(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 699 34 734 T2** 2007.10.11

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 955 746 B1**
(21) Deutsches Aktenzeichen: **699 34 734.3**
(96) Europäisches Aktenzeichen: **99 303 275.4**
(96) Europäischer Anmeldetag: **27.04.1999**
(97) Erstveröffentlichung durch das EPA: **10.11.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **10.01.2007**
(47) Veröffentlichungstag im Patentblatt: **11.10.2007**

(51) Int Cl.[8]: ***H04L 12/46*** (2006.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 29/12 (2006.01)

(30) Unionspriorität:
74745 **08.05.1998** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Lucent Technologies Inc., Murray Hill, N.J., US

(74) Vertreter:
derzeit kein Vertreter bestellt

(72) Erfinder:
Chuah, Mooi Choo, Eatontown, New Jersey 07724, US; Girish, Rai, Bartlett, Illinois 60103, US

(54) Bezeichnung: **Mehrstrecken Punkt-zu-Punkt Protokoll**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

Erfindungsgebiet

[0001] Die vorliegende Erfindung betrifft allgemein die Kommunikation und insbesondere Paketkommunikationssysteme.

Stand der Technik

[0002] Eine Anwendung des Internets als Kommunikationsmittel ist als erweiterter Datenbackbone zum Zusammenkoppeln von Arbeitsgruppen zur Bereitstellung von einem sogenannten „virtuellen Privatnetz" (VPN). Eine Anwendung eines VPN ist in einer Firmenumgebung, so daß Angestellte beispielsweise zu Hause aus der Ferne über das Internet auf Firmendatennetze zugreifen können. Ein VPN bietet Sicherheit und Authentifizierung für einen entfernten Benutzer, so daß er ungeachtet der Verwendung öffentlicher Einrichtungen an einer geschlossenen Benutzergruppe teilnehmen kann. Im Effekt stellt die Verwendung eines VPN der Firma und ihren Angestellten ein WAN-ähnliches Mittel bereit. (Obwohl das Firmennetz auch direkten Fernzugriff bereitstellen könnte, beispielsweise wählt sich ein Benutzer direkt in das Firmennetz ein, gibt es wirtschaftliche Vorteile für die Verwendung eines VPN.)

[0003] Zur Bereitstellung eines VPN werden Tunnelprotokolle wie beispielsweise das „Punkt-zu-Punkt-Tunnelprotokoll" (PPTP – Point-to-Point Tunneling Protocol) und das „Schicht-2-Weiterleitungs"-(L2F – Layer 2 Forwarding)-Protokoll benutzt. Allgemein gesagt ermöglicht ein Tunnelprotokoll die Erstellung eines privaten Datenstroms über ein öffentliches Netz, indem es ein Paket in ein anderes plaziert. Im Zusammenhang mit einem VPN wird ein IP-Paket in ein anderes IP-Paket plaziert. In einem Versuch zur Entwicklung eines Industriestandards entwickelt die IETF (Internet Engineering Task Force) das „Schicht-2-Tunnelprotokoll" (L2TP – Layer 2 Tunneling Protocol), das einen Hybrid der PPTP- und L2F-Protokolle darstellt (z.B. siehe K. Hamzeh, T. Kolar, M. Littlewood, G. Singh Pall, J. Taarud, A. J. Valencia, W. Verthein; „Layer Two Tunneling Protocol L2TP" (Schicht-2-Tunnelprotokoll), Internetentwurf, März 1998).

[0004] Für einen entfernten Benutzer besteht eine typische Zugriffsform auf ein VPN über eine herkömmliche Telefondienstverbindung mit einem „Internet-Diensteanbieter" (ISP – Internet Service Provider), der den VPN-Dienst bereitstellt. Beispielsweise wird von einem Benutzer ein Analogmodem in einen Personal Computer oder dergleichen eingebaut, und er besitzt ein Kundenkonto bei einem bestimmten ISP, der hier als „Heimat"-ISP bezeichnet wird (auch wird angenommen, daß der Personal Computer des Benutzers ordnungsgemäß zur Unterstützung eines der obenerwähnten Tunnelprotokolle konfiguriert ist.) Der Benutzer greift auf das VPN zu, indem er einfach eine Datenverbindung mit dem Heimat-ISP herstellt, z.B. eine dem „Heimat"-ISP zugeordnete Telefonnummer wählt und sich dann in das VPN „einloggt".

[0005] Von Malkin Gary Scott: „Dial-In Virtual Private Networks Using Layer 3 Tunneling" (Virtuelle private Einwählnetze unter Verwendung von Schicht-3-Tunnelung), Proceedings of the Conference on Local Computer Networks, 2. November 1997 (1997-11-02), Seiten 555-561, wird eine auf Mobile IP basierende Konstruktion für einen virtuellen privaten Einwählnetz-Dienst der Schicht 3 (DVS – Dial-In Virtual Private Network Service) geboten.

Kurze Beschreibung der Erfindung

[0006] Ein Verfahren und eine Vorrichtung gemäß der Erfindung entsprechen den unabhängigen Ansprüchen. Bevorzugte Ausführungsformen sind in den abhängigen Ansprüchen aufgeführt.

[0007] Es ist festgestellt worden, daß die oben beschriebenen Tunnelprotokolle einem fernen Benutzer nicht erlauben, sich in irgendeinen anderen ISP als ihren Heimat-ISP zum Zugreifen auf ein VPN einzuloggen. In der mobilen Welt von heute wirkt dies bedeutend begrenzend, besonders, wenn es im Zusammenhang mit einer drahtlosen PCS-Umgebung (Personal Communication Service) betrachtet wird, in der ein Benutzer seinen Standort physikalisch während des Anrufs verändern kann. Anders gesagt könnte der Heimat-ISP bei Veränderung des Standorts durch den entfernten Benutzer mindestens zeitweilig dem Benutzer nicht länger zur Verfügung stehen und blockiert daher den Zugriff des Benutzers auf das VPN.

