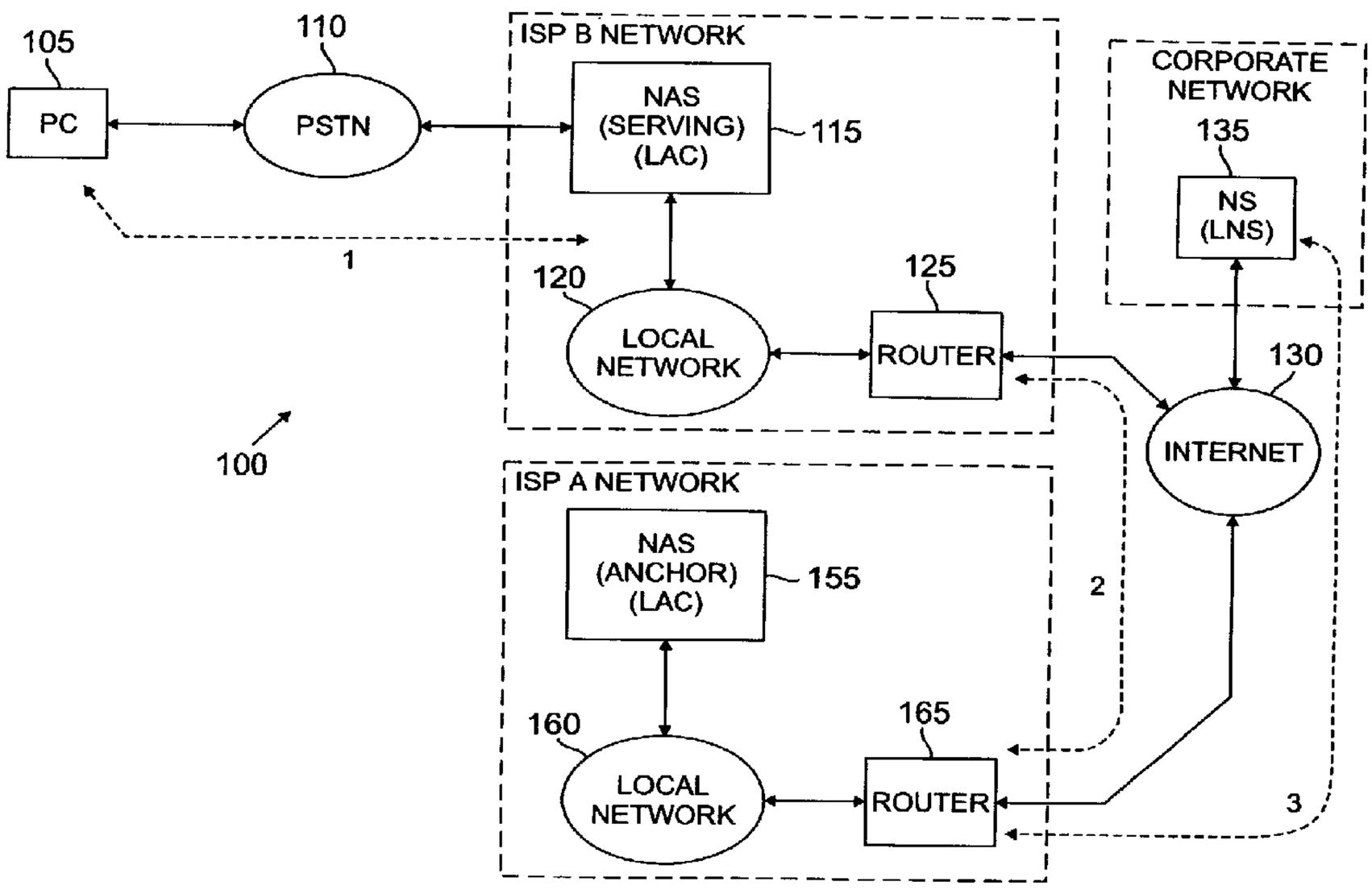
(12) (19) (CA) **Demande-Application**

(21) (A1) **2,279,667**
(22) 1999/08/05
(43) 2000/03/09

(72) CHUAH, MOOI C., US
(72) RAI, GIRISH, US
(71) LUCENT TECHNOLOGIES INC., US

(51) Int.Cl.[6] H04L 12/56
(30) 1998/09/09 (09/150,403) US

(54) **PROTOCOLE POINT A POINT MOBILE**
(54) **A MOBILE POINT-TO-POINT PROTOCOL**



(57) Apparatus for transferring packet data incorporates a "hand-off feature that allows the transfer of an existing PPP connection from one packet server to another packet server. Such a hand-off control message or call continue transaction can be initiated by any of the servers involved in the transactions. For instance, assume an initial arrangement where a point-to-point call is set up and in progress between a user and a private network via a first packet server (e.g., a first Serving LAC) and a second packet server (e.g., an Anchor LAC). If, for example, the user moves out of the region served by the first packet server into a region served by a third packet server (e.g., a second Serving LAC), then a hand-off control message transaction, according to the invention, is initiated. Either the second Serving LAC or the Anchor LAC may initiate the call continue transaction. Alternatively, radius servers respectively associated with the packet servers may be employed to perform the call continue transaction. Furthermore, assuming that a communication path is not yet established between the second packet server (e.g., Anchor LAC) and the third packet server (e.g., the second Serving LAC), a communication path (e.g., tunnel) set-up control message transaction may be performed concurrent with the call continue transaction. Still further, at least one packet server (e.g., the Anchor LAC) monitors state variables associated with the packet servers (e.g., the second Serving LAC and the private network) from which it receives packet data.

Chuah 18-14

A Mobile Point-to-Point Protocol

Abstract

Apparatus for transferring packet data incorporates a "hand-off" feature that allows the transfer of an existing PPP connection from one packet server to another packet server. Such a hand-off control message or call continue transaction can be initiated by any of the servers involved in the transactions. For instance, assume an initial arrangement where a point-to-point call is set up and in progress between a user and a private network via a first packet server (e.g., a first Serving LAC) and a second packet server (e.g., an Anchor LAC). If, for example, the user moves out of the region served by the first packet server into a region served by a third packet server (e.g., a second Serving LAC), then a hand-off control message transaction, according to the invention, is initiated. Either the second Serving LAC or the Anchor LAC may initiate the call continue transaction. Alternatively, radius servers respectively associated with the packet servers may be employed to perform the call continue transaction. Furthermore, assuming that a communication path is not yet established between the second packet server (e.g., Anchor LAC) and the third packet server (e.g., the second Serving LAC), a communication path (e.g., tunnel) set-up control message transaction may be performed concurrent with the call continue transaction. Still further, at least one packet server (e.g., the Anchor LAC) monitors state variables associated with the packet servers (e.g., the second Serving LAC and the private network) from which it receives packet data.

A Mobile Point-to-Point Protocol

Cross-Reference to Related Applications

This application is a continuation-in-part of copending U.S. Patent Application Serial No. 09/074,582, filed on May 8, 1998.

Field of the Invention

This invention relates generally to communications and, more particularly, to packet communications systems.

Background of the Invention

One use of the Internet as a communications vehicle is as an enhanced data back-bone for coupling together workgroups to provide what is referred to as a "virtual private network" (VPN). One application of a VPN is in a corporate environment such that employees, e.g., at home, can remotely access, via the Internet, corporate data networks. A VPN provides security, and authentication, for a remote user to join a closed user group notwithstanding the use of public facilities. In effect, the use of a VPN provides a WAN-like vehicle to the corporation and its employees. (Although the corporate network could also provide direct remote access, e.g., a user dials directly into the corporate network, there are economic advantages to the use of a VPN.)

To provide a VPN, tunneling protocols are used such as the "Point-to-Point Tunneling protocol" (PPTP) and the "Layer 2 Forwarding" (L2F) protocol. Generally speaking, a tunnel protocol enables the creation of a private data stream via a public network by placing one packet inside of another. In the context of a VPN, an IP packet is placed inside another IP packet. In an attempt to develop an industry standard, the Internet Engineering Task Force (IETF) is developing the "Layer 2 Tunneling Protocol" (L2TP), which is a hybrid of the PPTP and L2F protocols (e.g., see K. Hamzeh, T. Kolar, M. Littlewood, G. Singh Pall, J.Taarud, A. J. Valencia, W. Verthein; *Layer Two*

Tunneling Protocol "L2TP"; Internet draft, March, 1998).

For a remote user, a typical form of access to a VPN is via a "plain-old-telephone service" (POTS) connection to an "Internet service provider" (ISP) that provides the VPN service. For example, a user incorporates an analog modem into a personal computer, or equivalent, and has a customer account with a particular ISP, referred to herein as the "home" ISP. (It is also assumed that the user's personal computer is properly configured to support one of the above-mentioned tunneling protocols.) The user accesses the VPN by simply making a data call to the home ISP, e.g., dialing a telephone number associated with the "home" ISP and then "logging in" to the VPN.

Summary of the Invention

Access to an ISP is via a network access server (NAS). We have realized that in a Personal Communications Service (PCS) wireless environment the above-described tunneling protocols do not allow a remote user, on an existing call, to change the NAS that is providing access to a VPN. As such, the user's physical mobility may disconnect, or drop, the user from the existing VPN connection.

Therefore, and in accordance with one aspect of the invention, apparatus and methods for transferring packet data provide a "hand-off" feature that allows an existing point-to-point (PPP) connection to be transferred from one packet server to another packet server.

In an embodiment of the invention, three new hand-off control messages are defined for use with the packet servers, namely: (i) Continued Call Request, (ii) Continued Call Reply, and (iii) Continued Call Connect. These three new control messages comprise a L2TP control message header, message identifier (e.g., continued call request, etc.), and a number of fields. As a result, the user does not have to terminate the current PPP connection and then re-establish a new PPP connection.

Advantageously, such a hand-off control message or call continue transaction

can be initiated by any of the servers involved in the hand-off scenario. For instance, assume an initial arrangement where a point-to-point call is set up and in progress between a user and a private network via a first packet server (e.g., a first Serving LAC) and a second packet server (e.g., an Anchor LAC). If, for example, the user moves out of the region served by the first packet server into a region served by a third packet server (e.g., a second Serving LAC), then a hand-off control message transaction, according to the invention, is initiated. In accordance with the invention, the second Serving LAC may initiate the call continue transaction or the Anchor LAC may initiate the call continue transaction. Alternatively, in accordance with another aspect of the invention, radius servers respectively associated with the packet servers may be employed to perform the call continue transaction.

In another aspect of the invention, assuming that a communication path is not yet established between the second packet server (e.g., Anchor LAC) and the third packet server (e.g., the second Serving LAC), a communication path (e.g., tunnel) set-up control message transaction may be performed concurrent with the call continue transaction.

Further, in yet another aspect of the invention, at least one packet server (e.g., the Anchor LAC) monitors state variables associated with the packet servers (e.g., the second Serving LAC and the private network) from which it receives packet data.

Brief Description of the Drawing

FIG. 1 shows a communications system in accordance with the principles of the invention;

FIGs. 2 - 3 show flow charts of illustrative methods for use in the communications system of FIG. 1;

FIG. 4 shows an illustrative multi-hop message flow;

FIGs. 5 - 7 show illustrative control message transactions;

FIG. 8 shows another embodiment of a communications system in accordance with the principles of the invention;

FIG. 9 shows an illustrative hand-off message flow;

FIG. 10 shows a flow chart of an illustrative method for use in the communications system of FIG. 8;

FIG. 11 shows illustrative control message transactions;

FIG. 12 shows another embodiment of a communications system in accordance with the principles of the invention;

FIG. 13 shows an illustrative hand-off message flow;

FIG. 14 shows a flow chart of an illustrative method for use in the communications system of FIG. 12;

FIG. 15 shows illustrative control message transactions;

FIG. 16 shows an illustrative high level block diagram of Network Access Server; and

FIGs. 17 - 18 show illustrative control message transactions for outgoing calls.

FIG. 19 shows alternative illustrative control message transactions;

FIG. 20 shows further alternative illustrative control message transacations;

FIG. 21 shows still futher alternative illustrative control message transactions;

FIG. 22 shows an embodiment employing radius servers for performing a control message transaction; and

FIG . 23 shows another embodiment employing radius servers for performing a control message transaction.

Detailed Description

It is to be appreciated that, for ease of reference, the following detailed description is divided into three topical sections: multi-hop point-to-point protocol; mobile point-to-point protocol; and payload message overviews and congestion control for mL2TP.

Multi-Hop Point-to-Point Protocol

FIG. 1 shows an illustrative communications system 100 in accordance with the principles of the invention. Other than the inventive concept, the elements are well-known and will not be described in detail. For example, personal computer (PC) 110 includes data communications equipment (not shown) for dial-up access through public-switched-network (PSTN) 110 to ISP B for establishing an Internet connection. Likewise, the solid lines between elements of communications system 100 are representative of well-known communications facilities between the respective endpoints, e.g., the connection between PC 110 and PSTN 110 is representative of a local loop connection, the connection between ISP B and Internet 120 is supported by asynchronous transfer mode (ATM) over a synchronous optical network (SONET), etc. Further, its assumed that the reader is familiar with the above-mentioned L2TP protocol.

As can be observed from FIG. 1, communications system 100 comprises two ISPs: ISP A, represented by ISP A Network, and ISP B, represented by ISP B Network. The ISP B Network comprises Network Access Server (NAS) 115, which includes a point-of-presence (POP) router (not shown) as known in the art, a local network 120, and a router 125. Similarly, the ISP A Network comprises NAS 155, a local network 160, and a router 165. It is assumed that ISP A provides a VPN service for remotely located employees to access an illustrative Corporate Network via Network Server (NS) 135, which provides, among other functions, a routing and firewall capability. (The Corporate network is assumed to be, e.g., a collection of local area networks (not shown) suitably protected behind NS 135.

We have observed that a remote user may, even if only temporarily, be located in a portion of the country that is not served by ISP A but is, instead, served by ISP B. Further, ISP A may desire to extend such VPN coverage to other areas. Therefore, and in accordance with the principles of the invention, a remote user is allowed to access a VPN via a visiting, or serving, ISP in addition to their home, or anchor, ISP. (Although it is assumed that ISP A and ISP B are different service providers, this is not necessary to the inventive concept, e.g., they could just be separate networks within an ISP.) Thus, a user (not shown) located at PC 105 can access the corporate network while, e.g., roaming, about the country.

At this point, the following definitions are assumed:

mL2TP - the L2TP protocol as defined in K. Hamzeh, T. Kolar, M. Littlewood, G. Singh Pall, J.Taarud, A. J. Valencia, W. Verthein; *Layer Two Tunneling Protocol "L2TP"*; Internet draft, March, 1998; *plus modifications as described herein*;.

LAC - mL2TP Access Control, i.e., an NAS that supports mL2TP;

LNS - a NS that supports mL2TP;

Anchor LAC - a LAC that supports tunneling to the LNS for providing a VPN Service; and

Serving LAC - a LAC that supports tunneling to the Anchor LAC.

These definitions are used to simplify an illustrative description of the inventive concept. As such, and as those in the art will realize, the inventive concept is not so limited and can be applied to any tunneling protocol and associated processing equipment.

In accordance with the inventive concept, the ISP A network illustrates an Anchor LAC 155 and the ISP B network illustrates a Serving LAC 115. As described further below, and in accordance with the principles of the invention, communications

system 100 of FIG. 1 provides a multi-hop tunnel. The example of FIG. 1 illustrates a two-hop tunnel. One hop is from the ISP B Network to the ISP A Network and the other hop is from the ISP A Network to the Corporate Network.

Reference should now be made to FIG. 2, which shows an illustrative high-level flow chart of a method in accordance with the principles of the invention. (It is presumed that Serving LAC 115 and the other respective servers are suitably programmed to carry out the below-described methods using conventional programming techniques, which, as such, will not be described herein.) In step 205, the remote user initiates a PPP (Point-to-Point Protocol) connection to ISP B via PSTN 110. In step 210, Serving LAC 115 partially authenticates the user (e.g., using a predefined "username" and "password") and accepts the connection (represented by dotted line 1 of FIG. 1). (Alternatively, DNIS (dialed number identification service), CLID (calling line identification), or other equivalent forms of identification could be used.) Obviously, if Serving LAC 115 can not authenticate the user, the connection is not accepted (this step is not shown).

As background, and as known in the art, when a remote user wishes to establish a new PPP session, PC 110 initiates a PPP LCP (Link Control Protocol) Config Request to the Serving LAC. The Serving LAC completes both the PPP LCP and PPP PAP/CHAP phases, as known in the art, with the user's equipment before initiating any communication with the Anchor LAC in accordance with the inventive concept. (For secure Conduits, the IETF has defined two protocols for security over PPP connections - the Password Authentication Protocol (PAP) and the Challenge-Handshake Authentication Protocol (CHAP) (e.g., see IETF Request for Comment (RFC) 1334, "*PPP Authentication Protocols*").

In step 215, Serving LAC 115 determines is the remote user desires to use a VPN service. This selection could, e.g., be directly associated with particular "usernames" and/or be associated with a separate request from the user, e.g., via a pop-up "HyperText Transport Protocol" (http) form provided by Serving LAC 115.) If the remote user does not request a virtual dial-up service, Serving LAC 115 provides

standard Internet access is step 220. However, if the remote user desires to use a VPN, then Serving LAC 115 identifies as associated Anchor LAC in step 225 (described below).

Serving LAC 115 stores a VPN table that *a priori* associates, e.g., a user's identification with a particular Anchor LAC. A portion of such a table is shown below in Table One. In this example, the remote user associated with PC 110 is associated with Anchor LAC ISPA.com, i.e., Anchor LAC 155.

Table 1

User Identification	Anchor LAC
username	ISPA.com

It should be noted that equivalent structures, or operations, could be used, such as simply maintaining a list of fields formatted as "username@ISPA.com," where the portion after the "@" symbol indicates the Anchor LAC. Alternatively, ISP B may maintain a database mapping users to services. In the case of a virtual-dial-up, i.e., an identification of the remote user as being associated with a VPN service, the mapping further identifies the Anchor LAC. Alternatively, the Serving LAC can utilize a Radius Access Request/Response transaction with its local Radius Server for this task, as known in the art.

In step 230, Serving LAC 115 checks to see if a tunnel exists between itself and Anchor LAC 155. As such, Serving LAC 115 maintains a table, as illustrated in Table Two, below, of current tunnels, represented by a tunnel identification (Tid) value, associated call identifiers (Cid) of calls currently using that tunnel, and the associated Anchor LAC IP address.

Table 2

Tid	*Cid*	*Anchor LAC IP Address*
2	5	h.j.k.l

If no tunnel connection currently exists between the Serving LAC and the Anchor LAC, then a tunnel is initiated by Serving LAC 115 to the Anchor LAC in step 235 (described below). Once a tunnel exists between the Serving LAC and the Anchor LAC, Serving LAC 115, in step 240, allocates a new Cid, updates Table Two, and initiates a session with Anchor LAC 155 by forwarding a VPN request to Anchor LAC 155 via local network 120, router 125, Internet 130, router 165, and local network 160 (described further below). In this request, Serving LAC 115 conveys user identification information to Anchor LAC 155.

Turning now to FIG. 3, Anchor LAC 155 receives the request in step 305. In step 310, Anchor LAC 155 also performs authentication of the remote user (e.g., using a predefined "username" and "password" as noted above) and accepts the connection (represented by dotted line 2 of FIG. 1). (Alternatively, like the Serving LAC, DNIS, CLID, or other equivalent forms of identification could be used.) If Anchor LAC 155 can not authenticate the user, the connection is not accepted (this step is not shown). In this case, Serving LAC 115 similarly must convey an error message back to the remote user (not shown).

Anchor LAC 155 stores a VPN table that *a priori* associates, e.g., a user's identification with a particular LNS. A portion of such a table is shown below in Table Three. In this example, the remote user associated with PC 110 is associated with LNS 135, represented by IP address g.h.i.j.

Table 3

User Identification	LNS
username	g.h.i.j

Similar to Serving LAC 115, it should be noted that equivalent structures, or operations, could be used. For example, the Anchor LAC may also perform this function via Radius Access Request/Response messages with a Home Radius Server. In step 315, Anchor LAC 155 checks if this is a valid VPN request using Table Three. If

this is not a valid request, Anchor LAC 155 denies the request in step 320. If this is a valid request, Anchor LAC 155 identifies the associated LNS from Table Three in step 325.

It is assumed that the Anchor LAC maintains the following connection table for each direction of communication for each established VPN session with a remote user:

Table 4

Connection #	*Serving LAC*		*Serving LAC IP Address*	*LNS*		*LNS IP Address*	*User Assigned IP Address*
	Tid	*Cid*		*Tid*	*Cid*		
5	2	5	d.e.f.g	1	3	g.h.i.j	a.b.c.d

Anchor LAC associates with each VPN session a connection number. In addition, this connection number is mapped to the respective user. This table lists, by connection number, the Serving LAC IP Address (with associated tunnel ID and Call ID values for that hop), and the associated LNS IP Address (with associated tunnel ID and Call ID values for that associated hop). In step 330, Anchor LAC 155 establishes the VPN session (performs an authentication check, etc.). (Again, if LNS 135 should deny the VPN request (e.g., because of no authentication of the remote user or no capacity), appropriate error messages are generated by the Anchor LAC and the Serving LAC.) Other than the inventive concept, the VPN session with LNS 135 is established as in the prior art. For example, and in accordance with the principles of the invention, in establishing a new VPN session Anchor LAC 155 allocates a new Cid and updates Table 4, e.g., adds a new connection. This last connection is represented by dotted line 3 of FIG. 1.

At this point, the connectivity is a point-to-point PPP session whose endpoints are the remote user's networking application on one end, as represented by PC 105, and the termination of this connectivity into LNS 135 PPP support on the other. It should be noted that accounting, if necessary, can be performed at the Serving LAC, the Anchor

LAC, as well as the LNS, i.e., each element may count packets, octets and connection start and stop times.

In support of the above-described multi-hop virtual dial up service, a form of the L2TP (mL2TP) protocol is used and described further below. As in L2TP, there are two parallel components of mL2TP operating over a given tunnel: control messages between each LAC-LNS pair, and payload packets between the same LAC-LNS pair. The latter are used to transport mL2TP encapsulated PPP packets for user sessions between the LAC-LNS pair. As in L2TP, the *Nr* (Next Received) and *Ns* (Next Sent) fields are always present in control messages and are optionally present in payload packets. The control messages and payload messages use different sequence number states. For the above-mentioned LAC/LNS pair scenario, there are no changes to the L2TP draft protocol definition as far as the maintenance and usage of (*Nr*, *Ns*) is concerned.

However, as between the connection between the Serving LAC and the Anchor LAC, the Anchor LAC merely monitors the (*Nr*, *Ns*) values sent by the Serving LAC. That is, and in accordance with the inventive concept, the Anchor LAC simply re-transmits the values received from the Serving LAC to the LNS. In addition, the Anchor LAC now updates its (State Received, State Sent) values (*Sr*, *Ss*), with the corresponding (*Nr*, *Ns*) values it has observed from the packets sent by the Serving LAC. Since there will, undoubtedly, be packet losses between the Serving LAC and the Anchor LAC, the *Ss* (*Sr*) value at the Anchor LAC may be smaller (smaller) than the *Ss* (*Sr*) value at the Serving LAC. In addition, the Anchor LAC maintains two sets of (*Sr*, *Ss*) variables, one for the Serving LAC/Anchor LAC control connection and the other for the Anchor LAC/LNS control connection.

Before PPP tunneling can occur, in accordance with the inventive concept, between the Serving LAC, the Anchor LAC, and the LNS, control messages must be exchanged between them. Control messages are exchanged over the same tunnel which will be subsequently used to forward payload data once mL2TP call control and management information have been passed (described below).

In accordance with the inventive concept, additional Attribute Value Pairs (AVP)s (described below) are defined for use in the L2TP control messages (hence becoming mL2TP control messages). These additional AVPs are for supporting the multi-hop features and call transfer features described above. As defined in L2TP, AVPs are used to further specify control signaling.

As noted above, for the above-described LAC/LNS pair case, there is no change to the procedure described in the above-mentioned L2TP draft. As such, only the multi-hop case, requires additional procedures, described below.

An illustrative multi-hop message flow is shown in FIG. 4. As can be observed from FIG. 4, a tunnel (identified by a Tid value) and a call (identified by a Cid value) are established between the Serving LAC and the Anchor LAC. Similarly, a tunnel and a call are established between the Anchor LAC and the LNS. As shown in FIG. 4, the inventive concept requires the Serving LAC establish a tunnel to the Anchor LAC. In the context of this invention, the Serving LAC treats the Anchor LAC as an LNS and L2TP procedures are used to initially set up the tunnel.

Once a tunnel has been established, a number of control message transactions occur in order to set up a PPP session in accordance with the principles of the invention. These are illustrated in FIGs. 5 - 7. In these FIGs., only the relevant fields are shown for the various control messages. Note, if the tunnel-id and call-id for the tunnel between the Serving LAC and the Anchor LAC are different from those values for the tunnel between the Anchor LAC and LNS, the Anchor LAC modifies the relevant fields in the packet headers before relaying them in either direction.

As shown in FIG. 5, the Serving LAC first sends a Start-Control-Connect-Request Message (SCCRQ) message (as defined in L2TP) to the Anchor LAC to configure the tunnel between them. Upon receipt of this message, the Anchor LAC then responds with an Start-Control-Connect-Reply Message (SCCRP) (this occurs subsequent to any above-described authentication). The Serving LAC confirms with a Start-Control-Connection-Connect (SCCCN) message to the Anchor LAC.

Following the start control connection message exchanges shown in FIG. 5, the Serving LAC sends an Incoming-Call-Request (ICRQ) message to the Anchor LAC as shown in FIG. 6. The Incoming-Call-Request message contains sufficient user data and credentials to enable the Anchor LAC to identify the LNS.

As noted earlier, if no tunnel exists between the Anchor LAC and the LNS, the Anchor LAC first initiates the SCCR, SCCRP, SCCCN message exchanges with the LNS as defined in L2TP. Once the tunnel exists, an unused slot within the tunnel, a Cid, is allocated by the Anchor LAC. At this point, and in accordance with the principles of the invention, the Anchor LAC relays the ICRQ message (from the Serving LAC) to notify the LNS of this new dial-up session. As shown in FIG. 6 the Anchor LAC modifies the ICRQ message accordingly before relaying it to the LNS. The modified fields are indicated by a "*", e.g., the assigned call ID. The Anchor LAC also adds a hidden AVP to inform LNS what receive window size it can support. (Note that with the additional hop, the Anchor LAC records the maximum window size negotiated for both the control/payload connections. Also, the window size for the control connection between the Serving LAC and Anchor LAC may be different from that of the control connection between the Anchor LAC and LNS and buffering may be required. To eliminate additional buffering and sequence number monitoring, the Anchor LAC optionally adds an AVP to inform the LNS what receive window size for the payload session the Anchor LAC can support in the Anchor LAC-Serving LAC direction. As a result, the LNS will include only appropriate receive window size values in its ICRP reply and hence only one window size for the payload session in the LNS-Anchor LAC-Serving LAC direction.

As noted earlier, the LNS either accepts the connection or rejects it. Rejections MUST include a result condition and MAY include an error indication. In either case, the LNS sends an Incoming-Call-Reply (ICRP) message to the Anchor LAC as shown in FIG. 6. The Anchor LAC then modifies the ICRP message appropriately and relays it to the Serving LAC in accordance with the invention (again, modified fields are indicated by an "*" in FIG. 6). Since the packet processing delay (PPD) field received from the LNS only includes the processing delay at the LNS, the Anchor LAC add to

this value the processing delay at its own node. Then, the ICRQ message is relayed to the Serving LAC.

In response, the Serving LAC sends an Incoming-Call-Connected (ICCN) message to the Anchor LAC as shown in FIG. 7. Inside this message, the Serving LAC passes all the LCP Config Request information as well as the Proxy Authentication Information. That is, the Serving LAC is forwarding the results of the LCP Config Request/Ack, PPP PAP/CHAP performed with the user's equipment. The Anchor LAC modifies the PPD field of the received ICCN message before relaying it to the LNS. Currently, no use is made the tx connect speed and rx connect speed.) Although not shown, and in accordance with the invention, the Anchor LAC also relays all the Set-Link-Info, Hello and Wan-Error-Notify messages defined in L2TP. (It should be observed that the description above illustrates the concept of multi-hop packet tunnel. For example, FIG. 1 represents a 2-hop packet tunnel.

It should be observed that the multi-hop mL2TP tunnels described above occur exclusively at the frame layer. As such, actual policies of address management by the LNS are irrelevant to the above-described Virtual dial-up service since, for all purposes of the PPP protocol handling, the remote user appears to have connected at the LNS.

Mobile Point-to-Point Protocol

Turning now to FIG. 8, another embodiment of the inventive concept is shown. FIG. 8 is similar to FIG. 1. Other than the inventive concept, the elements are well-known and will not be described in detail. Like numbers indicate like functions and will not be further described except where necessary.

In FIG. 8, PC 805 includes data communications equipment (not shown) for establishing wireless access through Personal Communications Service (PCS) wireless network 810 to the Internet. PCS Wireless services are known in the art and will not be described in detail. PCS wireless network 810 comprises a plurality of mobile switching centers as represented by elements 815 and 820. Each switching center

serves a geographical area (not shown). It is assumed that elements 815 and 820 include an NAS, e.g., Serving LACs similar to Serving LAC 115 of FIG. 1. Initially, it is assumed that the remote user establishes a VPN session to the corporate network using the above-described multi-hop technique. In particular, the remote user is in a geographical area such that this initial connection is routed through element 815 via connections 814 and 816. In the context of a wireless PCS application, the initial PPP connection is between element 815 and PC 805. Although shown as a part of the switching elements for simplicity, the NAS functions could also be performed in separate pieces of equipment. Similarly, the other elements such as a local network and router are not shown for simplicity.

We have realized that in a wireless environment tunneling protocols, such as L2TP, do not allow a remote user to change the existing PPP connection from one switching element to another. For example, assuming for the moment that FIG. 8 does not embody the inventive concept, when the remote user roams, e.g., to a geographical area served by element 820 (and hence a different NAS) the user's communication session is handed-off to element 820 as known in the art. However, the existing PPP connection — and hence the VPN session — is dropped and must be re-established since, as noted, there is no ability to transfer existing PPP connections from one NAS to another. In this context, the communications system of FIG. 8 overcomes this problem.

Therefore, and in accordance with the invention, an NAS or LAC incorporates a "hand-off" feature that allows the existing NAS to hand-off an existing PPP connection to another NAS. In accordance with this feature, 3 new control messages are defined, namely: (i) Continued Call Request, (ii) Continued Call Reply, and (iii) Continued Call Connect. As a result of the above, the user does not have to terminate the current PPP connection and then re-establish a new PPP connection. These 3 new control messages comprise a L2TP control message header, message identifier (e.g., continued call request, etc.), and a number of fields (described below).

In accordance with the inventive concept, an illustrative hand-off message flow is shown in FIG. 9. As can be observed from FIG. 9, a tunnel (identified by a Tid

value) and a call (identified by a Cid value) are initially established between element 815, which includes a Serving LAC, and the Anchor LAC. Similarly, a tunnel and a call are established between the Anchor LAC and the LNS. (A method for establishing this initial VPN session was described above.) As shown in FIG. 9, the inventive concept allows the existing Serving LAC to transfer the existing PPP connection to a new Serving LAC, as represented by element 820.

Reference should now be made to FIG. 10, which is an illustrative flow chart of a method for use in providing a "hand-off feature." As noted, it is assumed that a VPN session exists between PC 805 and the Corporate network via element 815, which includes a Serving LAC, and Anchor LAC 155. In accordance with the inventive concept, PCS wireless network 810 adds to the existing call state variables additional variables indicating the presence (or lack thereof) of a PPP connection for each wireless call, and if a PPP connection exists, PPP connection information that includes the Anchor LAC identification, e.g., the IP address of the Anchor LAC.

In step 405 of FIG. 10, PCS wireless network 810 detects the need for a hand-off because PC 805 has moved from the geographical area served by element 815 to another geographical area, e.g., the area served by element 820, which includes another Serving LAC. In step 410, PCS Wireless system provides element 820 with notification of the impending hand-off. (The method(s) used by a wireless system to detect and prosecute a hand-off are known in the art and not relevant to the inventive concept. As such, they will not be described herein and are represented by signaling path 811 of FIG. 8.) Since the call state information now includes a PPP session indicator and PPP call information, the new Serving LAC (of element 820) identifies the Anchor LAC in step 415. In step 420, the new Serving LAC (of element 820) checks to see if there is an existing tunnel between itself and the identified Anchor LAC, here Anchor LAC 155.

If no tunnel exists, the new Serving LAC first establishes a tunnel (as described earlier) in step 425. Then, and in accordance with the inventive concept, the new Serving LAC sends a Continued-Call-Request (CCRQ) message to the Anchor LAC in

step 430. This CCRQ message includes the user's name associated with the existing PPP connection, the Tid and Cid values to be used for the transferred (new) PPP session.

In step 435, the Anchor LAC recovers the user's name from the received CCRQ message and uses this information to determine the LNS and IP address of the old Serving LAC, e.g., from a connection table represented by Table Four, above (this recovered information could also include the respective User Datagram Protocol (UDP) port number). In this step, the Anchor LAC sends a Call-Disconnect-Notify message (e.g., see L2TP) to the old Serving LAC and also identifies in, e.g., Table Four, above, the existing call variables associated with this PPP connection to the remote user, such as old tunnel-id, and old call-id. On the other hand, if the Anchor LAC should reject the Continued-Call-Request, the Serving LAC either sends a signal back to the user so that the existing PPP session can be torn down and a new PPP session can be initiated or the PPP session is simply dropped (steps not shown) .

In step 440, the Anchor LAC replies with a Continued-Call-Reply (CCRP) message with an appropriate Receive Window Size. The CCRP message includes information on the current *Nr* and *Ns* values. In step 445, the Anchor LAC updates its connection table, e.g., Table 4, above, by replacing the entries for the Tid, Cid, and Serving LAC IP address fields (identified in step 435), with the new call information for the existing PPP connection. In step 450, the new Serving LAC stores the *Nr*, *Ns*, into its *Sr*, *Ss*, values and also stores the receive window size from the received CCRP message, if necessary, and sends a Continued-Call-Connect (CCCN) message to the Anchor LAC, which completes the hand-off.

In support of the above-described hand-off feature for a PPP protocol, FIG. 11 illustrates the above-mentioned new control message transactions in accordance with the principles of the invention. As shown in FIG. 11, a CCRQ message is sent to the identified Anchor LAC.

In this embodiment, a CCRQ message preferably comprises the following fields:

-Assigned Cid,

- Call Serial No.,

- Bearer Type,

- Physical Channel ID,

- Dialed No.,

- Dialing No.,

- Sub-Address,

- Anchor LAC,

- Challenge,

- User AVP,

- User's name, and

- User's MIN/phone.

The Anchor LAC field presumes that this information is available during the hand-off. Alternatively, if the hand-off process does not provide information about the Anchor LAC to the New Serving LAC, the hand-off process must then provide enough user information to the New Serving LAC so that the New Serving LAC can search for the Anchor LAC information using help from a Foreign Radius Server as known in the art. That is, the New Serving LAC enquires about the Anchor LAC from a Home Radius Server via Radius Access/Response messages.

The User AVP information includes user information (such at the user's name) and other user credentials, e.g. multi-hop virtual dial up service, user's identity (MIN), service provider's phone number etc.

Subsequent to the CCRQ message, the Anchor LAC sends a Call-Disconnect-Notify message to the old Serving LAC. Then, the Anchor LAC replies with a Continued-Call Reply (CCRP) message that includes the current *Sr*, *Ss* values that it maintains.

In this embodiment, a CCRP message preferably comprises the following fields:

- Assigned Cid,
- Call Serial No.
- Result-Code,
- Receive Window Size,
- PPD,
- Sequence No. AVP: Nr, Ns,
- ACCM AVP,
- Last Sent LCP Config. Request,
- Last Rcv LCP Config. Request,
- Challenge, and
- Challenge Response.

Finally, the new Serving LAC replies with a Continued-Call Connect (CCCN) message. In this embodiment, a CCCN message preferably comprises the following fields:

- Connect Speed,
- Framing Type,
- Modified Window Size AVP,
- PPD, and
- Challenge Response.

An alternative embodiment with respect to the control message transactions according to the invention is shown in FIG. 19. In such an embodiment, the hand-off control messages (CCRQ, CCRP, and CCCN) are advantageously combined with the tunnel configuration (establishment) control messages (SCCRQ, SCCRP, and SCCCN) and are, respectively, concurrently transmitted between LACs. In this manner, transfer latency between the New Serving LAC and the anchor LAC is significantly improved.

In this case, it is assumed that an existing PPP connection or session is already in progress between, for example, PC 805, Serving LAC 815, Anchor LAC 155 and NS 135 (FIG. 8). Then, in accordance with the mobility of the user, the PC 805 moves into the coverage region of another serving LAC, e.g., Serving LAC 820. As mentioned, use of conventional methodology would result in the PPP connection being dropped, thus requiring that the call be re-established. However, according to the invention, the call is handed-off to the new Serving LAC without interruption from the perspective of the user. In the previous embodiment, assuming that a tunnel does not already exist between the new ServingLAC and the Anchor LAC, the process for establishing a tunnel, for example, as illustrated in FIG. 5, must be performed prior to the hand-off message exchange, for example, as illustrated in FIG. 11. However, in accordance with the embodiment illustrated in FIG. 19, the tunnel establishment process and hand-off process are performed concurrently. Advantageously, the latency associated with the communications between the new Serving LAC and the Anchor LAC is significantly reduce.

Tus, in order to concurrently perform tunnel establishment and call hand-off, the new Serving LAC (e.g., 820 in FIG. 8) attaches the SCCRQ message to the CCRQ message before it sends the CCRQ message to the Anchor LAC. Then, as described above, the Anchor LAC uses the user's information to determine the old Tid value, old Cid value, and old IP/UDP port and sends a Call-Disconnect-Notify (CDN) message to the old Serving LAC. Then, the Anchor LAC replies to the new Serving LAC with the SCCRP message appended to the CCRP message, Lastly, the new Serving LAC transmits the combined CCCN and SCCCN messages to the Anchor LAC. It is to be appreciated that while the tunnel establishment control messages are appended to the hand-off control messages, the individual functions and information contained therein, as described above in detail, remain unchanged.

Also, while FIG. 19 shows certain fields as comprising the hand-off control messages, such messages may contain the same or similar fields as shown in the messages shown in FIG. 11. In addition, it is to be appreciated that any of the fields shown in the context of FIGs 19, 20 and 21 with respect to CCRQ, CCRP, and CCCN,

may be present in the same messages of FIG. 11, and vice versa. Also, since these embodiments are illustrative in nature, none of the messages described herein are necessarily limited to the fields shown.