[0008] Daher wird erfindungsgemäß von einem Paketserver ein Mehrstreckentunnel zwischen anderen Paketendpunkten hergestellt und Nachrichten zwischen Teilen des Mehrstreckentunnels weitergeleitet. So kann ein entfernter Benutzer auf ein VPN über einen Besuchs-ISP zusätzlich zu seinem Heimat-ISP zugreifen.

[0009] Bei einer Ausführungsform der Erfindung wird ein virtueller Wähldienst über mehrere ISP (Internet Service Providers) bereitgestellt. Insbesondere greift ein entfernter Benutzer durch Herstellen einer Verbindung zu einem versorgenden ISP auf den virtuellen Wähldienst zu. Vom versorgenden ISP wird ein erster Tunnel zu einem Anker-ISP hergestellt. Vom letzteren wird ein Tunnel beispielsweise zu einem privaten Intranet hergestellt. Als Ergebnis wird ein VPN-Dienst (Virtual Private Network) bereitgestellt, der Fernzugriff auf ein Privatnetz über mehrere Tunnel ermöglicht.

Kurze Beschreibung der Zeichnung

[0010] Fig. 1 zeigt ein Kommunikationssystem gemäß den Grundsätzen der Erfindung;

[0011] Fig. 2-Fig. 3 zeigen Flußdiagramme von beispielhaften Verfahren zur Verwendung in dem Kommunikationssystem der Fig. 1;

[0012] Fig. 4 zeigt einen beispielhaften Mehrstrecken-Nachrichtenfluß;

[0013] Fig. 5-Fig. 7 zeigen beispielhafte Steuernachrichtentransaktionen;

[0014] Fig. 8 zeigt eine weitere Ausführungsform eines Kommunikationssystems gemäß den Grundsätzen der Erfindung;

[0015] Fig. 9 zeigt einen beispielhaften Weiterschaltungs-Nachrichtenfluß;

[0016] Fig. 10 zeigt ein Flußdiagramm eines beispielhaften Verfahrens zur Verwendung in dem Kommunikationssystem der Fig. 8;

[0017] Fig. 11 zeigt beispielhafte Steuernachrichtentransaktionen;

[0018] Fig. 12 zeigt eine weitere Ausführungsform eines Kommunikationssystems gemäß den Grundsätzen der Erfindung;

[0019] Fig. 13 zeigt einen beispielhaften Weiterschaltungs-Nachrichtenfluß;

[0020] Fig. 14 zeigt ein Flußdiagramm eines beispielhaften Verfahrens zur Verwendung in dem Kommunikationssystem der Fig. 12;

[0021] Fig. 15 zeigt beispielhafte Steuernachrichten-Transaktionen;

[0022] Fig. 16 zeigt ein beispielhaftes höheres Blockdiagramm des Netzzugangsservers; und

[0023] Fig. 17-Fig. 18 zeigen beispielhafte Steuernachrichten-Transaktionen für abgehende Verbindungen.

Mehrstrecken-Punkt-zu-Punkt-Protokoll

[0024] Fig. 1 zeigt ein beispielhaftes Kommunikationssystem **100** gemäß den Grundsätzen der Erfindung. Außer dem erfinderischen Konzept sind die Elemente wohlbekannt und werden nicht ausführlich beschrieben. Beispielsweise enthält der Personal Computer (PC) **110** (nicht gezeigtes) Datenkommunikationsgerät für Wählzugang über das öffentliche Wählnetz (PSTN) **110** zum ISP B zum Herstellen einer Internet-Verbindung. Gleicherweise stellen die durchgezogenen Linien zwischen Elementen des Kommunikationssystems **100** wohlbekannte Kommunikationseinrichtungen zwischen den jeweiligen Endpunkten dar, z.B. stellt die Verbindung zwischen PC **110** und PSTN **110** eine Ortsanschlußverbindung dar, die Verbindung zwischen ISP B und Internet **120** wird durch ATM (Asynchronous Transfer Mode) über ein synchrones optisches Netz (SONET) unterstützt, usw. Weiterhin wird angenommen, daß dem Leser das oben erwähnte L2TP-Protokoll bekannt ist.

[0025] Wie aus Fig. 1 ersichtlich, umfaßt das Kommunikationssystem **100** zwei ISP: ISP A, vertreten durch Netz ISP A, und ISP B, vertreten durch Netz ISP B. Das Netz ISP B umfaßt den Netzzugangsserver (NAS – Network Access Server) **115**, der einen (nicht gezeigten) POP-Router (Point of Presence – Zugriffspunkt) auf dem Stand der Technik, ein Ortsnetz **120** und einen Router **125** enthält. Auf ähnliche Weise umfaßt das Netz ISP A den NAS **155**, ein Ortsnetz **160** und einen Router **165**. Es wird angenommen, daß ISP A einen VPN-Dienst für entfernte Angestellte zum Zugreifen auf ein beispielhaftes Firmennetz über den Netzserver

(NS) **135** bereitstellt, der unter anderen Funktionen eine Routing- und Firewall-Fähigkeit bereitstellt. (Es wird angenommen, daß das Firmennetz beispielsweise eine Ansammlung von (nicht gezeigten) Ortsnetzen ist, die auf geeignete Weise hinter dem NS **135** geschützt sind.)

[0026] Es ist festgestellt worden, daß ein entfernter Benutzer sich auch nur zeitweilig in einem Teil des Landes befinden kann, der nicht von ISP A versorgt wird, sondern statt dessen von ISP B versorgt wird. Weiterhin kann der ISP A wünschen, diese VPN-Versorgung auf andere Bereiche auszudehnen. Daher und gemäß den Grundsätzen der Erfindung kann ein entfernter Benutzer auf ein VPN über einen Besuchs- oder versorgenden ISP zusätzlich zu seinem Heimat- oder Anker-ISP zugreifen. (Obwohl angenommen wird, daß ISP A und ISP B verschiedene Diensteanbieter sind, ist dies für das erfinderische Konzept nicht notwendig, beispielsweise könnten sie einfach getrennte Netze im gleichen ISP sein.) So kann ein (nicht gezeigter) Benutzer, der sich am PC **105** befindet, auf das Firmennetz zugreifen, während er beispielsweise im Land herumreist.