It is to be appreciated that the term "AVP" refers to Attribute Value Pairs, as is known in PPP operations. Such AVPs are information contained in particular fields of the messages which provide the recipient equipment with relevant information. For example, Window Size AVP and Modified Window Size AVP are fields which respectively indicate to the recipient the window capacity of the sender and a notification to modify the window size. Also, ACCM AVP refers to an Asynchronous Control Character Map AVP. This is a four octet bit map that enables/disables character escapes for 32 ASCII control characters in range 00(hex) to iF(hex). Further, the Sequence No. AVP is the field used to transmit the state variables, Nr and Ns, between servers. Still further, the fields referred to as "Last Sent LCP (Link Control Protocol) Config. Request" and "Last Rcv LCP (Link Control Protocol) Config. Request" are LCP options that are negotiated between servers during an LCP phase associated with the set-up of a PPP session, as is known in the art.

Referring now to FIG. 20, a further alternative embodiment for performing the hand-off control message transaction is shown. In such an embodiment, it is to be appreciated that the Anchor LAC advantageously initiates the hand-off control message transaction with the new Serving LAC, rather than the new Serving LAC. That is, with respect to the arrangement illustrated in FIGs 8, and 9, rather than the new serving LAC 820 initiating the hand-off control message transaction, the Anchor Lac initiates the transaction, once it receives an indication from the PCS 810 (via a wireless link layer) that the PC 805 has moved from the region covered by the Serving LAC 815 to the region covered by the Serving LAC 820. Thus, as shown in FIG. 20, the Anchor LAC transmits the CCRQ message to the new Serving LAC, the new Serving LAC returns the CCRP message, and the Anchor LAC replies with the CCCN message. It is to be appreciated that the information contained in each message, and functions thereof, are similar to that discussed previously and, therefore, will not be repeated here. However, it may be noted that because the Anchor LAC initiates the transactions in FIG. 20, the

fields in the CCRQ message of FIG. 20, sent by the Anchor LAC, are similar to the fields in the CCRP message in FIG. 19, sent by the Anchor LAC. This is due to the fact that the Anchor LAC has this information and sends it to the Serving LAC regardless of who initiates the transaction.

Also, it is to be appreciated that, as in the embodiment shown with respect to FIG. 19, the tunnel establishement control message transaction may also be initiated by the Anchor LAC and, thus, the control message, SCCRQ, SCCRP, and SCCCN, may be respectively combined and concurrently transmitted with the hand-off control messages, CCRQ, CCRP and CCCN.

Turning now to FIG. 12, another embodiment of the inventive concept is shown, in the context of transferring an existing PPP connection from one NAS to another NAS, where the old NAS has a connection to the LNS. In this example, there is no Serving LAC per se, but simply, e.g., an Anchor LAC that is directly supporting an existing PPP connection. FIG. 12 is similar to FIG. 8. Other than the inventive concept, the elements are well-known and will not be described in detail. Like numbers indicate like functions and will not be further described except where necessary.

In FIG. 12, PC 805 includes data communications equipment (not shown) for establishing wireless access through Personal Communications Service (PCS) wireless network 910 to the Internet. PCS Wireless services are known in the art and will not be described in detail. PCS wireless network 910 comprises a plurality of mobile switching centers as represented by elements 875 and 880. Each switching center serves a geographical area (not shown). It is assumed that elements 875 and 880 include an NAS, e.g., LACs similar to Anchor LAC 115 of FIG. 1. Initially, it is assumed that the remote user establishes a VPN session to the corporate network as known in the art using, e.g., that portion of L2TP. In particular, the remote user is in a geographical area such that this initial connection is routed through element 875 via connections 874 and 876 to LNS 935. In the context of a wireless PCS application, the initial PPP connection is between element 875 and PC 805. Although shown as a part of the switching elements for simplicity, the NAS functions could also be performed in

separate pieces of equipment. Similarly, the other elements such as a local network and router are not shown for simplicity.

In this embodiment, the same hand-off procedure is carried out for the LAC/LNS pair except that the above-described CCRQ, CCRP, CCCN messages are exchanged between the new LAC and LNS. In accordance with the inventive concept, an illustrative hand-off message flow is shown in FIG. 13. As can be observed from FIG. 13, a tunnel (identified by a Tid value) and a call (identified by a Cid value) are initially established between element 875, which includes a LAC, and LNS 935. As shown in FIG. 13, the inventive concept allows the existing LAC to transfer the existing PPP connection to a new LAC, as represented by element 880.

Reference should now be made to FIG. 14, which is an illustrative flow chart of a method for use in providing a "hand-off feature." As noted, it is assumed that a VPN session exists between PC 805 and the Corporate network via element 875, which includes a LAC. In accordance with the inventive concept, PCS wireless network 910 adds to the existing call state variables additional variables indicating the presence (or lack thereof) of a PPP connection for each wireless call, and if a PPP connection exists, PPP connection information that includes the LNS identification, e.g., the IP address of the LNS.

In step 505 of FIG. 14, PCS wireless network 910 detects the need for a hand-off because PC 805 has moved from the geographical area served by element 875 to another geographical area, e.g., the area served by element 880, which includes another LAC. In step 510, PCS Wireless system provides element 880 with notification of the impending hand-off. (The method(s) used by a wireless system to detect and prosecute a hand-off are known in the art and not relevant to the inventive concept. As such, they will not be described herein and are represented by signaling path 911 of FIG. 12.) Since the call state information now includes a PPP session indicator and PPP call information, the new LAC (of element 880) identifies the LNS in step 515. In step 520, the new LAC (of element 880) checks to see if there is an existing tunnel between itself and the identified LNS, here LNS 935.

If no tunnel exists, the new LAC first establishes a tunnel (as described earlier) in step 525. Then, and in accordance with the inventive concept, the new LAC sends a Continued-Call-Request (CCRQ) message to the LNS in step 530. This CCRQ message includes the user's name associated with the existing PPP connection, the Tid and Cid values to be used for the transferred (new) PPP session.

In step 535, the LNS recovers the user's name from the received CCRQ message and uses this information to determine the IP address of the old LAC (this information could also include the respective User Datagram Protocol (UDP) port number). In this step, the LNS sends a Call-Disconnect-Notify message (e.g., see L2TP) to the old LAC and also identifies in, e.g., a connection table similar to that shown in Table Four, above, but sans the Serving LAC information etc., the existing call variables associated with this PPP connection to the remote user, such as old tunnel-id, and old call-id. On the other hand, if the LNS should reject the Continued-Call-Request, the new LAC either sends a signal back to the user so that the existing PPP session can be torn down and a new PPP session can be initiated or the PPP session is simply dropped (steps not shown) .

In step 540, the LNS replies with a Continued-Call-Reply (CCRP) message with an appropriate Receive Window Size. The CCRP message includes information on the current *Nr* and *Ns* values. In step 545, the LNS updates its connection table by replacing the entries for the Tid, Cid, and LAC IP address fields (identified in step 535), with the new call information for the existing PPP connection. In step 550, the new LAC updates the Nr, Ns, and receive window size from the received CCRP message, if necessary, and sends a Continued-Call-Connect (CCCN) message to the LNS, which completes the hand-off.

In support of the above-described hand-off feature for a PPP protocol, FIG. 15 illustrates the above-mentioned new control message transactions in accordance with the principles of the invention. As shown in FIG. 15, a CCRQ message is sent to the identified LNS. Alternatively, if the hand-off process does not provide information about the LNS to the new LAC, the hand-off process must then provide enough user

information to the new LAC so that the new LAC can search for the LNS information using help from a Foreign Radius Server as known in the art. That is, the new LAC enquires about the LNS from a Home Radius Server via Radius Access/Response messages. Subsequent to the CCRQ message, the LNS sends a Call-Disconnect-Notify message to the old LAC. Then, the LNS replies with a Continued-Call Reply message that includes the current *Sr*, *Ss* values that it maintains. Finally, the new LAC replies with a Continued-Call Connect (CCCN) message.

As described above, a PPP connection is transferred from one NAS to another NAS. In support of the newly defined messages, additional call states are defined for the respective NAS as illustrated in Tables 5 and 6, below.

Table 5 – New LAC (or NAS)

Call State	Event	Action	New State
idle	hand-off notification	Send CCRQ	wait-CCRP-reply
wait-CCRP-reply	Receive CCRP, not accepted,	Clean-up	idle
wait-CCRP-reply	Receive CCRP, accepted,	Send CCCN	established,

As can be observed, the additional, or, new, call state for mL2TP associated with the new LAC (or NAS) for a continued call is the wait-CCRP-reply state.

Referring now to FIG. 21, still a further alternative embodiment for performing the hand-off control message transaction is shown. In such an embodiment, it is to be appreciated that the LNS initiates the hand-off control message transaction with the new Serving LAC, rather than the new Serving LAC. That is, with respect to the arrangement illustrated in FIGs 12 and 13, rather than the new serving LAC 880 initiating the hand-off control message transaction, the LNS initiates the transaction, once it receives an indication from the PCS 910 (via a wireless link layer) that the PC

805 has moved from the region covered by the Serving LAC 875 to the region covered by the Serving LAC 880. Thus, as shown in FIG. 21, the LNS transmits the CCRQ message to the new Serving LAC, the new Serving LAC returns the CCRP message, and the LNS replies with the CCCN message. It is to be appreciated that the information contained in each message, and functions thereof, are similar to that which was discussed previously and, therefore will not be repeated here. Also, it is to be appreciated that, as in the embodiment shown with respect to FIG. 19, the tunnel establishment control message transaction may also be initiated by the LNS and, thus, the control messages, SCCRQ, SCCRP, and SCCCN, may be respectively combined and concurrently transmitted with the hand-off control messages, CCRQ, CCRP, and CCCN.

Referring now to FIGs 22 and 23, respective alternative embodiments for performing a hand-off control message transaction, according to the invention, by employing radius servers are shown. Particularly, FIG. 22 shows an arrangement similar to the arrangement shown in FIGs 8 and 9, while FIG 23 shows an arrangement similar to the arrangement shown in FIGs 12 and 13. As previously mentioned radius servers, as are known in the art, may be used by the other servers (e.g., Serving LAC, Anchor LAC, LNS) employed in the communication path to assist in identifying and/or confirming particular information necessary for performing communication functions. For instance, as mentioned, a radius server operatively coupled to a Serving LAC may contain a database which associates a particular user with a particular Anchor LAC. In this way, the Serving LAC consults with its radius server to determine such information. Likewise, the Anchor LAC may consult a radius server (home), operatively coupled thereto, to determine similar information pertaining to a user and the LNS with which he is associated.

However, according to the invention, the radius servers may be advantageously utilized to also perform a hand-off control message transaction therbetween. That is, rather than a Serving LAC and an Anchor LAC or a Serving LAC and an LNS performing the transaction, respective radius servers operatively coupled thereto and to one another are used to transfer these control messages. In such case, the Serving LAC,

Anchor LAC, and LNS are merely tasked with performing any additional processing caused by these messages.

FIG. 22 shows such an arrangement int he context of a hand-off of a PPP connection from and old Serving LAC 815 to a new Serving LAC 820 with respect to the Anchor LAC. A radius server 822, associated with the new Serving LAC 820 is in communication with a radius server 824, associated with the Anchor LAC. Thus, according to the invention, when a hand-off notification is received from the PCS 810 (FIG. 8), the radius servers 822 and 824 directly transfer the control messages, CCRQ, CCRP, and CCCN, therebetween. In accordance with the invention, either radius server may initiate the transfer.

Similarly, FIG. 23 shows such an arrangement in the context of a hand-off of a PPP connection from an old Serving LAC 875 to a new Serving LAC 880 with respect to the LNS 935. A radius server 922, associated with the new Serving LAC 880, is in communication with a radius server 924, associated with the LNS. Thus, according to the invention, when a hand-off notification is received from the PCS 910 (FIG. 12), the radius servers 922 and 924 directly transfer the control messages, CCRQ, CCRP, and CCCN, therebetween. In accordance with the invention, either radius server may initiate the transfer.

Payload Message Overviews and Congestion Control for mL2TP

With respect to payload messages for mL2TP, the Serving LAC and the LNS follow L2TP procedures. The Anchor LAC swaps the Tid and Cid for the payload packets. The Anchor LAC also monitors the (*Nr*, *Ns*) values sent by the Serving LAC. (It should be noted that since there may be packet losses between the Serving LAC and the Anchor LAC, it is expected that both the *Sr* and *Ss* values at the Anchor LAC may be lagging behind those values maintained at the Serving LAC.) The Anchor LAC does not change the (*Nr*, *Ns*) of the payload packets in either directions. The Anchor LAC only makes use of its own *Sr*, *Ss* values when it receives a Continued-Call Request message from a new Serving LAC.

With respect to congestion control, the L2TP requirements on when to abide to receive window size, when to send *Nr/Ns*, and when to send an ACK apply to mL2TP. In addition, mL2TP also has the following additional requirements for the Serving LAC and the Anchor LAC.

The Anchor LAC is required to monitor the (*Nr*, *Ns*) value sent by the Serving LAC. The Anchor LAC should include the (*Sr*, *Ss*) value it maintains in the Continued-Call-Reply message when it replies to the Continued-Call-Connect message it receives from a Serving LAC. Since a network between the Serving LAC and an Anchor LAC is lossy, the *Sr* value maintained by an Anchor LAC may be lagging behind the Serving LAC.

The following is a detailed description of the payload processing rules associated with mL2TP, as affected by the multi-hop point-to-point protocol of the invention. As mentioned, for the multi-hop scenario, the Anchor LAC performs the swappin gof the Tid and Cid values for the payload packets. In addition, the Anchor LAC maintains a 4 tuple state variable (Sr^S, Ss^S, Sr^L, Ss^L) for nL2TP payload packets. The Anchor LAC stores the (Nr, Ns) value sent by the Serving LAC in (Sr^S, Ss^S) and the (Nr, Ns) values from the LNS in (Sr^L, Ss^L).

Note that since there may be packet losses and/or delay between the serving lAC and the Anchor LAC, it is expected that $Sr^S < Sr$ and $Ss^S < Ss$, where Sr and Ss are the state variables maintained at the serving LAC. Similarly, since there are also packet losses and/or delays between the Anchor LAC and LNS, it is expected that $Sr^L < Sr$ and $Ss^L < Ss$, where Sr and Ss are the state variables maintained at the LNS. It is to be appreciated that the Anchor LAC will not change the (Nr, Ns) values of the payload packets in either direction. Three example are given below to illustrate how state variable monitoring according to the invention operates.

The first monitoring example is with respect to the case where the communication scenario converts from the one-hop to a two-hop arrangement. It is to be understood that a one-hop arrangement includes, for example, communication links

between a PC, an Anchor LAC, and an LNS. A two-hop arrangement includes, for example, communication links between a PC, a Serving LAC, an Anchor LAC, and an LNS. If the Anchor LAC previously maintains a two tuple state variable for a PPP session and receives a CCRQ message, then the Anchor LAC knows that it needs to convert from a one-hop session to a two-hop session. The Anchor LAC first sets Nr = Sr and Ms = Ss in the CCRP message using its current two tuple state variable, (Sr, Ss). Then, the Anchor LAC changes the state variables into four typle, setting $Sr^S = Sr$, $Ss^S = Ss$, $Sr^L = x$, and $Sr^L = x$. When the Anchor LAC receives the first packet from the LNS after the handover, it updates the Ss^L and Sr^L variables with the observed (Nr, Ns) values. For example, assume the old LAC has Ss = 13 and Sr = 6, and the LNS has Ss = 7 and Sr = 10. The Old LAC, which is now the Anchor LAC, sets Nr = Sr and Ns = Ss in the CCRP message. After the handover, the new Serving LAC has Ss = 13 and Sr = 6, the LNS has Ss = 7+ and Sr = 10+, and the Anchor LAC (old LAC) has $Ss^S = 13$, $Sr^S = 6$, $Ss^L = 7+$, and $Sr^L = 10+$. It is to be appreciated that the plus sign (+) at the end of certain values means that the value could be larger, depending on whether the sequence numbers are being updated during the hand-off process.

The second monitoring example is with respect to the case where the communication scenario converts from a two-hop to a one-hop arrangement. Again, it is to be understood that a one-hop arrangement includes, for example, communication links between a PC, an Anchor LAC, and an LNS, while a two-hop arrangement includes, for example, communication links between a PC, a Serving LAC, an Anchor LAC, and an LNS. If the Anchor LAC receives indication that a two-hop PPP session is turned into a one-hop session (e.g., receiving a link layer handover message rather than a mL2TP CCRQ message), the Anchor LAC turns the four tuple state variable into a two tuple state variable and sets $Ss = Ss^S$ and $Sr = Ss^L$. For example, assume the new Serving LAC has Ss = 13 and Sr = 5, the LNS has Ss = 7 and Sr = 10, and the Anchor LAC has $Ss^S = 12$, $Sr^S = 4$, $Ss^L = 6$, and $Sr^L = 9$. Then, after conversion from the two-hop to the one-hop arrangement, the Anchor LAC has Ss = 12 and Sr = 6 and the LNS has Ss =7+ and Sr = 10+.

The third monitoring example is with respect to the case where the communication scenario converts from a two-hop to another two-hop arrangement, for example, as shown in FIG. 9. If the Anchor LAC receives a CCRQ message and the PPP session is already a two-hop session, then the Anchor LAC knows that there is a change of Serving LACs. The Anchor LAC then sets $Nr = Ss^L$ and $Ns = Ss^S$ in the CCRP message. The Anchor LAC also updates Sr^S to $Sr^S = Ss^L$. For example, assume the old Serving LAC has SS = 13 and Sr = 5, the LNS has Ss = 7 and Sr = 10, and the Anchor LAC has $Ss^S = 12$, $Sr^S = 4$, $Ss^L = 6$, and $Sr^L = 9$. Then, the Ancor LAC sets $Ns = Ss^S$ and $Nr = Ss^L$ in the CCRP message sent to the new Serving LAC. After the handover, the new Serving LAC has Ss = 12 and Sr = 6, the LNS has Ss = 7+ and Sr = 10+, and the Anchor LAS has $Ss^S = 12$, $Sr^S = 4$, $Ss^L = 6+$, and $Sr^L = 9+$.

In addition, the Serving LAC implements a full receiver rather than a simple receiver, as referred to in the art. This requirement is to prevent the new Serving LAC from passing out-of-sequence or duplicate packets to upper layers when there is a change of Serving LAC during the lifetime of a PPP session.

Turning briefly to FIG. 16, a high level block diagram of a representative NAS is shown. An NAS is a stored-program-control based processor architecture and includes processor 650, memory 660 for storing program instructions and data, e.g., the above-mentioned connection tables, etc., and communications interface(s) 665 for coupling to one or more communication facilities as represented by path 666.

The foregoing merely illustrates the principles of the invention and it will be appreciated that those skilled in the art will be able to devise numerous alternative arrangements which, although not explicitly described herein, embody the principles of the invention and are within its spirit and scope. For example, although the inventive concept was described in the context of a Serving NAS initiating the establishment of a multi-hop tunnel for incoming calls, the inventive concept is equally applicable to, e.g., the LNS initiating the establishment of a multi-hop sequence for outgoing calls. Such modifications are straightforward and will not be described herein as illustrated by

Chuan 18-14

FIGs. 17 - 18.

Claims:

1. Apparatus comprising:

a first packet server;

a second packet server having a point-to-point communication path established with the first packet server; and

a third packet server configured for establishing a point-to-point communication path with the second packet server in response to receipt of a hand-off notification, the third packet server transmitting a message signal to the second packet server, the message signal including a communication path set-up request and a continue communcation request.

2. The apparatus of Claim 1, wherein the second packet server is configured for transmitting a message signal to the first packet server, the message signal including notification that the communication path between the first packet server and the second packet server is to be disconnected.

3. The apparatus of Claim 1, wherein the message signal contains at least a portion of information associated with the point-to-point communication path between the first packet server and the second packet server.

4. The apparatus of Claims 1, wherein the second packet server is configured for transmitting a message signal to the third packet server, the message signal including a reply to the communication path set-up request and the continue communication request transmitted by the third packet server.

5. The apparatus of Claim 4, wherein the third packet server is configured for transmitting a message signal to the second packet server, the message signal including a reply to the reply message signal transmitted by the secodnd packet server.

6. The apparatus of Claim 1, wherein the point-to-point communication path between the servers is established according to a tunneling protocol.

7. Apparatus for transferring packet data comprising:

a first packet server;

a second packet server having a point-to-point communication path established with the first packet server; and

a third packet server; and

the second packet server configured for establishing a point-to-point communication path with the second packet server in response to receipt of a hand-off notification, the second packet server transmitting a message signal to the third packet server, the message signal including a communication path set-up request and a continue communciation request.

8. The apparatus of Claim 7, wherein the second packet server is configured for transmitting a message signal to the first packet server, the message signal including notification that the communication path between the first packet server and the second packet server is to be disconnected.

9. The apparatus of Claim 7, wherein the message signal contains at least a portion of information associated with the point-to-point communication path between the first packet server and the second packet server.

10. The apparatus of Claims 7, wherein the third packet server is configured for transmitting a message signal to the second packet server, the message signal including a reply to the communication path set-up request and the continue communciation request transmitted by the second packet server.

11. The apparatus of Claim 10, wherein the second packet server is configured for transmitting a message signal to the third packet server, the message signal including a reply to the reply message signal transmitted by the third packet server.

12. The apparatus of Claim 7, wherein the point-to-point communication path between the servers is established according to a tunneling protocol.

13. Apparatus for transferring packet data comprising:

a first packet server;

a second packet server having a point-to-point communication path established with the first packet server; and

a third packet server; and

the second packet server configured for establishing a point-to-point communication path with the third packet server in response to receipt of a hand-off notification, the second packet server transmitting a message signal to the third packet server, the message signal including a continue communication request.

14. The apparatus of Claim 13, wherein the second packet server is configured for transmitting a message signal to the first packet server, the message signal including notification that the communication path between the first packet server and the second packet server is to be disconnected.

15. The apparatus of Claim 13, wherein the message signal contains at least a portion of information associated with the point-to-point communication path between the first packet server and the second packet server.

16. The apparatus of Claims 13, wherein the third packet server is configured for transmitting a message signal to the second packet server, the message signal

including a reply to the continue communication request transmitted by the second packet server.

17. The apparatus of Claim 16, wherein the second packet server is configured for transmitting a message signal to the third packet server, the message signal including a reply to the reply message signal transmitted by the third packet server.

18. The apparatus of Claim 13, wherein the point-to-point communication path between the servers is established according to a tunneling protocol.

19. Apparatus for transferring packet data comprising:

a first packet server;

a second packet server having a point-to-point communication path established with the first packet server; the second packet server having a radius server associated therewith;

a third packet server configured for establishing a point-to-point communication path with the second packet server in response to receipt of a hand-off notification, the third packet server having a radius server associated therewith for transmitting a message signal to the radius server of the second packet server, the message signal including a continue communication request.

the second packet server configured for establishing a point-to-point communication path with the third packet server in response to receipt of a hand-off notification, the second packet server transmitting a message signal to the third packet server, the message signal including a continue communication request.

20. The apparatus of Claim 19, wherein the message signal further includes a communication path set-up request.

21. Apparatus for transferring packet data comprising:

a first packet server;

a second packet server having a point-to-point communication path established with the first packet server; the second packet server having a radius server associated therewith;

a third packet having a radius server associated therewith; and

the second packet server configured for establishing a point-to-point communication path with the third packet server in response to receipt of a hand-off notification, the radius server associated with the second packet server transmitting a message signal to the radius server of the third packet server, the message signal including a continue communication request.

22. The apparatus of Claim 21, wherein the message signal further includes a communication path set-up request.

23. A method for transferring packet data comprising the steps of:

establising a point-to-point communication path between a first packet server and a second packet server;

receiving a hand-off notification signal;;

transmitting a message signal between a third packet server and the second packet server in response to the hand-off notification signal, the message signal including a communication path set-up request and a continue communication request.

24. The apparatus of Claim 23, wherein the message signal is initiated by the second packet server.

25. The method of Claim 23, wherein the message signal is initiated by the third packet server.

Chuah-Rai 8-4

11. A method for transferring packet data comprising the steps of:

establishing a point-to-point communication path between a first packet server and a second packet server;

receifing a hand-off notification signal;

transmitting a message signal between a radius server associated with a third packet server and a radius server associated with the second packet server in response to the hand-off notification signal, the message signal including a communication path set-up request and a continue communication request.

27. The method of Claim 26, wherein the message signal is initiated by the radius server of the second packet server.

28. The method of Claim 26, wherein the message signal is initiated by the radius server of the third packet server.

29. A method for transferring packet data comprising the steps of:

establishing a point-to-point communication path between a first packet server and a second packet server;

receiving a hand-off notification signal;

a second packet server having a point-to-point communication path established with the first packet server; the second packet server having a radius server associated therewith;

a third packet having a radius server associated therewith; and

transmitting a message signal from the secodnd packet server to a third packet server in response to the hand-off notification signal, the message signal including a continue communication path set-up request and a continue communication request.

Chuah-Rai 8-4

30. Apparatus for transferring packet data comprising:

a first packet server configured for establishing a point-to-point communication path between a user and a private network;

a second packet, server configured for establishing a point-to-point communication path between the user and the first packet server such that a multi-hop communication path is established between the user and the private network; and

the first packet server monitoring state variables transmitted between the second packet server and the private network.

31. The apparatus of Claim 30, wherein a tunnel protocol is used to establish the multi-hop communication path.

32. The apparatus of Claim 30, wherein the first packet server stores a four tuple state variable set wherein two state variables are associated with the second packet server and two state variables are associated with the private network.

33. A method for transferring packet data comprising the steps of:

establishing a point-to-point communication path between a user and a private network via a first packet server;

establishing a point-to-point communication path between the user and the first packet server via a second packet server such that a multi-hop communication path is established between the user and private network; and

monitoring state variables transmitted between the second packet server and the private netwok;

34. The method of Claim 33, wherein a tunnel protocol is used to establish the multi-hop communication path.

35. The method of Claim 33, wherein the first packet server stores a four tuple state variable set wherein two state variables are associated with the second packet server and two state variables are associated with the private network.

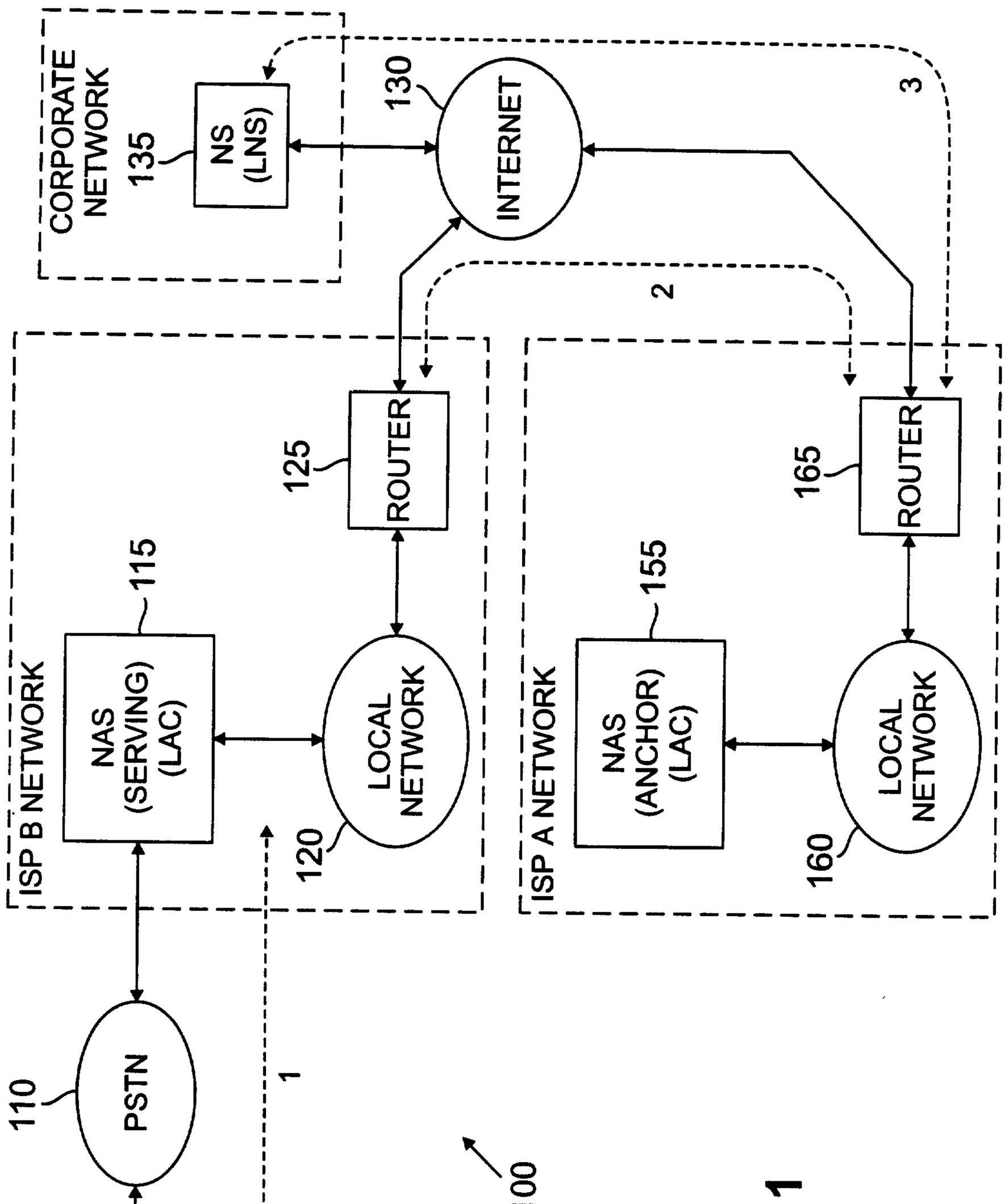
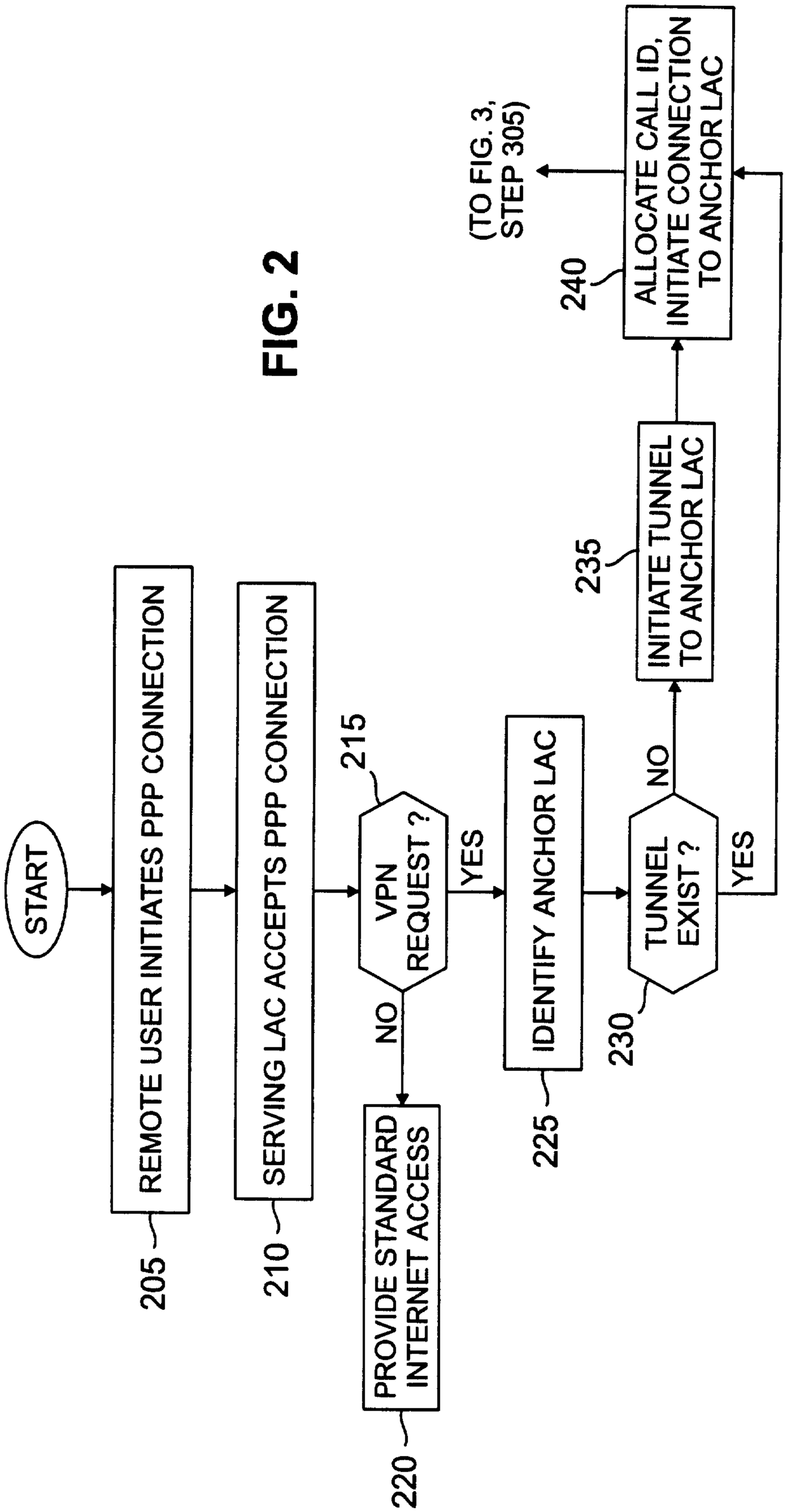

CORPORATE NETWORK
NS (LNS)
135
130
INTERNET
3
2
ROUTER
125
ROUTER
165
115
155
ISP B NETWORK
NAS (SERVING) (LAC)
LOCAL NETWORK
120
ISP A NETWORK
NAS (ANCHOR) (LAC)
LOCAL NETWORK
160
PSTN
110
1
100
PC
105

FIG. 1

FIG. 2


START
REMOTE USER INITIATES PPP CONNECTION
205
SERVING LAC ACCEPTS PPP CONNECTION
210
VPN REQUEST ?
215
NO
YES
PROVIDE STANDARD INTERNET ACCESS
220
IDENTIFY ANCHOR LAC
225
TUNNEL EXIST ?
230
NO
YES
INITIATE TUNNEL TO ANCHOR LAC
235
ALLOCATE CALL ID, INITIATE CONNECTION TO ANCHOR LAC
240
(TO FIG. 3, STEP 305)

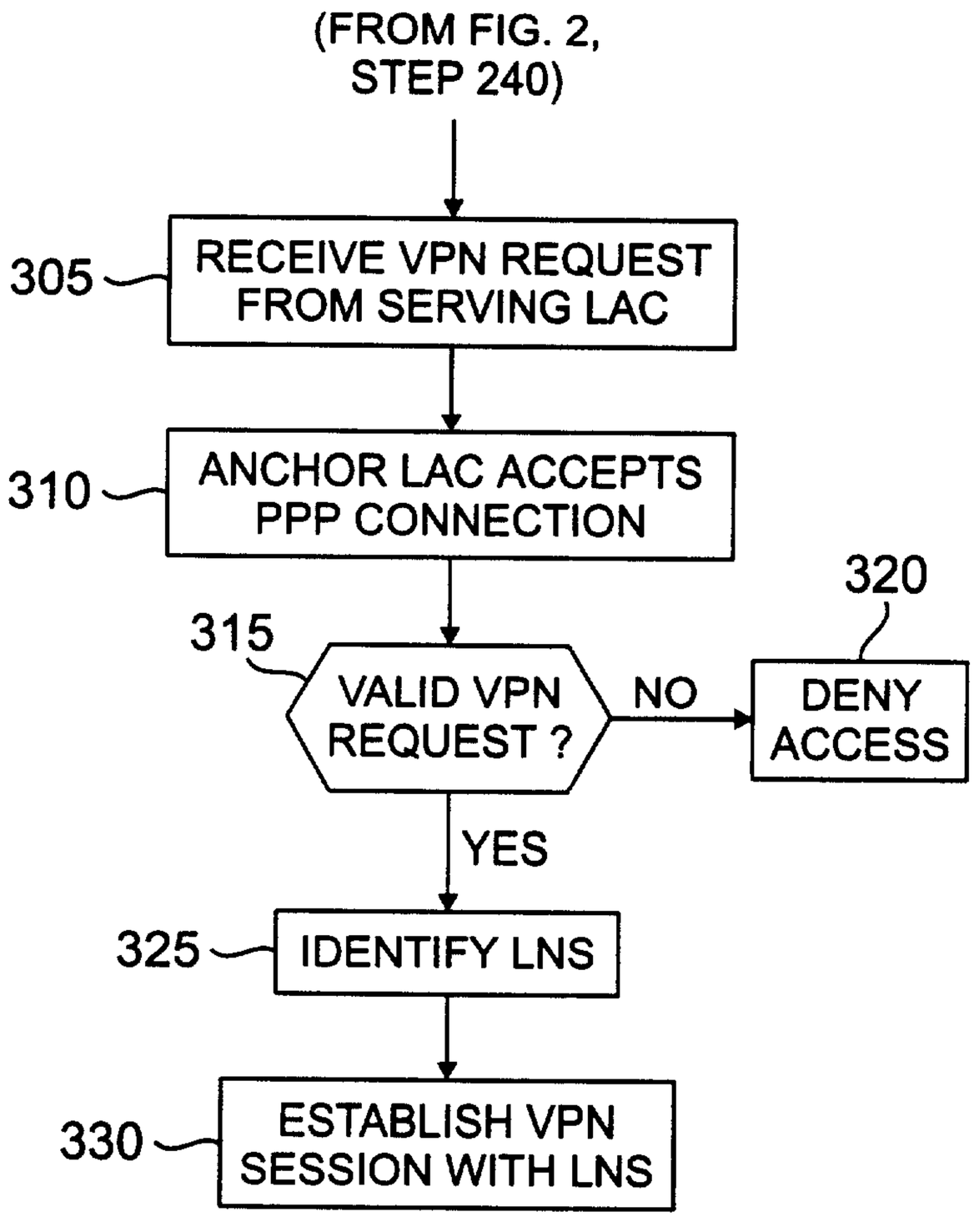

(FROM FIG. 2,
STEP 240)
305
RECEIVE VPN REQUEST
FROM SERVING LAC
310
ANCHOR LAC ACCEPTS
PPP CONNECTION
315
VALID VPN
REQUEST ?
NO
320
DENY
ACCESS
YES
325
IDENTIFY LNS
330
ESTABLISH VPN
SESSION WITH LNS