[0027] An dieser Stelle werden folgende Definitionen angenommen:
mL2TP – das L2TP-Protokoll nach Definition bei K. Hamzeh, T. Kolar, M. Littlewood, G. Singh Pall, J. Taarud, A. J. Valencia, W. Verthein; Layer Two Tunneling Protocol „L2TP" (Schicht-2-Tunnelprotokoll L2TP); Internetentwurf, März 1998; zuzüglich hier beschriebener Abänderungen;
LAC – mL2TP Access Control (mL2TP-Zugangssteuerung), d.h. ein mL2TP unterstützender NAS;
LNS – ein mL2TP unterstützender NS;
Anker-LAC – Eine LAC, die Tunneln zum LNS zur Bereitstellung eines VPN-Dienstes unterstützt, und Versorgende LAC – eine LAC, die Tunneln zur Anker-LAC unterstützt.

[0028] (Diese Definitionen werden zum Vereinfachen einer beispielhaften Beschreibung des erfinderischen Konzepts benutzt. Als solche ist das erfinderische Konzept nicht darauf begrenzt, was auch vom Fachmann erkannt werden wird, und kann auf jedes Tunnelprotokoll und zugehörige Verarbeitungseinrichtung angewandt werden.)

[0029] Gemäß dem erfinderischen Konzept stellt das Netz ISP A eine Anker-LAC **155** dar, und das Netz ISP B stellt eine versorgende LAC **115** dar. Wie weiter unten beschrieben und gemäß den Grundsätzen der Erfindung wird durch das Kommunikationssystem **100** der Fig. 1 ein Mehrstreckentunnel bereitgestellt. Das Beispiel der Fig. 1 zeigt einen Zweistrecken-Tunnel. Eine Strecke ist vom Netz ISP B zum Netz ISP A und die andere Strecke ist vom Netz ISP A zum Firmennetz.

[0030] Es ist nunmehr auf Fig. 2 Bezug zu nehmen, die ein beispielhaftes höheres Flußdiagramm eines Verfahrens gemäß den Grundsätzen der Erfindung zeigt. (Es wird angenommen, daß die versorgende LAC **115** und die anderen jeweiligen Server auf geeignete Weise programmiert sind, um die unten beschriebenen Verfahren unter Verwendung herkömmlicher Programmierungsverfahren auszuführen, die als solche hier nicht beschrieben werden.) Im Schritt **205** wird vom entfernten Benutzer eine PPP-Verbindung (Point-to-Point Protocol) zum ISP B über das PSTN **110** eingeleitet. Im Schritt **210** wird von der versorgenden LAC **115** der Benutzer teilweise authentifiziert (z.B. unter Verwendung eines vordefinierten „Benutzernamens" und „Paßworts") und die (durch gestrichelte Linie 1 der Fig. 1 dargestellte) Verbindung angenommen. (Als Alternative könnte DNIS (Dialed Number Identification Service – Wählnummeridentifikationsdienst), CLID (Calling Line Identification – Anruferidentifikation) oder eine sonstige gleichwertige Identifikationsform benutzt werden.) Natürlich wird die Verbindung nicht angenommen, wenn die versorgende LAC **115** den Benutzer nicht identifizieren kann (dieser Schritt ist nicht dargestellt).

[0031] (Als Hintergrund und nach dem Stand der Technik wird, wenn ein entfernter Benutzer eine neue PPP-Sitzung herstellen möchte, vom PC **110** eine PPP LCP Konfigurationsanforderung (Link Control Protocol) an die versorgende LAC eingeleitet. Von der versorgenden LAC werden beide Phasen PPP LCP und PPP PAP/CHAP nach dem Stand der Technik mit dem Benutzergerät abgeschlossen, ehe irgendeine Kommunikation mit der Anker-LAC gemäß dem erfinderischen Konzept eingeleitet wird. (Für sichere Leitungsführung sind von IETF zwei Protokolle für Sicherheit über PPP-Verbindungen definiert worden – das PAP (Password Authentication Protocol – Paßwortauthentifizierungsprotokoll) und das CHAP (Challenge Handshake Authentication Protocol – Abfrage-Quittungs-Authentifizierungsprotokoll) (z.B. siehe IETF RFC **1334**, „PPP Authentication Protocols" (PPP-Authentifizierungsprotokolle))

[0032] Im Schritt **215** bestimmt die versorgende LAC **115**, ob der entfernte Benutzer einen VPN Dienst zu benutzen wünscht (diese Auswahl könnte beispielsweise direkt mit bestimmten „Benutzernamen" verbunden sein und/oder mit einer getrennten Anforderung vom Benutzer, z.B. über ein von der versorgenden LAC **115** bereitgestelltes Popup-http-Formular (Hypertext Transport Protokoll) verbunden sein.) Wenn der entfernte Benutzer

keinen virtuellen Wähldienst anfordert, wird von der versorgenden LAC **115** Standard-Internetzugriff im Schritt **220** bereitgestellt. Wenn der entfernte Benutzer jedoch ein VPN zu benutzen wünscht, dann wird von der versorgenden LAC **115** eine zugeordnete Anker-LAC im Schritt **225** identifiziert (unten beschrieben).

[0033] Von der versorgenden LAC **115** wird eine VPN-Tabelle gespeichert, die a priori z.B. die Identifikation eines Benutzers mit einer bestimmten Anker-LAC zuordnet. Ein Teil einer solchen Tabelle wird unten in Tabelle 1 gezeigt. In diesem Beispiel wird der dem PC **110** zugeordnete entfernte Benutzer der Anker-LAC ISPA.com, d.h. Anker-LAC **155** zugeordnet.

Benutzeridentifikation	Anker-LAC
Benutzername	ISPA.com

Tabelle 1

[0034] (Es ist zu bemerken, daß ebenbürtige Strukturen oder Operationen benutzt werden können, wie beispielsweise die einfache Unterhaltung einer als „Benutzername@ISPA.com" formatierten Liste von Feldern, wo der Teil nach dem „@"-Symbol die Anker-LAC anzeigt. Als Alternative kann der ISP B eine Datenbank unterhalten, die Benutzer auf Dienste abbildet. Im Fall einer virtuellen Einwahl (d.h. einer Identifikation des entfernten Benutzers als einem VPN-Dienst zugeordnet) wird von der Abbildung weiterhin die Anker-LAC identifiziert. Als Alternative kann die versorgende LAC eine Transaktion Radius-Zugangsanforderung/Antwort (Radius Access Request/Response) mit ihrem örtlichen Radius-Server für diese Aufgabe nach dem Stand der Technik benutzen.)

[0035] Im Schritt **230** überprüft die versorgende LAC **115**, ob zwischen ihr und der Anker-LAC **155** ein Tunnel besteht. Dabei unterhält die versorgende LAC **115** eine in der Tabelle 2 unten dargestellte Tabelle von aktuellen Tunneln, vertreten durch einen Tunnelidentifikationswert (Tid – Tunnel Identification), zugeordnete Verbindungskennungen (Cid – Call Identifiers) von gegenwärtig diesen Tunnel benutzenden Verbindungen, und die zugeordnete Anker-LAC-IP-Adresse.

Tid	Cid	Anker-LAC-IP-Adresse
2	5	h.j.k.l

Tabelle 2

[0036] Wenn gegenwärtig keine Tunnelverbindung zwischen der versorgenden LAC und der Anker-LAC besteht, dann wird von der versorgenden LAC **115** im Schritt **235** ein Tunnel zur Anker-LAC eingeleitet (unten beschrieben). Sobald ein Tunnel zwischen der versorgenden LAC und der Anker-LAC besteht, wird von der versorgenden LAC **115** im Schritt **240** eine neue Cid zugeordnet, die Tabelle 2 aktualisiert, und eine Sitzung mit der Anker-LAC **155** durch Weiterleitung einer VPN-Anforderung zur Anker-LAC **155** über das Ortsnetz **120**, den Router **125**, das Internet **130**, den Router **165** und das Ortsnetz **160** eingeleitet (weiter unten beschrieben). In dieser Anforderung werden von der versorgenden LAC **115** Benutzeridentifikationsinformationen zur Anker-LAC **155** übermittelt.

[0037] Uns nunmehr der Fig. 3 zuwendend wird die Anforderung im Schritt **305** von der Anker-LAC **155** empfangen. Im Schritt **310** wird von der Anker-LAC **155** auch Authentifizierung des entfernten Benutzers (z.B. unter Verwendung eines vordefinierten „Benutzernamens" und „Paßworts" wie oben bemerkt) durchgeführt und die Verbindung angenommen (dargestellt durch die gestrichelte Linie 2 der Fig. 1). (Als Alternative könnten wie bei der versorgenden LAC, DNIS, CLID oder sonstige gleichwertige Identifikationsformen benutzt werden.) Wenn die Anker-LAC **155** den Benutzer nicht identifizieren kann, wird die Verbindung nicht angenommen (dieser Schritt ist nicht dargestellt). (In diesem Fall muß die versorgende LAC **115** auf ähnliche Weise eine Fehlernachricht zum entfernten Benutzer zurückübermitteln (nicht dargestellt).)

[0038] Von der Anker LAC **155** wird eine VPN-Tabelle gespeichert, auf der a priori z.B. die Identifikation eine Benutzers einem bestimmten LNS zugeordnet wird. Ein Teil einer solchen Tabelle ist unten in der Tabelle 3 dargestellt. In diesem Beispiel wird der dem PC **110** zugeordnete entfernte Benutzer dem LNS **135**, vertreten durch IP-Adresse g.h.i.j, zugeordnet.

Benutzeridentifikation	LNS
Benutzername	g.h.i.j

Tabelle 3

[0039] (Ähnlich der versorgenden LAC **115** ist zu bemerken, daß gleichwertige Strukturen oder Operationen benutzt werden könnten. Beispielsweise könnte die Anker-LAC diese Funktion auch über Radius-Zugangsanforderung/Antwort-Nachrichten mit einem Heimat-Radius-Server durchführen.) Im Schritt **315** überprüft die Anker-LAC **155** anhand der Tabelle 3, ob dies eine gültige VPN-Anforderung ist. Wenn es keine gültige Anforderung ist, wird die Anforderung von der Anker-LAC **155** im Schritt **320** abgewiesen. Wenn es eine gültige Anforderung ist, wird der zugeordnete LNS von der Anker-LAC **155** im Schritt **325** aus der Tabelle 3 identifiziert.