FIG. 3


SERVING LAC
TID = 2
CID = 5
ANCHOR LAC
TID = 1
CID = 3
LNS

FIG. 4

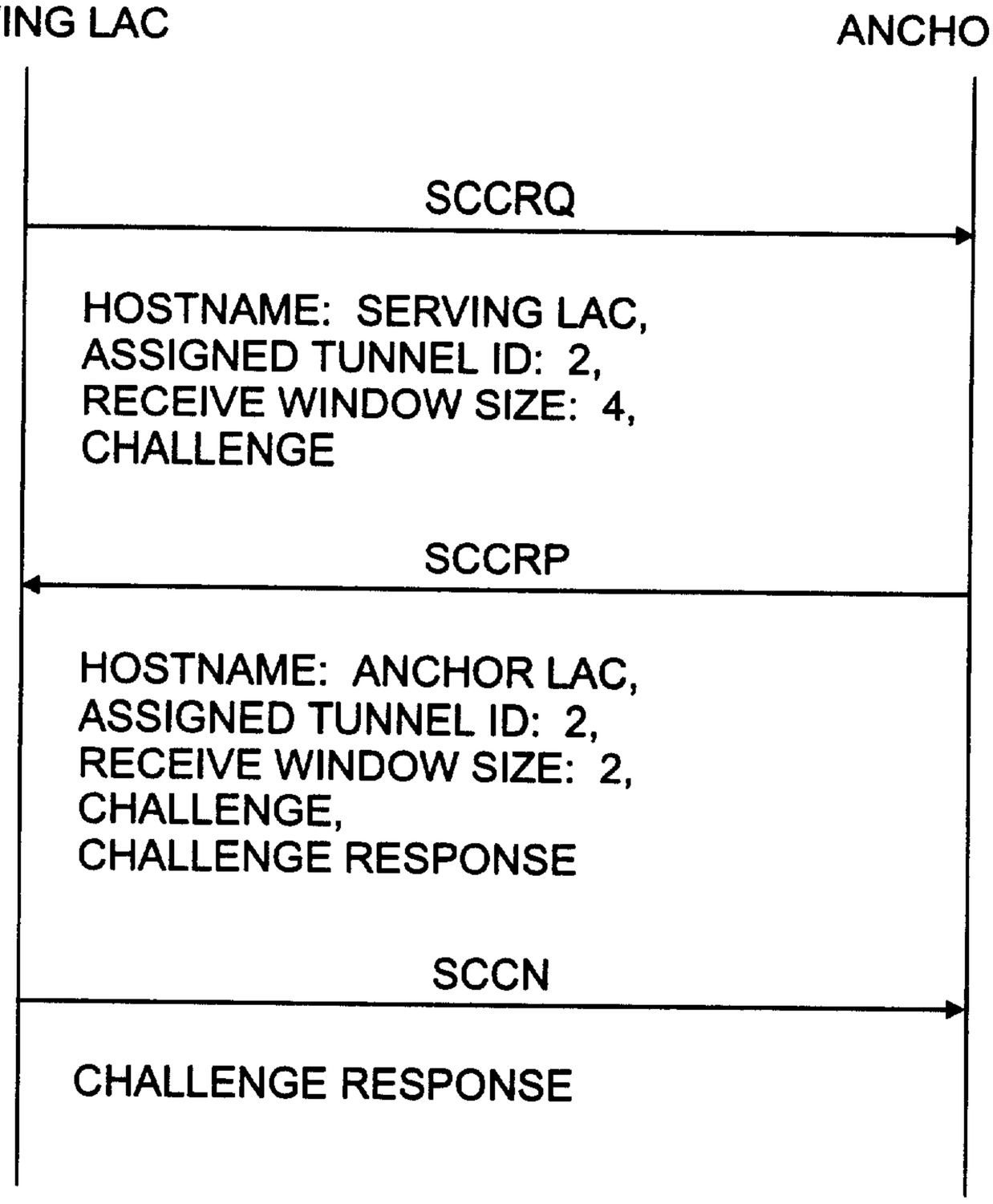

SERVING LAC
ANCHOR LAC
SCCRQ
HOSTNAME: SERVING LAC,
ASSIGNED TUNNEL ID: 2,
RECEIVE WINDOW SIZE: 4,
CHALLENGE
SCCRP
HOSTNAME: ANCHOR LAC,
ASSIGNED TUNNEL ID: 2,
RECEIVE WINDOW SIZE: 2,
CHALLENGE,
CHALLENGE RESPONSE
SCCN
CHALLENGE RESPONSE

FIG. 5

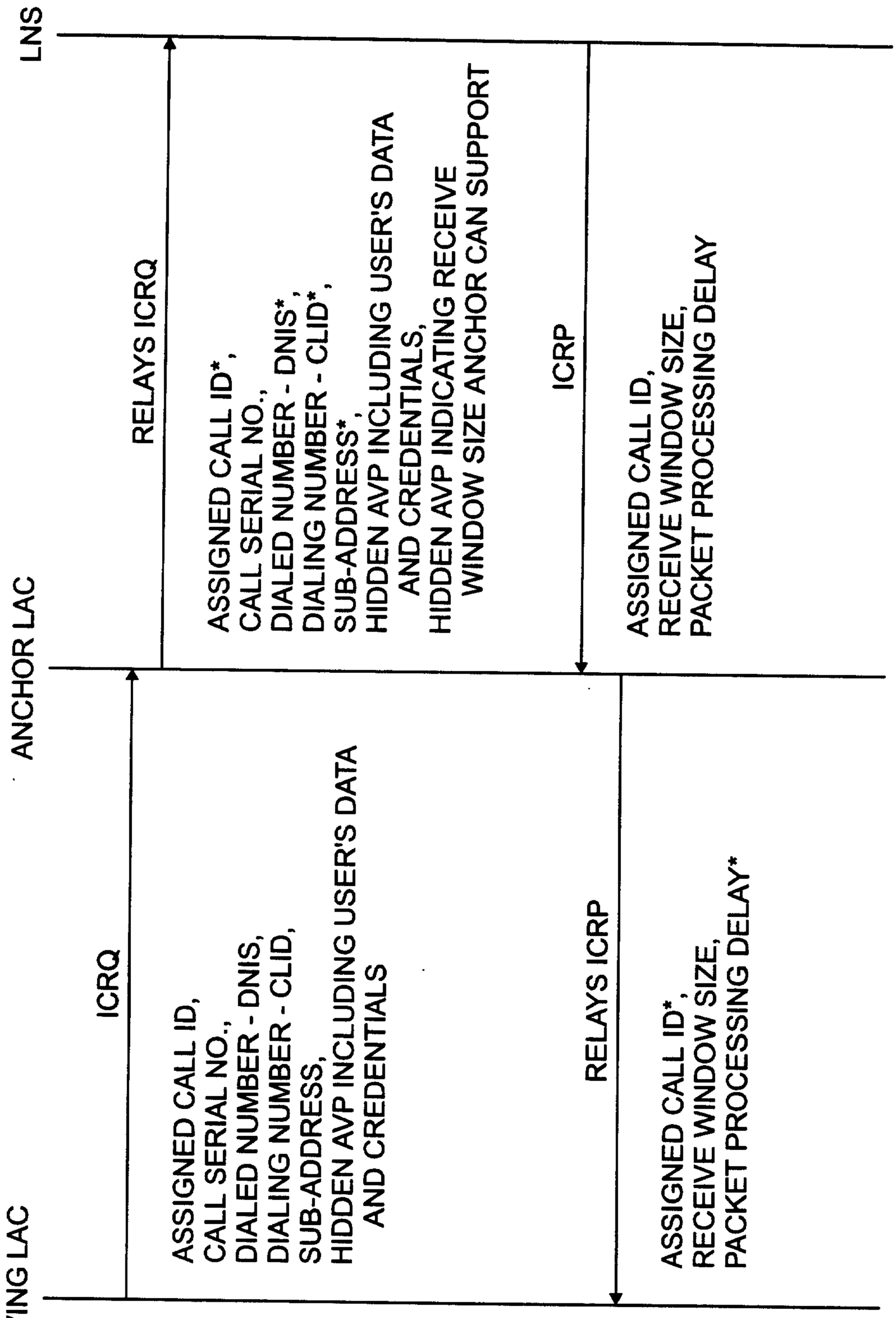

SERVING LAC
ANCHOR LAC
ICRQ
ASSIGNED CALL ID,
CALL SERIAL NO.,
DIALED NUMBER - DNIS,
DIALING NUMBER - CLID,
SUB-ADDRESS,
HIDDEN AVP INCLUDING USER'S DATA
AND CREDENTIALS
RELAYS ICRQ
ASSIGNED CALL ID*,
CALL SERIAL NO.,
DIALED NUMBER - DNIS*,
DIALING NUMBER - CLID*,
SUB-ADDRESS*,
HIDDEN AVP INCLUDING USER'S DATA
AND CREDENTIALS,
HIDDEN AVP INDICATING RECEIVE
WINDOW SIZE ANCHOR CAN SUPPORT
ICRP
ASSIGNED CALL ID,
RECEIVE WINDOW SIZE,
PACKET PROCESSING DELAY
RELAYS ICRP
ASSIGNED CALL ID*,
RECEIVE WINDOW SIZE,
PACKET PROCESSING DELAY*

FIG. 6

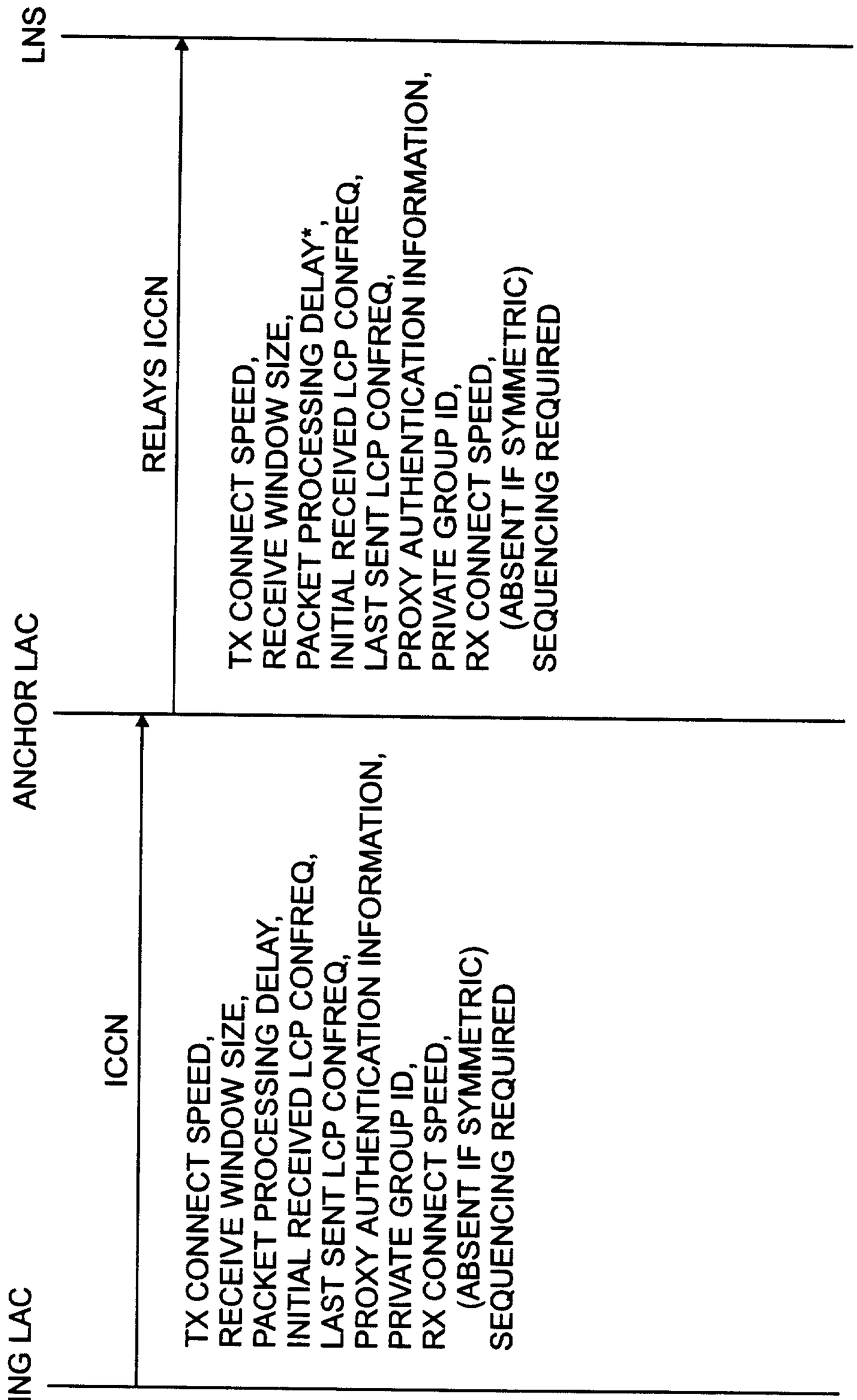

SERVING LAC
ICCN
TX CONNECT SPEED,
RECEIVE WINDOW SIZE,
PACKET PROCESSING DELAY,
INITIAL RECEIVED LCP CONFREQ,
LAST SENT LCP CONFREQ,
PROXY AUTHENTICATION INFORMATION,
PRIVATE GROUP ID,
RX CONNECT SPEED,
(ABSENT IF SYMMETRIC)
SEQUENCING REQUIRED
ANCHOR LAC
RELAYS ICCN
TX CONNECT SPEED,
RECEIVE WINDOW SIZE,
PACKET PROCESSING DELAY*,
INITIAL RECEIVED LCP CONFREQ,
LAST SENT LCP CONFREQ,
PROXY AUTHENTICATION INFORMATION,
PRIVATE GROUP ID,
RX CONNECT SPEED,
(ABSENT IF SYMMETRIC)
SEQUENCING REQUIRED
LNS

FIG. 7

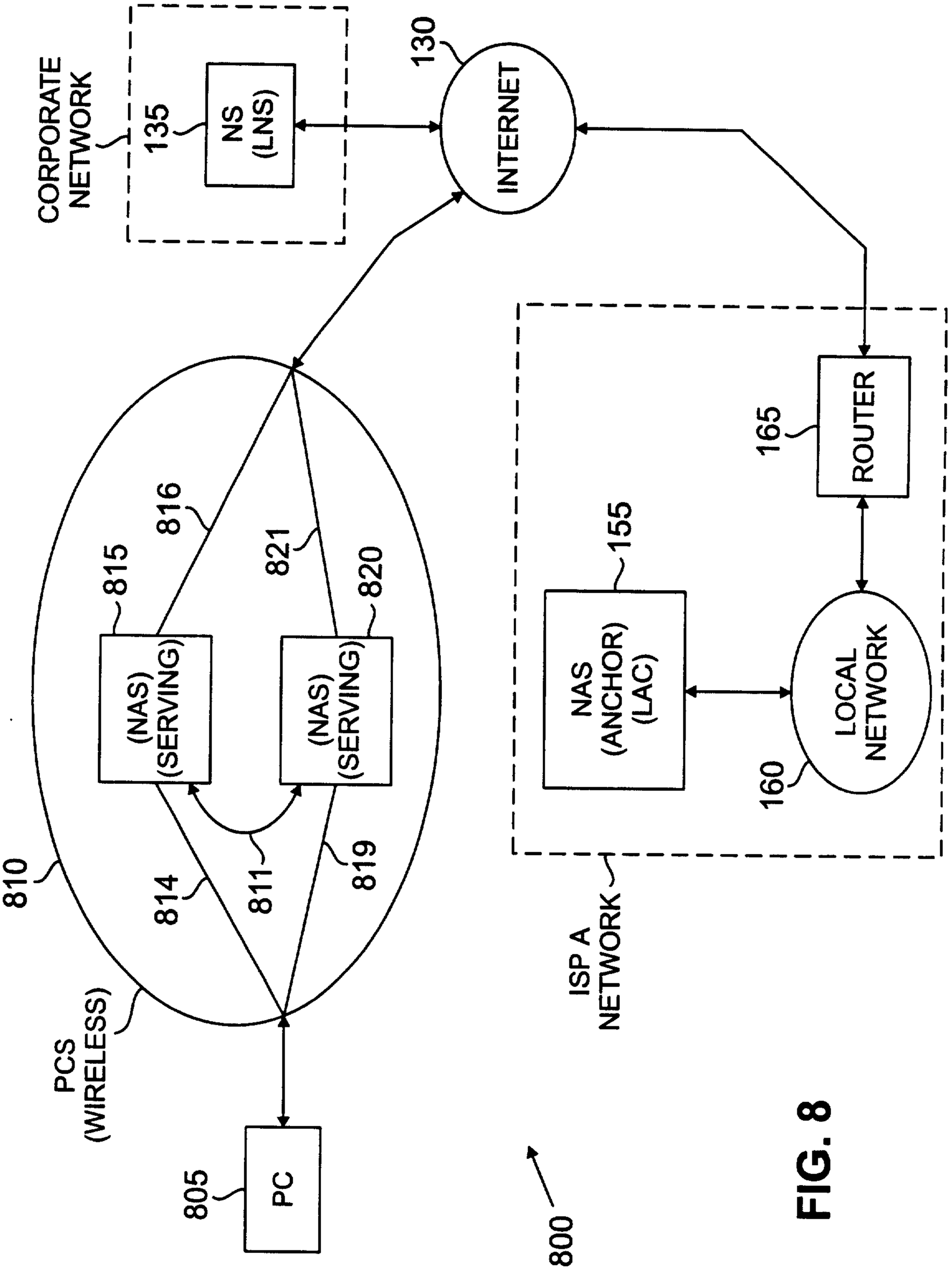

CORPORATE NETWORK
135
NS (LNS)
130
INTERNET
165
ROUTER
155
NAS (ANCHOR) (LAC)
160
LOCAL NETWORK
ISP A NETWORK
816
815
821
820
(NAS) (SERVING)
(NAS) (SERVING)
810
814
811
819
PCS (WIRELESS)
805
PC
800