[0040] Es wird angenommen, daß von der Anker-LAC die folgende Verbindungstabelle für jede Kommunikationsrichtung für aufgebaute VPN-Sitzung mit einem entfernten Benutzer unterhalten wird:

Verbindungs-Nr.	Versorgende LAC		Versorgende LAC	LNS		LNS IP-Adresse	Vom Benutzer zugewiesene IP-Adresse
	Tid	Cid		Tid	Cid		
5	2	5	d.e.f.g	1	3	g.h.i.j	a.b.c.d

Tabelle 4

[0041] Von der Anker-LAC wird jeder VPN-Sitzung eine Verbindungsnummer zugeordnet. Zusätzlich wird diese Verbindungsnummer auf den jeweiligen Benutzer abgebildet. In dieser Tabelle wird nach Verbindungsnummer die IP-Adresse der versorgenden LAC (mit zugeordneter Tunnel-ID- und Verbindungs-ID-Werten für diese Strecke) und die zugeordnete LNS-IP-Adresse (mit zugeordneten Tunnel-ID- und Verbindungs-ID-Werten für diese zugeordnete Strecke) aufgeführt. Im Schritt **330** wird von der Anker-LAC **155** die VPN-Setzung hergestellt (eine Authentifizierungsprüfung usw. durchgeführt). (Wiederum werden, wenn LNS **135** die VPN-Anforderung abweist (z.B. aufgrund keiner Authentifizierung des entfernten Benutzers oder keiner Kapazität) von der Anker-LAC der versorgenden LAC entsprechende Fehlernachrichten erzeugt.) Außer dem erfinderischen Konzept wird die VPN-Sitzung mit LNS **135** nach dem Stand der Technik hergestellt. Beispielsweise und gemäß den Grundsätzen der Erfindung wird von der Anker-LAC **155** bei Herstellung einer neuen VPN-Sitzung eine neue Cid zugeordnet und die Tabelle 4 aktualisiert (z.B. eine neue Verbindung zugefügt). Diese letztere Verbindung wird durch gestrichelte Linie 3 der **Fig. 1** dargestellt.

[0042] An dieser Stelle besteht die Konnektivität aus einer Punkt-zu-Punkt-PPP-Sitzung, deren Endpunkte die Vernetzungsanwendung des entfernten Benutzers an einem Ende (wie durch PC **110** dargestellt) und der Abschluß dieser Konnektivität in PPP-Unterstützung von LNS **135** am anderen besteht. (Es ist zu bemerken, daß Buchführung gegebenenfalls an der versorgenden LAC der Anker-LAC wie auch dem LNS durchgeführt werden kann, d.h. jedes Element kann Pakete, Oktette und Verbindungsstart- und -stoppzeiten zählen.)

[0043] Zur Unterstützung des oben beschriebenen virtuellen Mehrstrecken-Wähldienstes wird eine Form des L2TP-(mL2TP-)Protokolls benutzt und weiter unten beschrieben. Wie bei L2TP gibt es zwei parallele Komponenten von mL2TP, die über einen gegebenen Tunnel Steuernachrichten zwischen jedem Paar LAC/LNS und Nutzlastpakete über das gleiche Paar LAC/LNS betreiben. Die letzteren werden zum Transportieren von mL2TP-verkapselten PPP-Paketen für Benutzersitzungen zwischen dem Paar LAC/LNS benutzt. Wie bei L2TP sind die Felder Nr. (Next Receive) und Ns (Next Sent) stets in Steuernachrichten vorhanden und sind wahlweise in Nutzlastpaketen vorhanden. Die Steuernachrichten und Nutzlastnachrichten benutzen unterschiedliche Folgenummerzustände. Für das obenerwähnte Szenario des Paars LAC/LNS gibt es hinsichtlich der Unterhaltung und Nutzung von (Nr, Ns) keine Änderungen an der Definition des L2TP-Entwurfsprotokolls.

[0044] Wie bei der Verbindung zwischen der versorgenden LAC und der Anker-LAC werden jedoch von der Anker-LAC, die von der versorgenden LAC gesendeten Werte (Nr, Ns) nur überwacht. Das heißt, und entsprechend dem erfinderischen Konzept, werden die von der versorgenden LAC empfangenden Werte von der Anker-LAC einfach zum LNS übertragen. Zusätzlich werden von der Anker-LAC nunmehr ihre Werte (Sr, Ss –

State Received, State Sent) mit den entsprechenden Werten (Nr, Ns) aktualisiert, die sie aus den durch die versorgende LAC gesendeten Paketen beobachtet hat. Da es zweifellos Paketverluste zwischen der versorgenden LAC und der Anker-LAC geben wird, könnte der wert Ss (Sr) an der Anker-LAC kleiner als der Wert Ss (Sr) an der versorgenden LAC sein. Zusätzlich werden von der Anker-LAC zwei Sätze von Variablen (Sr, Ss) unterhalten, eine für die Steuerverbindung versorgende LAC/Anker-LAC und die andere für die Steuerverbindung Anker-LAC/LNS.

[0045] Ehe PPP-Tunnelung gemäß dem erfinderischen Konzept zwischen der versorgenden LAC, der Anker-LAC und dem LNS stattfinden kann, müssen zwischen ihnen Steuernachrichten ausgetauscht werden. Steuernachrichten werden über den gleichen Tunnel ausgetauscht, der danach zur Weiterleitung von Nutzlastdaten benutzt wird, sobald mL2TP-Verbindungssteuerungs- und Verwaltungsinformationen zugelassen worden sind (unten beschrieben).

[0046] Gemäß dem erfinderischen Konzept werden zusätzliche AVP (Attribute Value Pairs – Attributwertepaare) (unten beschrieben) zur Verwendung in den L2TP-Steuernachrichten definiert (die daher mL2TP-Steuernachrichten werden). Diese zusätzlichen AVP dienen zur Unterstützung der oben beschriebenen Mehrstreckenmerkmale und Verbindungsübertragungsmerkmale. Nach Definition in L2TP werden AVP zur weiteren Spezifikation von Steuersignalisierung benutzt.

[0047] Wie oben bemerkt, gibt es für den Fall des oben beschriebenen Paars LAC/LNS keine Änderung an der in dem obenerwähnten L2TP-Entwurf beschriebenen Prozedur. Dabei erfordert nur der Mehrstreckenfall zusätzliche Prozeduren wie unten beschrieben.