FIG. 8

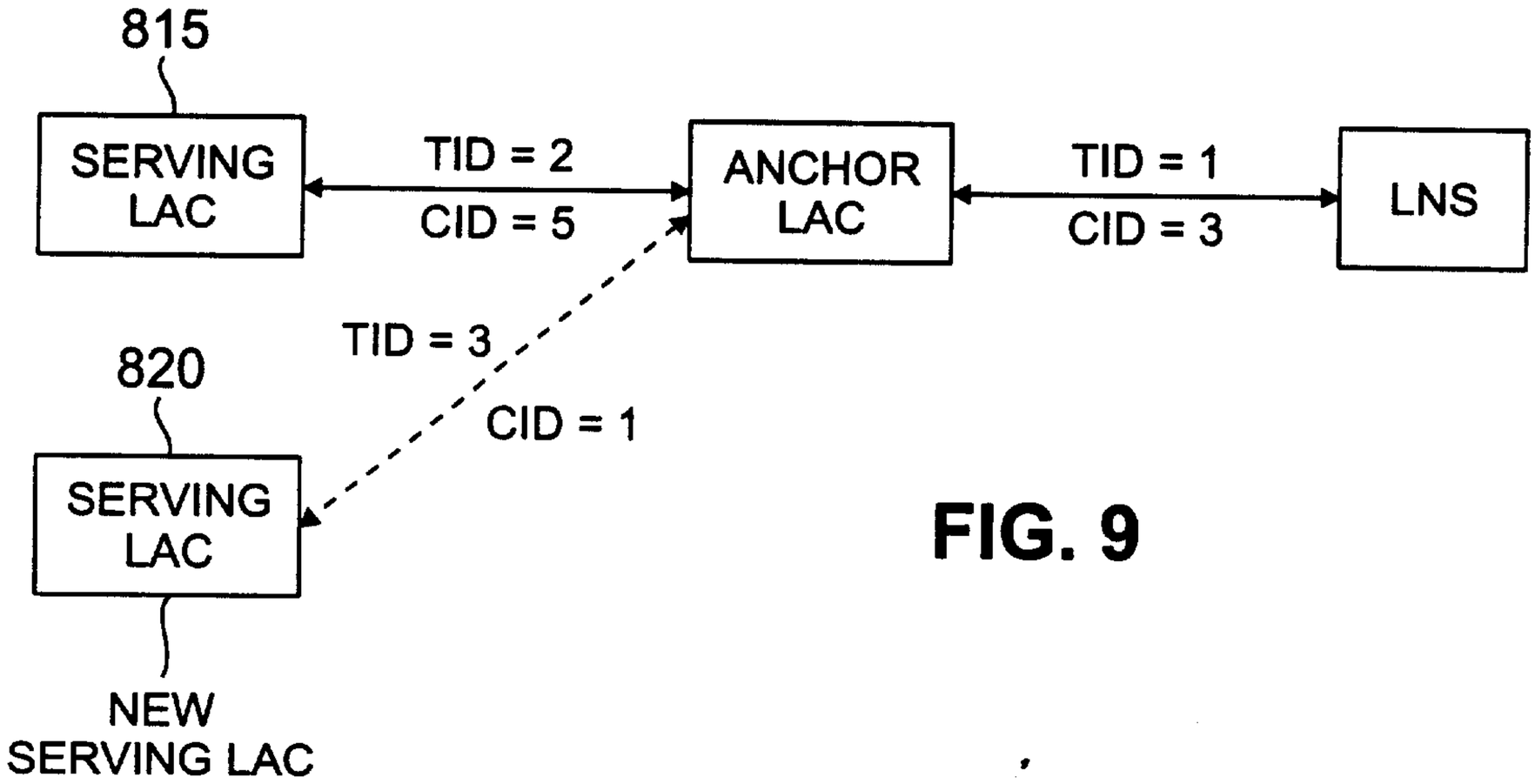

815
SERVING LAC
TID = 2
CID = 5
ANCHOR LAC
TID = 1
CID = 3
LNS
TID = 3
CID = 1
820
SERVING LAC
NEW SERVING LAC

FIG. 9

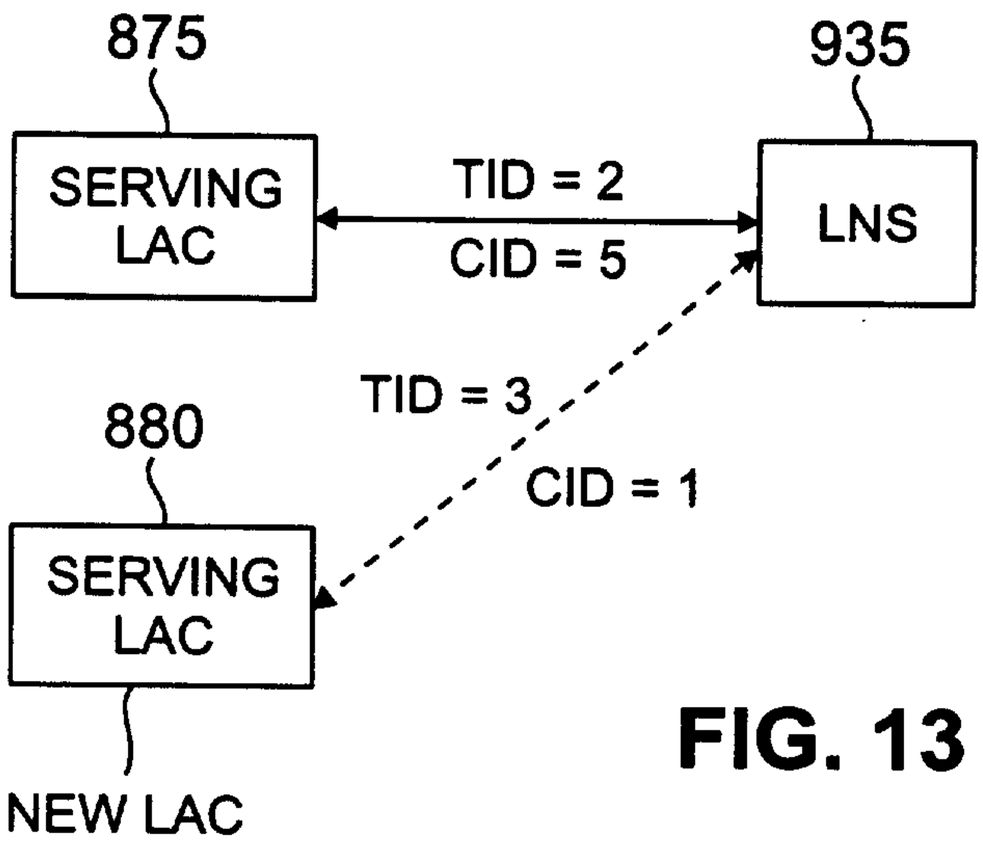

875
SERVING LAC
TID = 2
CID = 5
935
LNS
TID = 3
CID = 1
880
SERVING LAC
NEW LAC

FIG. 13

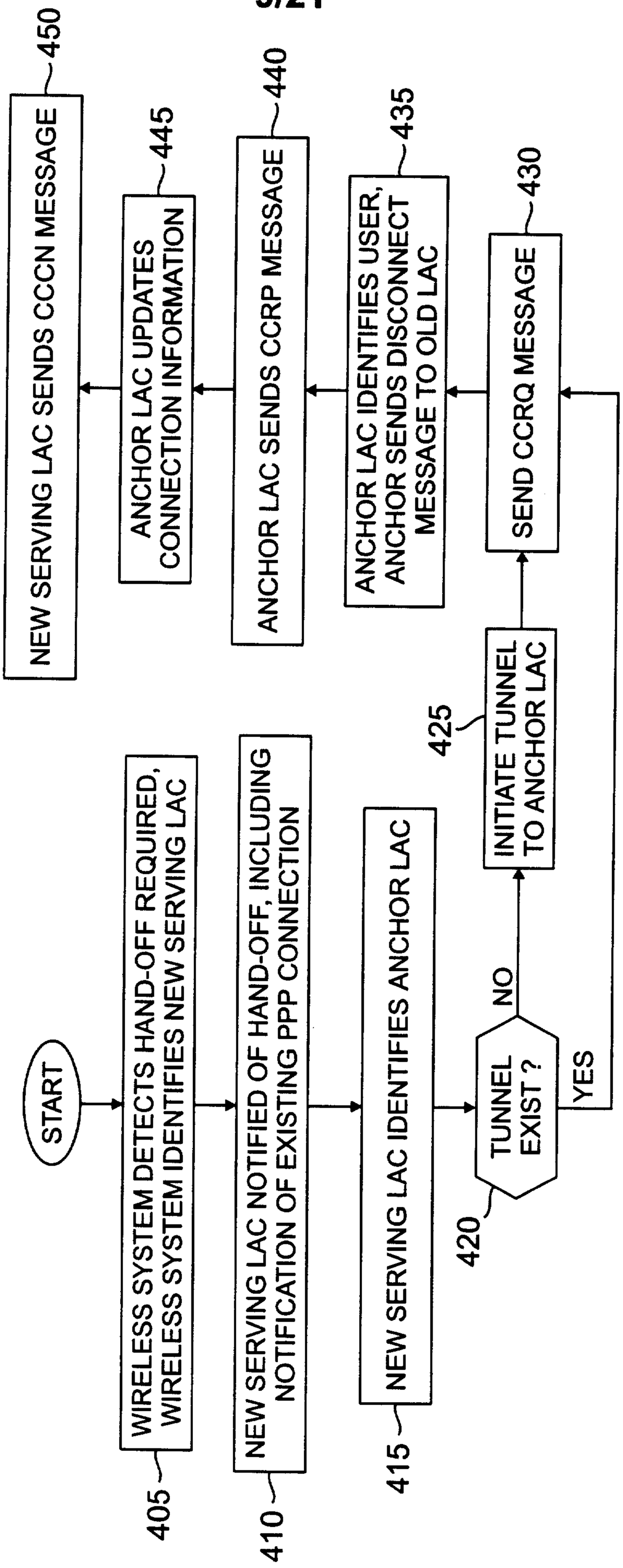

START
WIRELESS SYSTEM DETECTS HAND-OFF REQUIRED, WIRELESS SYSTEM IDENTIFIES NEW SERVING LAC
405
NEW SERVING LAC NOTIFIED OF HAND-OFF, INCLUDING NOTIFICATION OF EXISTING PPP CONNECTION
410
NEW SERVING LAC IDENTIFIES ANCHOR LAC
415
TUNNEL EXIST ?
420
NO
YES
INITIATE TUNNEL TO ANCHOR LAC
425
SEND CCRQ MESSAGE
430
ANCHOR LAC IDENTIFIES USER, ANCHOR SENDS DISCONNECT MESSAGE TO OLD LAC
435
ANCHOR LAC SENDS CCRP MESSAGE
440
ANCHOR LAC UPDATES CONNECTION INFORMATION
445
NEW SERVING LAC SENDS CCCN MESSAGE
450

FIG. 10

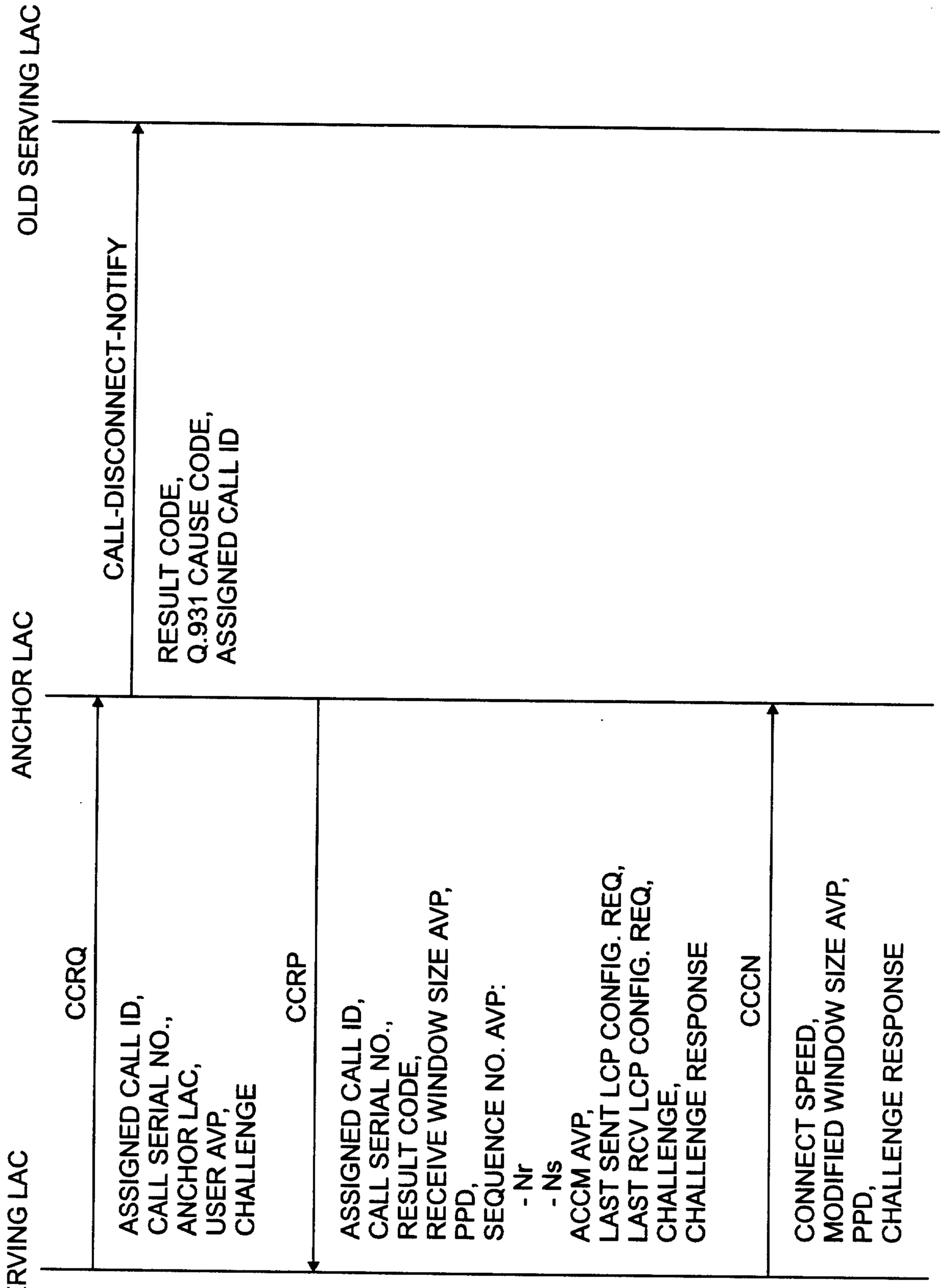

OLD SERVING LAC
ANCHOR LAC
CALL-DISCONNECT-NOTIFY
RESULT CODE,
Q.931 CAUSE CODE,
ASSIGNED CALL ID
NEW SERVING LAC
CCRQ
ASSIGNED CALL ID,
CALL SERIAL NO.,
ANCHOR LAC,
USER AVP,
CHALLENGE
CCRP
ASSIGNED CALL ID,
CALL SERIAL NO.,
RESULT CODE,
RECEIVE WINDOW SIZE AVP,
PPD,
SEQUENCE NO. AVP:
- Nr
- Ns
ACCM AVP,
LAST SENT LCP CONFIG. REQ,
LAST RCV LCP CONFIG. REQ,
CHALLENGE,
CHALLENGE RESPONSE
CCCN
CONNECT SPEED,
MODIFIED WINDOW SIZE AVP,
PPD,
CHALLENGE RESPONSE

FIG. 11

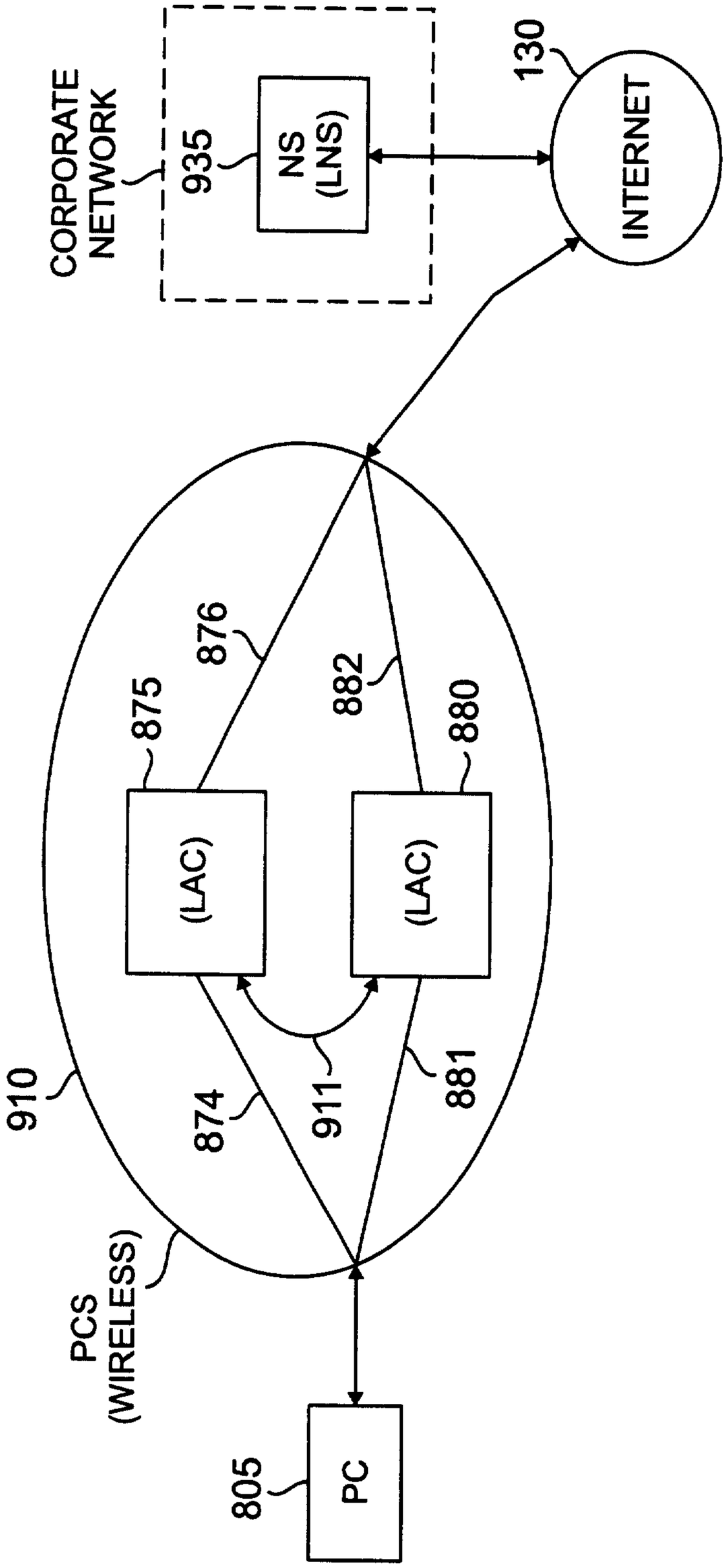

PC
805
PCS
(WIRELESS)
900
910
874
911
881
(LAC)
875
876
(LAC)
882
880
CORPORATE
NETWORK
935
NS
(LNS)
130
INTERNET

FIG. 12

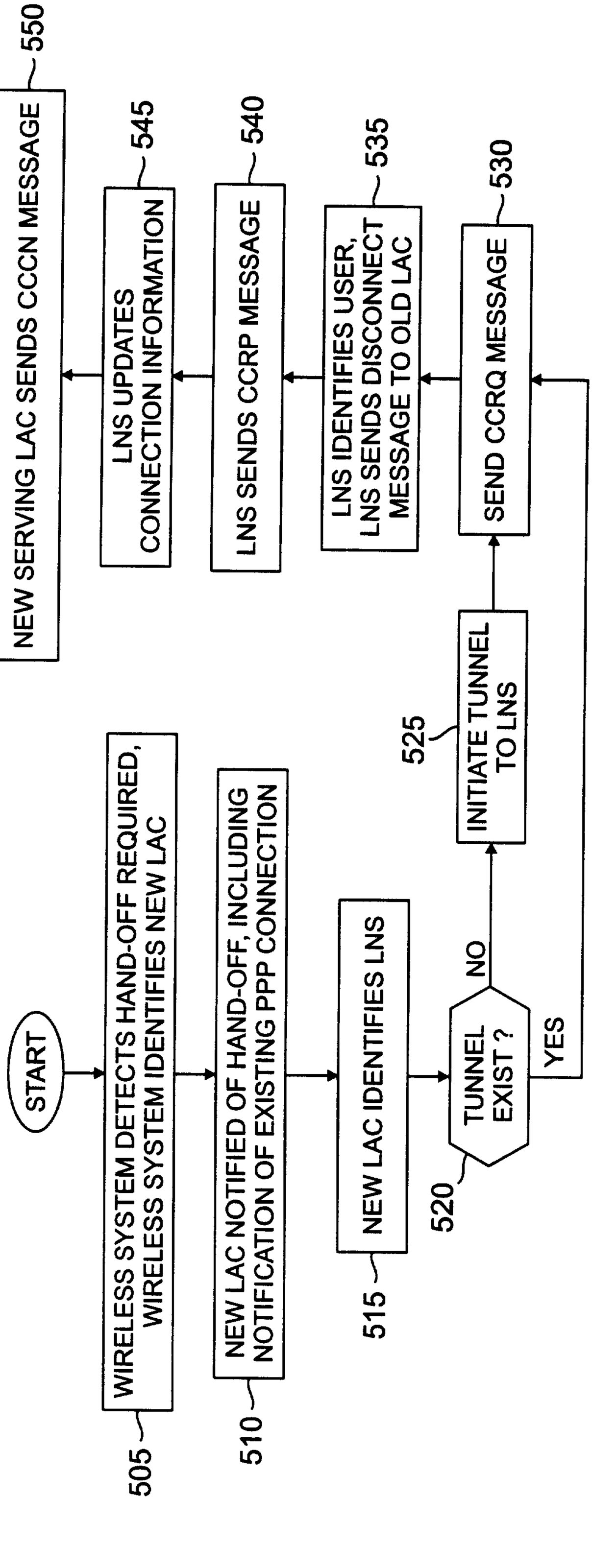

START
WIRELESS SYSTEM DETECTS HAND-OFF REQUIRED, WIRELESS SYSTEM IDENTIFIES NEW LAC
505
NEW LAC NOTIFIED OF HAND-OFF, INCLUDING NOTIFICATION OF EXISTING PPP CONNECTION
510
NEW LAC IDENTIFIES LNS
515
TUNNEL EXIST ?
520
NO
YES
INITIATE TUNNEL TO LNS
525
SEND CCRQ MESSAGE
530
LNS IDENTIFIES USER, LNS SENDS DISCONNECT MESSAGE TO OLD LAC
535
LNS SENDS CCRP MESSAGE
540
LNS UPDATES CONNECTION INFORMATION
545
NEW SERVING LAC SENDS CCCN MESSAGE
550

FIG. 14

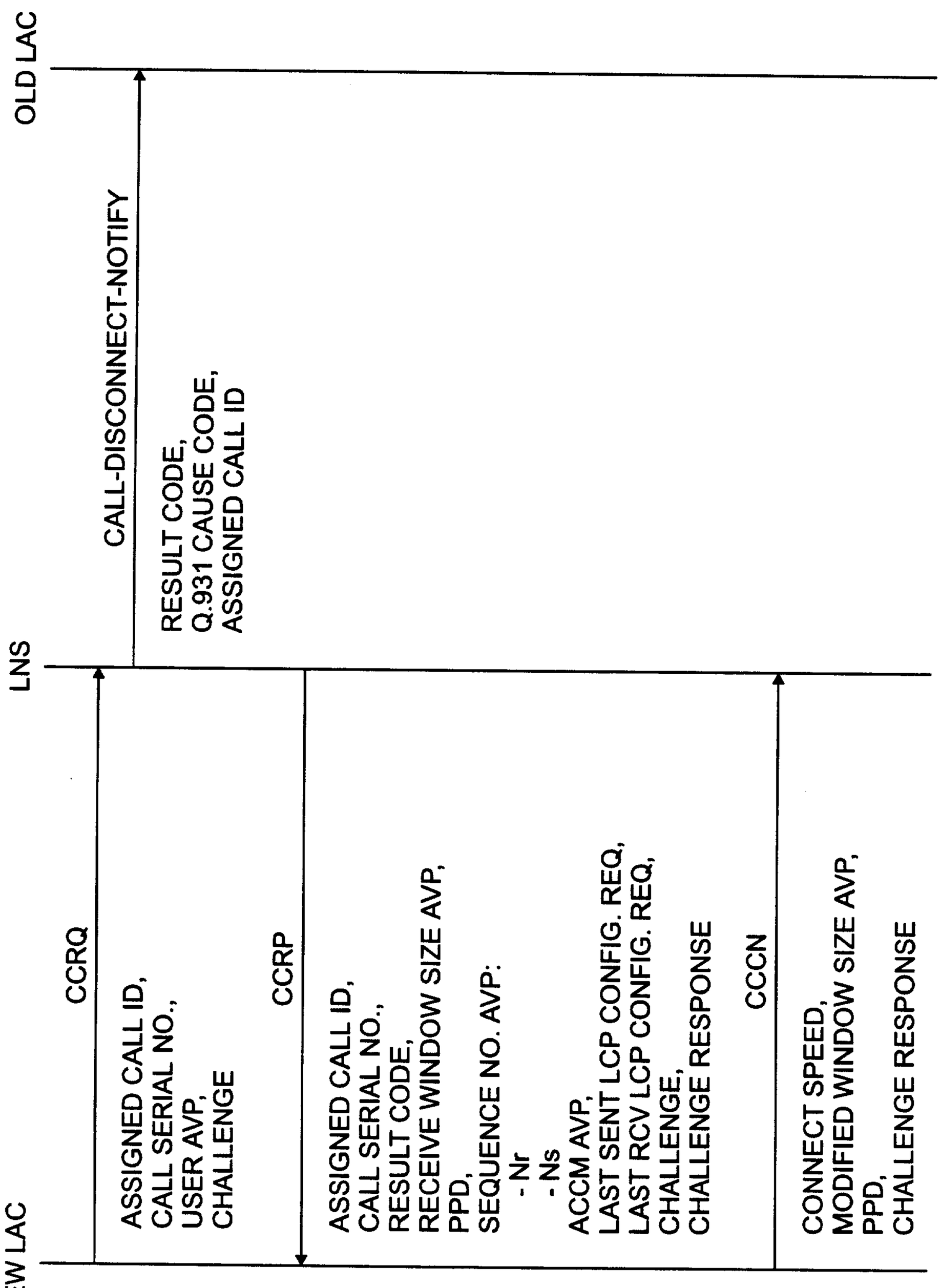

OLD LAC
LNS
NEW LAC
CALL-DISCONNECT-NOTIFY
RESULT CODE,
Q.931 CAUSE CODE,
ASSIGNED CALL ID
CCRQ
ASSIGNED CALL ID,
CALL SERIAL NO.,
USER AVP,
CHALLENGE
CCRP
ASSIGNED CALL ID,
CALL SERIAL NO.,
RESULT CODE,
RECEIVE WINDOW SIZE AVP,
PPD,
SEQUENCE NO. AVP:
- Nr
- Ns
ACCM AVP,
LAST SENT LCP CONFIG. REQ,
LAST RCV LCP CONFIG. REQ,
CHALLENGE,
CHALLENGE RESPONSE
CCCN
CONNECT SPEED,
MODIFIED WINDOW SIZE AVP,
PPD,
CHALLENGE RESPONSE

FIG. 15

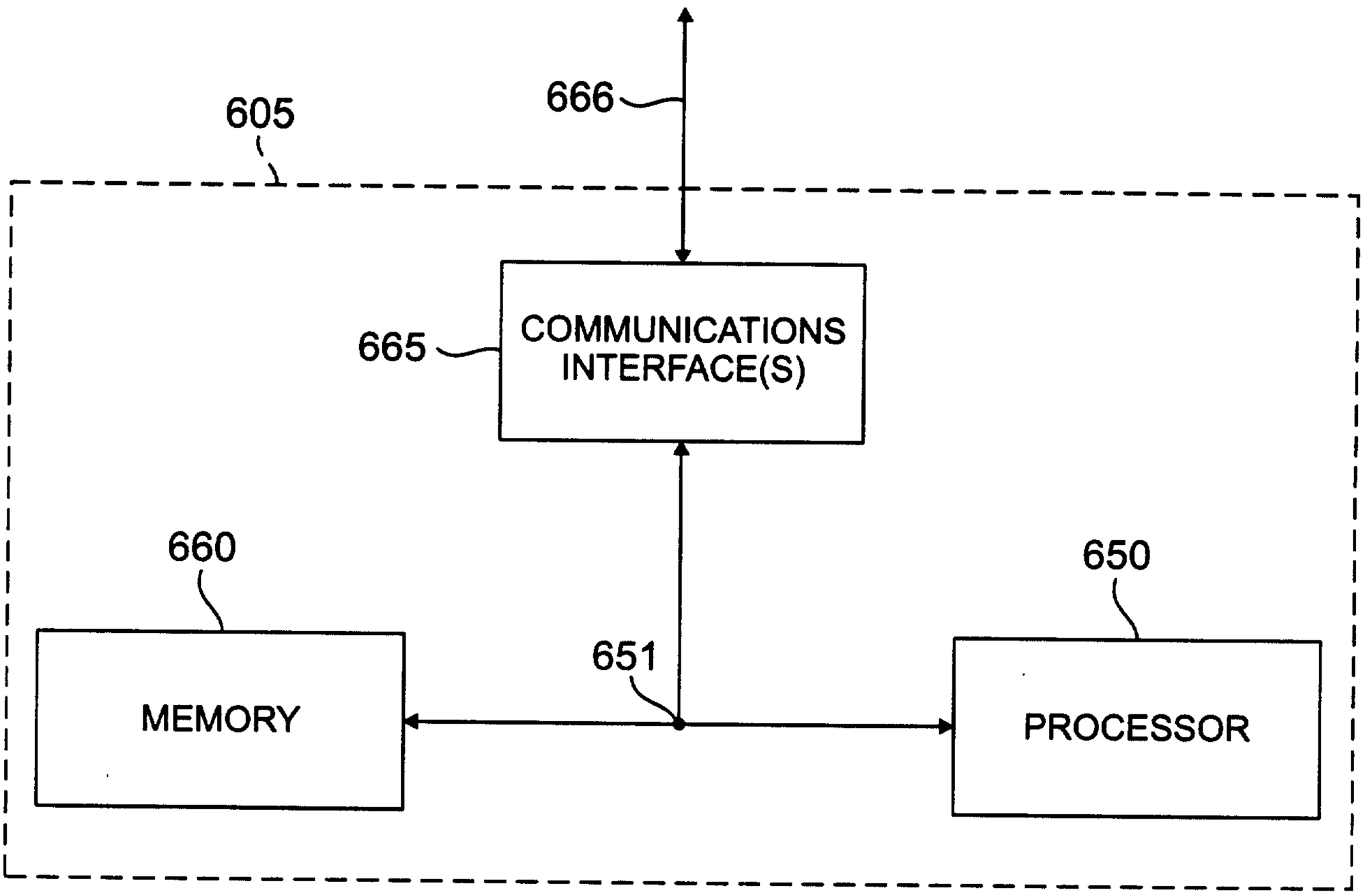

605
666
665
COMMUNICATIONS INTERFACE(S)
660
MEMORY
651
650
PROCESSOR

FIG. 16

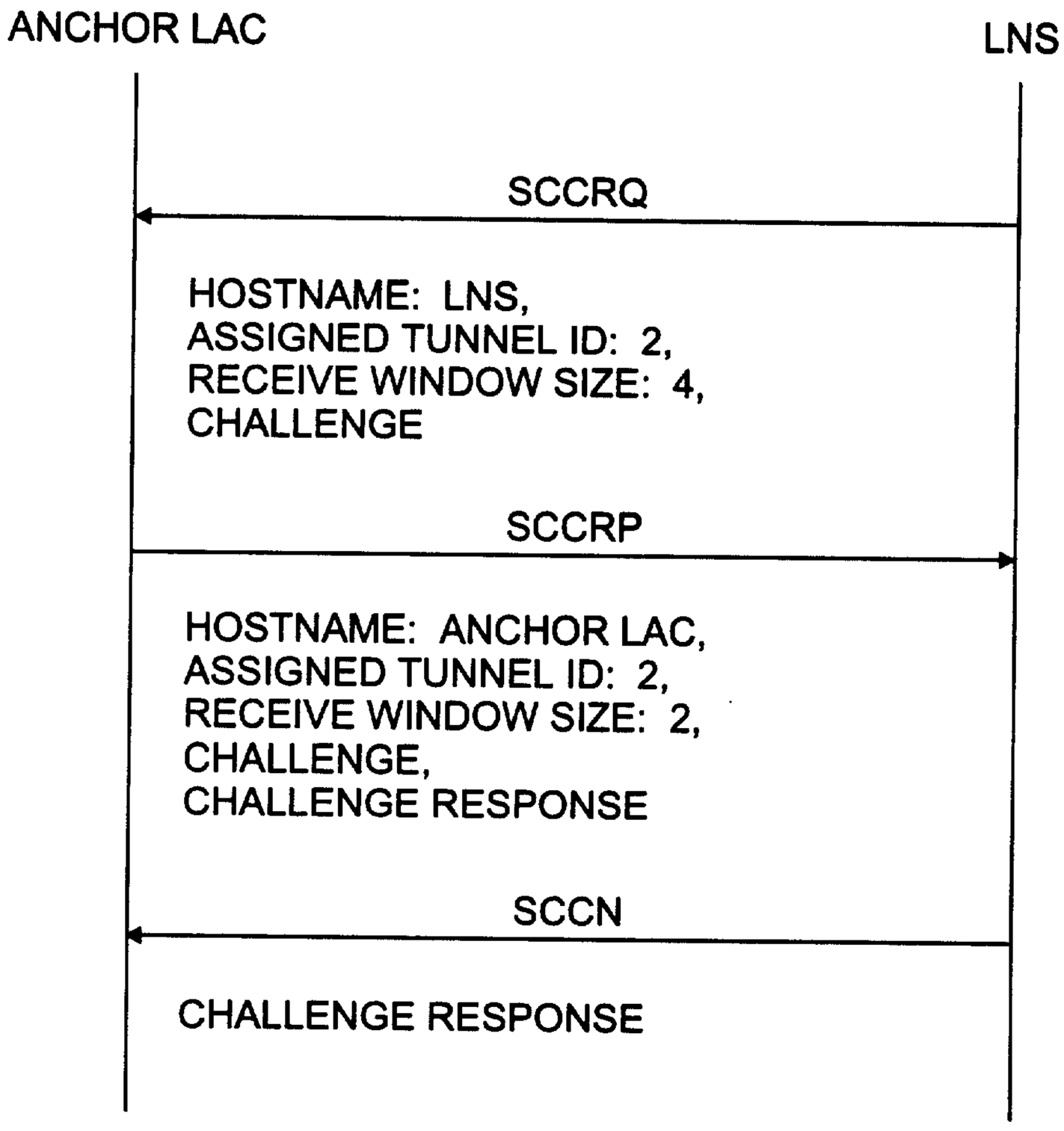

ANCHOR LAC
LNS
SCCRQ
HOSTNAME: LNS,
ASSIGNED TUNNEL ID: 2,
RECEIVE WINDOW SIZE: 4,
CHALLENGE
SCCRP
HOSTNAME: ANCHOR LAC,
ASSIGNED TUNNEL ID: 2,
RECEIVE WINDOW SIZE: 2,
CHALLENGE,
CHALLENGE RESPONSE
SCCN
CHALLENGE RESPONSE

FIG. 17

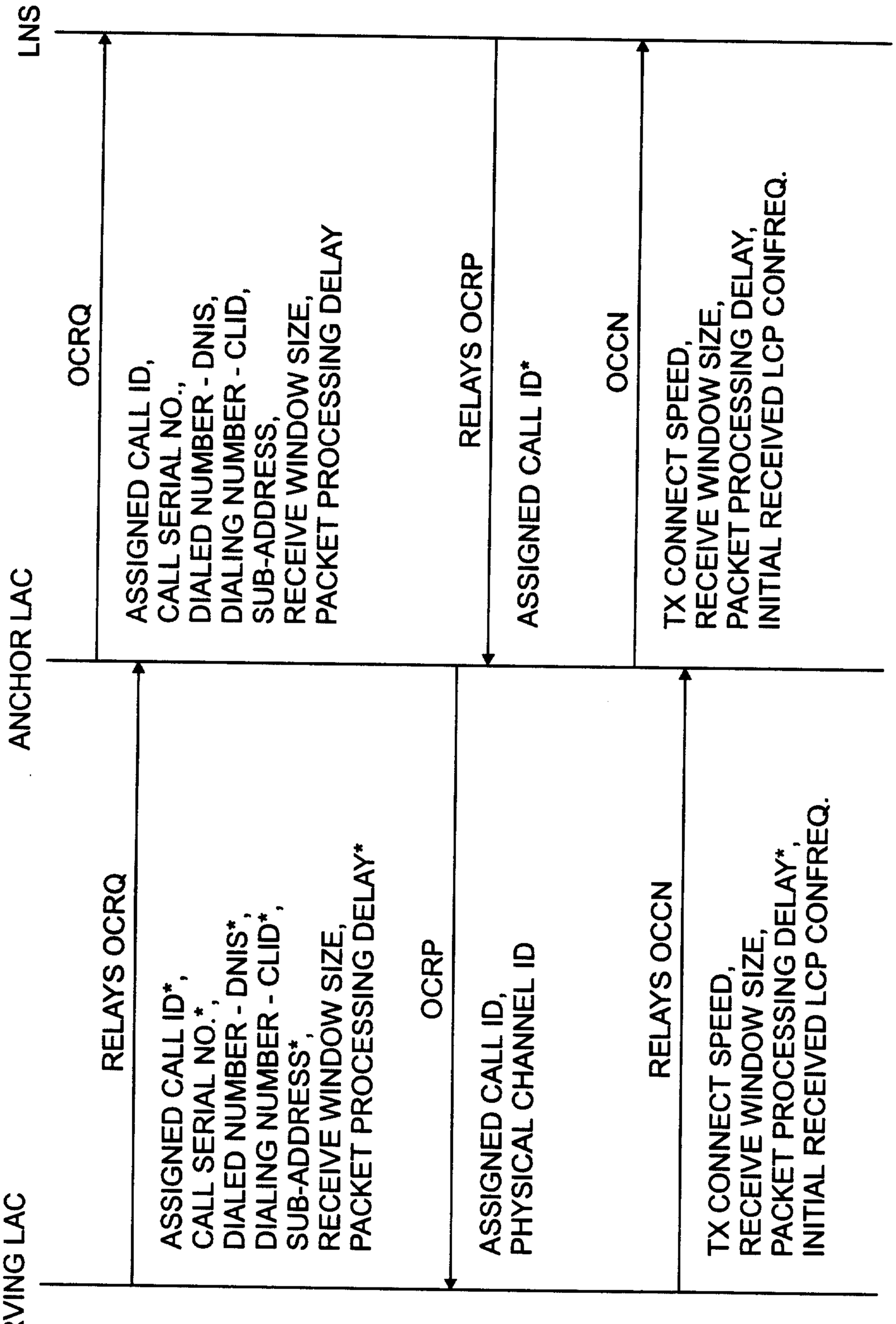

SERVING LAC
ANCHOR LAC
LNS
RELAYS OCRQ
ASSIGNED CALL ID*,
CALL SERIAL NO.*,
DIALED NUMBER - DNIS*,
DIALING NUMBER - CLID*,
SUB-ADDRESS*,
RECEIVE WINDOW SIZE,
PACKET PROCESSING DELAY*
OCRQ
ASSIGNED CALL ID,
CALL SERIAL NO.,
DIALED NUMBER - DNIS,
DIALING NUMBER - CLID,
SUB-ADDRESS,
RECEIVE WINDOW SIZE,
PACKET PROCESSING DELAY
OCRP
ASSIGNED CALL ID,
PHYSICAL CHANNEL ID
RELAYS OCRP
ASSIGNED CALL ID*
OCCN
TX CONNECT SPEED,
RECEIVE WINDOW SIZE,
PACKET PROCESSING DELAY,
INITIAL RECEIVED LCP CONFREQ.
RELAYS OCCN
TX CONNECT SPEED,
RECEIVE WINDOW SIZE,
PACKET PROCESSING DELAY*,
INITIAL RECEIVED LCP CONFREQ.