[0048] In Fig. 4 wird ein beispielhafter Mehrstrecken-Nachrichtenfluß dargestellt. Wie aus Fig. 4 ersichtlich, wird ein (durch einen Tid-Wert gekennzeichneter) Tunnel und eine (durch einen Cid-wert gekennzeichnete) Verbindung zwischen der versorgenden LAC und der Anker-LAC hergestellt. Auf ähnliche Weise wird ein Tunnel und eine Verbindung zwischen der Anker-LAC und den LNS hergestellt. Wie in Fig. 4 gezeigt, erfordert das erfinderische Konzept, daß die versorgende LAC einen Tunnel zur Anker-LAC herstellt. Im Zusammenhang mit der vorliegenden Erfindung behandelt die versorgende LAC die Anker-LAC als ein LNS, und L2TP-Prozeduren werden für den anfänglichen Aufbau des Tunnels benutzt.

[0049] Sobald ein Tunnel hergestellt worden ist, findet eine Anzahl von Steuernachrichtentransaktionen statt, um eine PPP-Sitzung gemäß den Grundsätzen der Erfindung aufzubauen. Diese sind in Fig. 5-Fig. 7 dargestellt. In diesen Figuren sind nur die entsprechenden Felder für die verschiedenen Steuernachrichten gezeigt. (Man beachte, daß, wenn sich die Tunnel-ID und Verbindungs-ID für den Tunnel zwischen der versorgenden LAC und der Anker-LAC von den Werten für den Tunnel zwischen der Anker-LAC und den LNS unterscheiden, die Anker-LAC die entsprechenden Felder in den Paketköpfen abändert, ehe sie sie in beiden Richtungen weiterleitet.)

[0050] Wie in Fig. 5 gezeigt, sendet die versorgende LAC zuerst eine SCCRQ-Nachricht (Start Control Connect Request) (wie in L2TP definiert) zur Anker-LAC, um den Tunnel zwischen ihnen zu konfigurieren. Bei Empfang dieser Nachricht antwortet die Anker-LAC dann mit einer SCCRP-Nachricht (Start Control Connect Reply) (dies findet nach jeder oben beschriebenen Authentifizierung statt). Die versorgende LAC bestätigt mit einer SCCCN-Nachricht (Start Control Connection Connect) zur Anker-LAC.

[0051] Nach den in Fig. 5 gezeigten Austauschvorgängen der Nachricht Start Control Connection (Steuerverbindung starten) sendet die versorgende LAC eine ICRQ-Nachricht (Incoming Call Request – Anforderung ankommender Verbindung) zur Anker-LAC wie in Fig. 6 dargestellt. Die Incoming-Call-Request-Nachricht enthält genügend Benutzerdaten und Kennzeichnungen, um der Anker-LAC die Identifikation des LNS zu ermöglichen.

[0052] Wie früher bemerkt, werden von der Anker-LAC, wenn kein Tunnel zwischen der Anker-LAC und den LNS besteht, zuerst die Austauschvorgänge der SCCR-, SCCRP-, SCCCN-Nachricht mit den LNS wie in L2TP definiert eingeleitet. Sobald der Tunnel besteht, wird ein unbenutzter Schlitz in dem Tunnel, eine Cid, durch die Anker-LAC zugeteilt. An diesem Punkt und entsprechend den Grundsätzen der Erfindung wird von der Anker-LAC die ICRQ-Nachricht (von der versorgenden LAC) weitergeleitet, um den LNS über diese neue Wählsitzung zu benachrichtigen. Wie in Fig. 6 gezeigt, wird die ICRQ-Nachricht von der Anker-LAC entsprechend abgeändert, ehe sie zum LNS weitergeleitet wird. Die abgeänderten Felder werden durch ein „*" angezeigt, z.B. die zugewiesene Verbindungs-ID. von der Anker-LAC wird auch ein verborgenes AVP zugefügt, um den LNS darüber zu informieren, welche Empfangsfenstergröße sie unterstützen kann. (Man beachte, daß mit der

zusätzlichen Strecke die Anker-LAC die maximale Fenstergröße aufzeichnet, die für beide Steuerungs-/Nutzlastverbindungen ausgehandelt worden ist. Auch kann die Fenstergröße für die Steuerverbindung zwischen der versorgenden LAC und der Anker-LAC sich von der der Steuerungsverbindung zwischen der Anker-LAC und den LNS unterscheiden und Pufferspeicherung kann erforderlich sein. Um zusätzliche Pufferspeicherung und Folgenummerüberwachung zu eliminieren, wird von der Anker-LAC wahlweise ein AVP zugefügt, um den LNS darüber zu informieren, welche Empfangsfenstergröße für die Nutzlastsitzung die Anker-LAC in Richtung Anker-LAC-versorgende LAC unterstützen kann. Als Ergebnis wird der LNS nur zutreffende Empfangsfenstergrößenwerte in seine ICRP-Antwort einschließen, und daher nur eine Fenstergröße für die Nutzlastsitzung in der Richtung LNS-Anker-LAC-versorgende LAC).

[0053] Wie früher bemerkt, wird die Verbindung vom LNS entweder angenommen oder abgewiesen. Abweisungen MÜSSEN einen Ergebniszustand umfassen und KÖNNEN eine Fehleranzeige umfassen. In beiden Fällen sendet der LNS eine ICRP-Nachricht (Incoming Call Reply – Antwort ankommender Verbindung) zur Anker-LAC wie in Fig. 6 gezeigt. Von der Anker-LAC wird dann die ICRP-Nachricht entsprechend abgeändert und gemäß der Erfindung zur versorgenden LAC weitergeleitet (abgeänderte Felder sind wiederum durch ein „*" in der Fig. 6 angezeigt). Da das vom LNS empfangene PPD-Feld (Packet Processing Delay – Paketverarbeitungsverzögerung) nur die Verarbeitungsverzögerung am LNS enthält, wird diesem Wert von der Anker-LAC die Verarbeitungsverzögerung an ihrem eigenen Knoten zugefügt. Dann wird die ICRQ-Nachricht zur versorgenden LAC weitergeleitet.

[0054] Als Antwort sendet die versorgende LAC eine ICCN-Nachricht (Incoming Call Connected – Ankommende Verbindung verbunden) zur Anker-LAC wie in Fig. 7 gezeigt. In dieser Nachricht werden von der versorgenden LAC alle LCP-Config-Request-Informationen wie auch die Proxy-Authentication Informationen weitergegeben. Das heißt, die versorgende LAC leitet die Ergebnisse der mit der Benutzereinrichtung durchgeführten LCP Config Request/Ack, PPP PAP/CHAP weiter. Von der Anker-LAC wird das PPD-Feld der empfangenen ICCN-Nachricht vor Weiterleitung zum LNS abgeändert. (Gegenwärtig wird tx Connect Speed und rx Connect Speed nicht benutzt). Obwohl dies nicht dargestellt ist und gemäß der Erfindung, werden von der Anker-LAC auch die in L2TP definierten Nachrichten Set-Link-Info, Hello und Wan-Error-Notify weitergeleitet. (Es ist zu beachten, daß die obige Beschreibung das Konzept von Mehrstrecken-Pakettunnel darstellt. Beispielsweise stellt die Fig. 1 einen Zweistrecken-Pakettunnel dar.)

[0055] Es ist zu beachten, daß die oben beschriebenen Mehrstrecken mL2TP-Tunnel ausschließlich auf der Rahmenschicht stattfinden. Dabei sind eigentliche Strategien von Adressenverwaltung durch den LNS für den oben beschriebenen virtuellen Wähldienst bedeutungslos, da der entfernte Benutzer sich für alle Zwecke der PPP-Protokollbearbeitung am LNS angeschlossen zu haben scheint.

Mobiles Punkt-zu-Punkt-Protokoll

[0056] Uns nunmehr der Fig. 8 zuwendend, ist eine weitere Ausführungsform des erfinderischen Konzepts dargestellt. Fig. 8 ist der Fig. 1 ähnlich. Außer dem erfinderischen Konzept sind die Elemente wohlbekannt und werden nicht ausführlich beschrieben. Gleiche Nummern zeigen gleiche Funktionen an und werden nur wenn nötig weiter beschrieben.

[0057] In der Fig. 8 enthält der PC **805** (nicht gezeigte) Datenkommunikationseinrichtung zum Herstellen von drahtlosem Zugang zum Internet über das drahtlose PCS-Netz **810** (Personal Communication Service). Drahtlose PCS-Dienste sind in der Technik bekannt und werden nicht ausführlich beschrieben. Das drahtlose PCS-Netz **810** umfaßt eine Mehrzahl von durch Elemente **815** und **820** dargestellten Mobilvermittlungsstellen. Jede Vermittlungsstelle versorgt ein (nicht gezeigtes) geographisches Gebiet. Es wird angenommen, daß Elemente **815** und **820** einen NAS einschließen, z.B. versorgende LAC ähnlich der versorgenden LAC **115** der Fig. 1. Anfänglich wird angenommen, daß der entfernte Benutzer eine VPN-Sitzung zum Firmennetz unter Verwendung des oben beschriebenen Mehrstreckenverfahrens herstellt. Insbesondere befindet sich der entfernte Benutzer in einem geographischen Gebiet, so daß seine anfängliche Verbindung über Verbindungen **814** und **816** durch das Element **815** geleitet wird. Im Zusammenhang mit einer drahtlosen PCS-Anwendung besteht die anfängliche PPP-Verbindung zwischen dem Element **815** und dem PC **805**. (Obwohl der Einfachheit halber als Teil der Vermittlungselemente dargestellt, könnten die NAS-Funktionen auch in getrennten Einrichtungsstücken durchgeführt werden. Auf ähnliche Weise sind die anderen Elemente, wie beispielsweise ein Ortsnetz und Router, der Einfachheit halber nicht dargestellt.)

[0058] Es ist festgestellt worden, daß Tunnelprotokolle wie beispielsweise L2TP in einer drahtlosen Umgebung einem entfernten Benutzer nicht erlauben, die bestehende PPP-Verbindung von einem Vermittlungsele-

ment zu einem anderen umzuwechseln. In der momentanen Annahme, daß Fig. 8 nicht das erfinderische Konzept verkörpert, wird beispielsweise, wenn der entfernte Benutzer herumreist, z.B. zu einem durch das Element **820** versorgten geographischen Gebiet (und daher einem unterschiedlichen NAS), die Kommunikationssitzung des Benutzers nach dem Stand der Technik zum Element **820** weitergeschaltet. Die bestehende PPP-Verbindung – und daher die VPN-Sitzung – wird jedoch abgeworfen und muß wieder hergestellt werden, da, wie bemerkt, es keine Fähigkeit zur Übertragung bestehender PPP-Verbindungen von einem NAS zu einem anderen gibt. In diesem Zusammenhang wird dieses Problem durch das Kommunikationssystem der Fig. 8 überwunden.

[0059] Ein NAS oder eine LAC umfaßt daher und erfindungsgemäß ein Merkmal „Hand-Off" (Weiterschaltung), das im bestehenden NAS das Weiterschalten einer bestehenden PPP-Verbindung zu einem anderen NAS erlaubt. Nach diesem Merkmal sind 3 neue Steuernachrichten definiert, nämlich: (i) Continued Call Request (Anforderung Verbindungsweiterführung), (ii) Continued Call Reply (Antwort Verbindungsweiterführung), und (iii) Continued Call Connect (Verbinden Verbindungsweiterführung). Als Ergebnis des obigen muß der Benutzer nicht die aktuelle PPP-Verbindung abschließen und dann eine neue PPP-Verbindung wiederherstellen. Diese 3 neuen Steuernachrichten umfassen einen L2TP Steuernachrichtenkopf, Nachrichtenkennung (z.B. Anforderung Verbindungsweiterführung, usw.) und eine Anzahl von Feldern (unten beschrieben).