FIG. 18

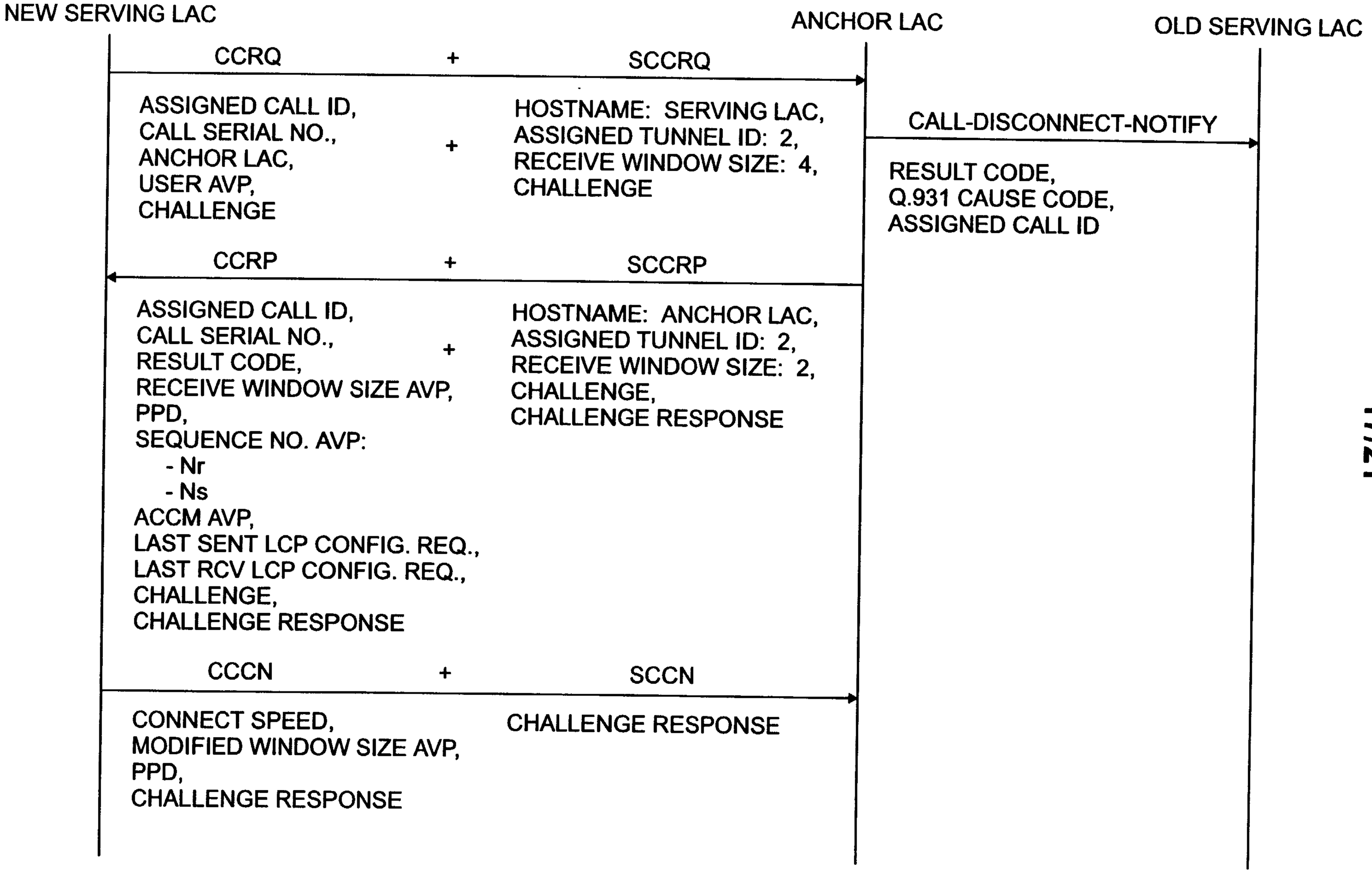


FIG. 19

CA 02279667 1999-08-05

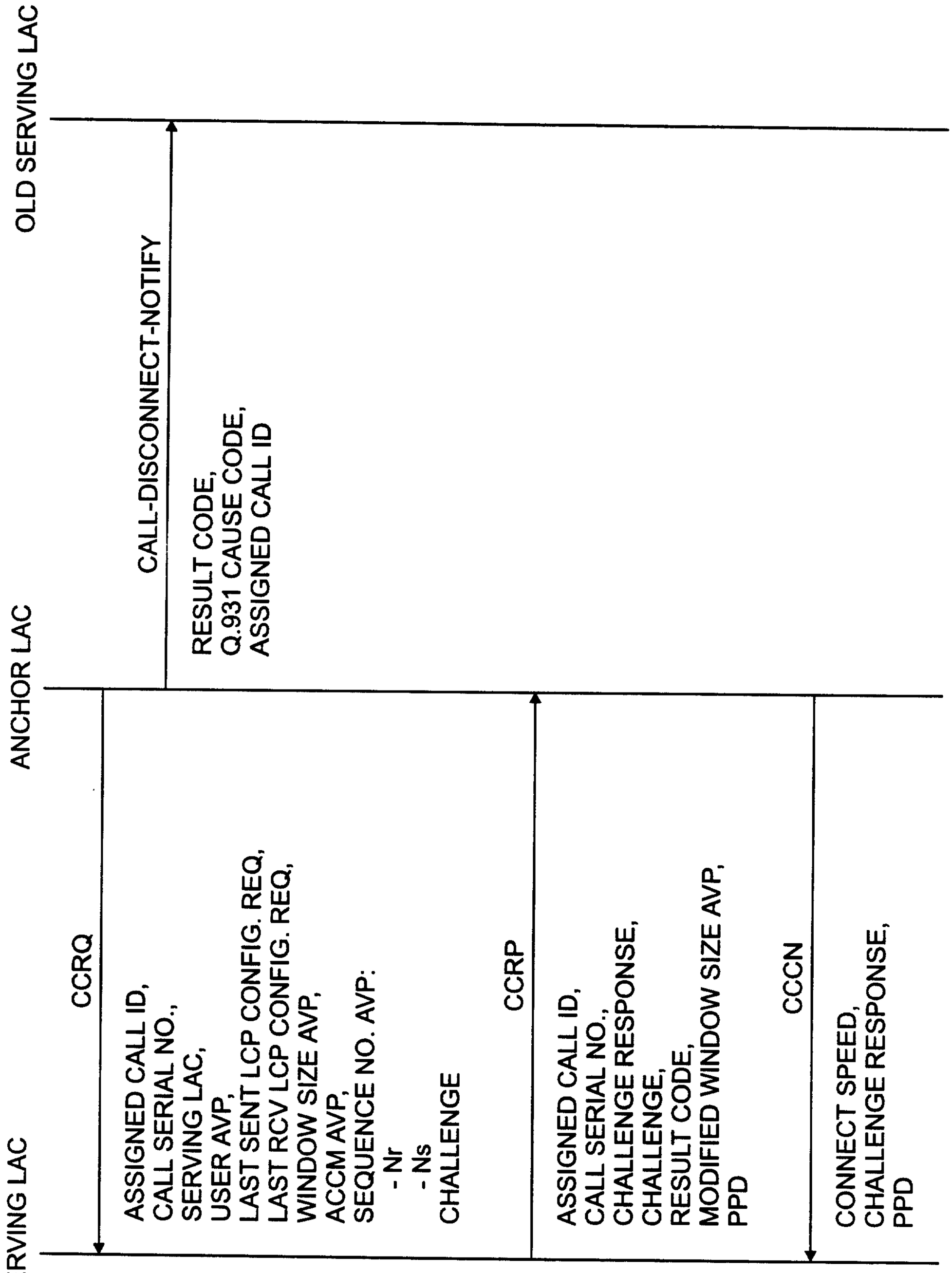

NEW SERVING LAC
ANCHOR LAC
OLD SERVING LAC
CCRQ
ASSIGNED CALL ID,
CALL SERIAL NO.,
SERVING LAC,
USER AVP,
LAST SENT LCP CONFIG. REQ,
LAST RCV LCP CONFIG. REQ,
WINDOW SIZE AVP,
ACCM AVP,
SEQUENCE NO. AVP:
- Nr
- Ns
CHALLENGE
CCRP
ASSIGNED CALL ID,
CALL SERIAL NO.,
CHALLENGE RESPONSE,
CHALLENGE,
RESULT CODE,
MODIFIED WINDOW SIZE AVP,
PPD
CCCN
CONNECT SPEED,
CHALLENGE RESPONSE,
PPD
CALL-DISCONNECT-NOTIFY
RESULT CODE,
Q.931 CAUSE CODE,
ASSIGNED CALL ID

FIG. 20

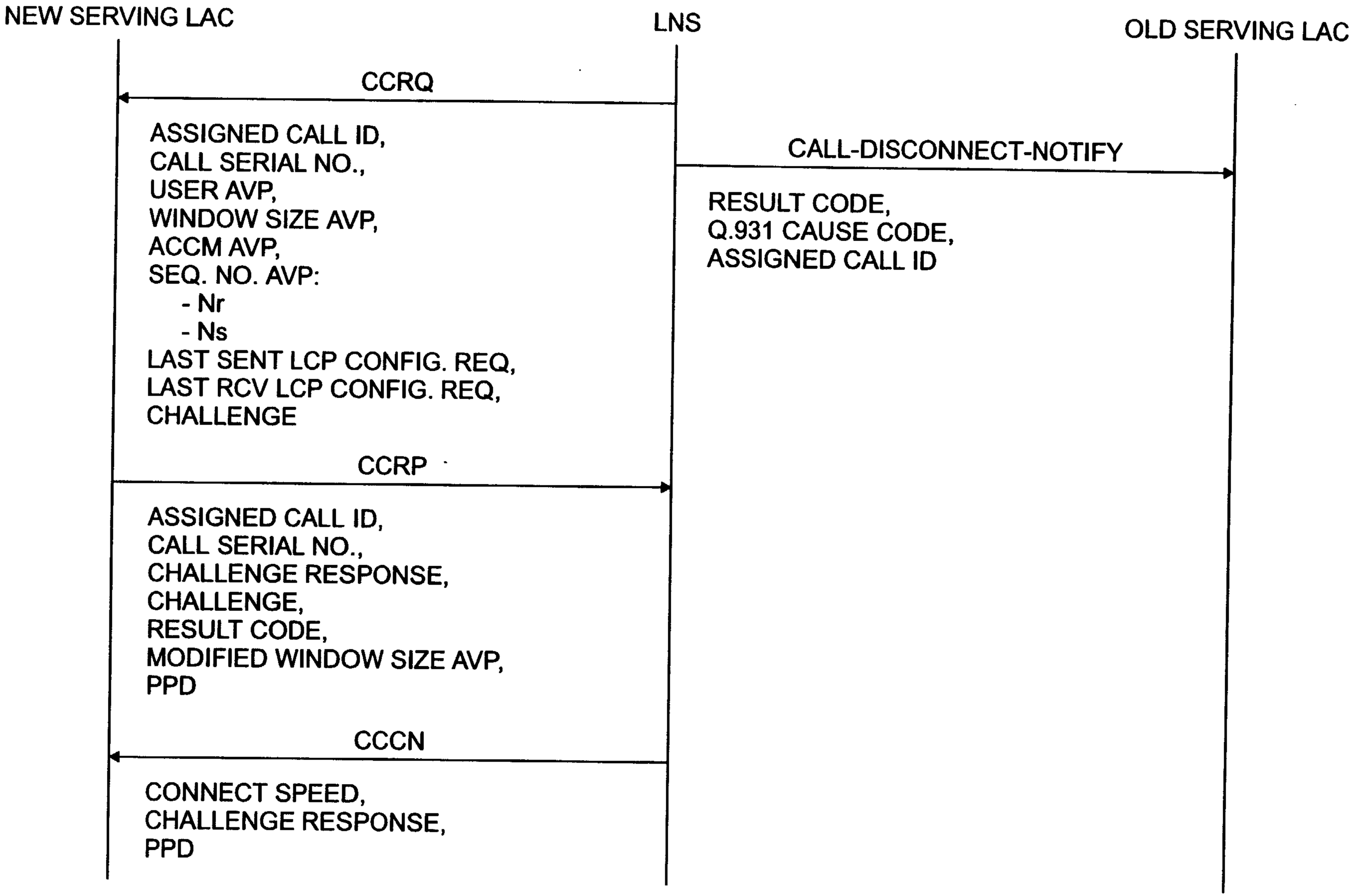


FIG. 21

CA 02279667 1999-08-05

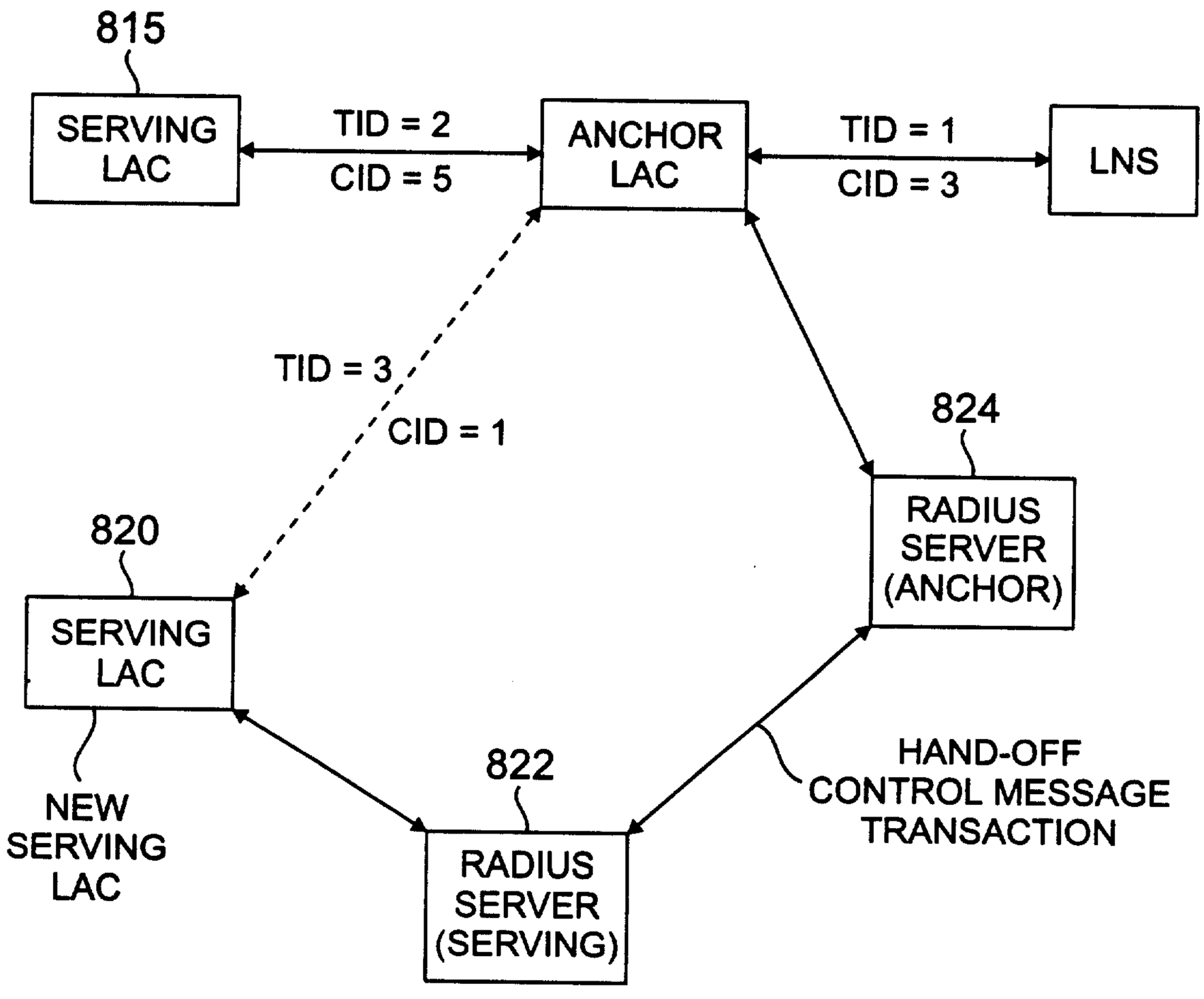

815
SERVING LAC
TID = 2
CID = 5
ANCHOR LAC
TID = 1
CID = 3
LNS
TID = 3
CID = 1
824
RADIUS SERVER (ANCHOR)
820
SERVING LAC
NEW SERVING LAC
822
RADIUS SERVER (SERVING)
HAND-OFF CONTROL MESSAGE TRANSACTION

FIG. 22

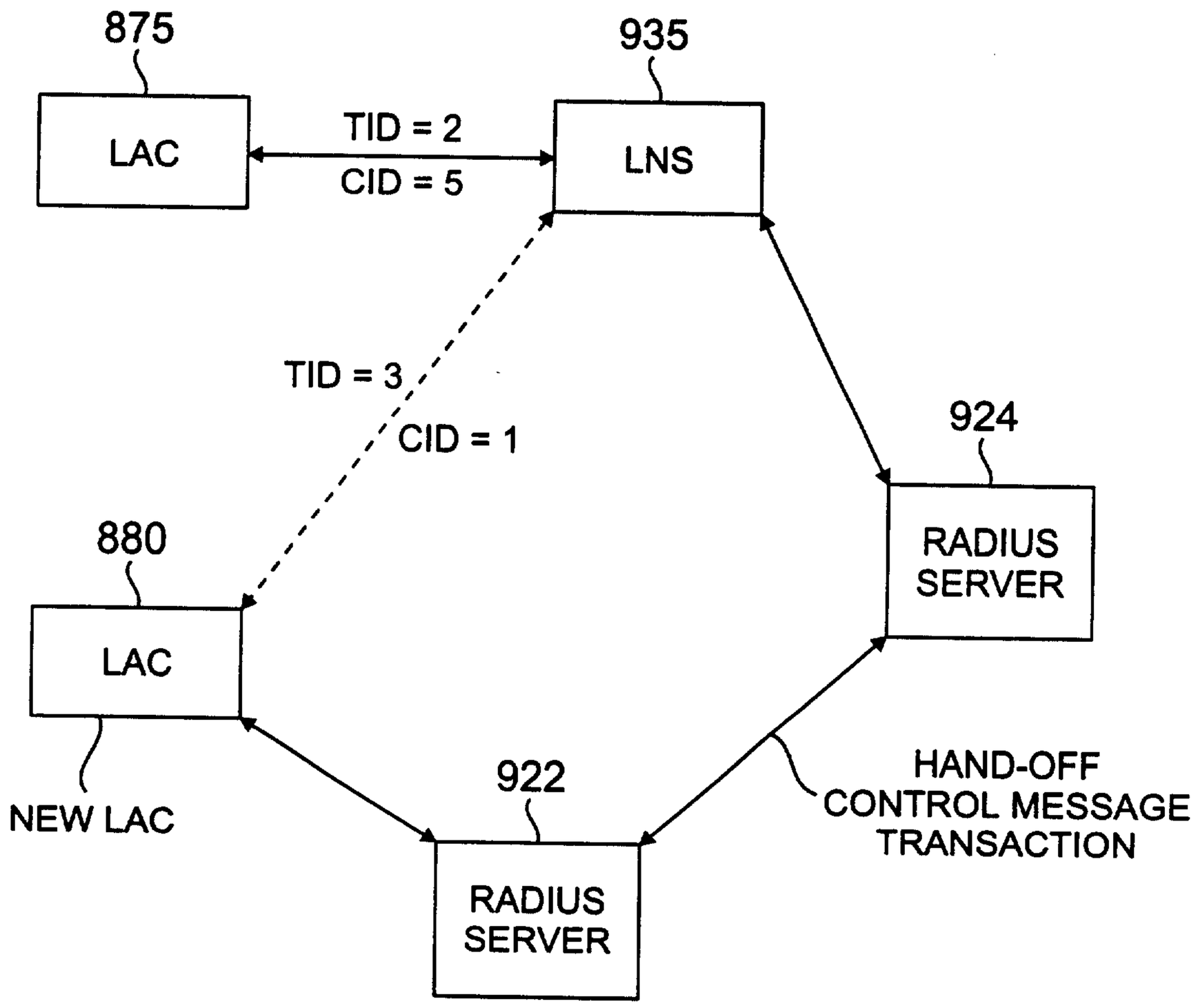

875
935
LAC
TID = 2
CID = 5
LNS
TID = 3
CID = 1
924
RADIUS SERVER
880
LAC
NEW LAC
922
RADIUS SERVER
HAND-OFF CONTROL MESSAGE TRANSACTION

FIG. 23