[0060] Nach dem erfinderischen Konzept ist ein beispielhafter Weiterschaltungsnachrichtenfluß in Fig. 9 dargestellt. Wie aus Fig. 9 ersichtlich, werden anfänglich ein (durch einen Tid-Wert gekennzeichneter) Tunnel und eine (durch einen Cid-Wert gekennzeichnete) Verbindung zwischen dem Element **815**, das eine versorgende LAC enthält, und der Anker-LAC hergestellt. Auf ähnliche Weise wird ein Tunnel und eine Verbindung zwischen der Anker-LAC und dem LNS hergestellt. (Ein Verfahren zum Herstellen dieser anfänglichen VPN-Sitzung wurde oben beschrieben.) Nach der Darstellung in Fig. 9 erlaubt das erfinderische Konzept der bestehenden versorgenden LAC, die bestehende PPP-Verbindung zu einer neuen versorgenden LAC wie durch das Element **820** dargestellt zu übertragen.

[0061] Es ist nunmehr auf Fig. 10 Bezug zu nehmen, die ein beispielhaftes Flußdiagramm eines Verfahrens zur Verwendung bei der Bereitstellung eines „Weiterschaltungsmerkmals" ist. Wie bemerkt, wird angenommen, daß eine VPN-Sitzung zwischen PC **805** und dem Firmennetz über das Element **815**, das eine versorgende LAC enthält, und die Anker-LAC **155**, besteht. Nach dem erfinderischen Konzept fügt das drahtlose PCS-Netz **810** den bestehenden Verbindungszustandsvariablen zusätzliche Variablen hinzu, die die Gegenwart (oder den Mangel) einer PPP-Verbindung für jede drahtlose Verbindung anzeigen, und wenn eine PPP-Verbindung besteht, PPP-Verbindungsinformationen, die die Anker-LAC-Kennung, z.B. die IP-Adresse der Anker-LAC, umfassen.

[0062] Im Schritt **405** der Fig. 10 erkennt das drahtlose Netz **810** das Erfordernis einer Weiterschaltung, da sich der PC **805** aus dem durch das Element **815** versorgten geographischen Gebiet in ein anderes geographisches Gebiet, z.B. das durch Element **820** versorgte Gebiet, bewegt hat, das eine weitere versorgende LAC enthält. Im Schritt **410** benachrichtigt das drahtlose PCS-System das Element **820** über die bevorstehende Weiterschaltung. (Das (die) durch ein drahtloses System zum Erkennen und Durchführen einer Weiterschaltung benutzte(n) Verfahren sind in der Technik bekannt und für das erfinderische Konzept bedeutungslos. Sie werden daher hier nicht beschrieben und sind durch den Signalisierungsweg **811** der Fig. 8 dargestellt.) Da die Verbindungszustandsinformationen nunmehr einen PPP-Sitzungsanzeiger und PPP-Verbindungsinformationen enthalten, wird die Anker-LAC von der neuen versorgenden LAC (des Elements **820**) im Schritt **415** identifiziert. Im Schritt **420** überprüft die neue versorgende LAC (des Elements **820**), ob ein bestehender Tunnel zwischen ihr selbst und der identifizierten Anker-LAC, hier der Anker-LAC **155**, besteht.

[0063] Wenn kein Tunnel besteht, wird von der neuen versorgenden LAC (wie vorher beschrieben) zuerst im Schritt **425** ein Tunnel hergestellt. Danach und erfindungsgemäß sendet die neue versorgende LAC eine CCRQ-Nachricht (Continued-Call-Request) zur Anker-LAC im Schritt **430**. Diese CCRQ-Nachricht enthält den der bestehenden PPP-Verbindung zugeordneten Benutzernamen, die für die übertragene (neue) PPP-Sitzung zu benutzenden Tid- und Cid-Werte.

[0064] Im Schritt **435** wird von der Anker-LAC der Benutzername aus der empfangenen CCRQ-Nachricht wiedergewonnen, und diese Informationen zur Bestimmung der LNS- und IP-Adresse der alten versorgenden LAC, z.B. aus einer durch Tabelle 4 oben dargestellten Verbindungstabelle (diese wiedergewonnenen Informationen könnten auch die jeweilige UDP-Anschlußnummer (User Datagram Protocol) enthalten). In diesem Schritt sendet die Anker-LAC eine Nachricht Call-Disconnect-Notify (Benachrichtigung Verbindungsabbruch) (z.B. siehe L2TP) zur alten versorgenden LAC und identifiziert auch in z.B. der Tabelle 4 oben die dieser

PPP-Verbindung dem entfernten Benutzer zugeordneten bestehenden Verbindungsvariablen wie beispielsweise alte Tunnel-ID und alte Verbindungs-ID. (Wenn andererseits die Continued-Call-Request von der Anker-LAC zurückgewiesen werden sollte, sendet die versorgende LAC entweder ein Zeichen zurück zum Benutzer, so daß die bestehende PPP-Sitzung abgebrochen werden kann und eine neue PPP-Sitzung eingeleitet werden kann, oder die PPP-Sitzung wird einfach abgeworfen (nicht gezeigte Schritte).)

[0065] Im Schritt **440** antwortet die Anker-LAC mit einer CCRP-Nachricht (Continued-Call-Reply – Antwort Verbindungsfortführung) mit einer entsprechenden Empfangsfenstergröße (Receive Window Size). Die CCRP-Nachricht enthält Informationen über die aktuellen Nr- und Ns-Werte. Im Schritt **445** wird von der Anker-LAC ihre Verbindungstabelle, z.B. Tabelle 4 oben, durch Ersetzen der Einträge für die Adreßfelder Tid, Cid und versorgende LAC IP-Adresse (im Schritt **435** identifiziert), durch die neuen Verbindungsinformationen für die bestehende PPP-Verbindung aktualisiert. Im Schritt **450** werden von der neuen versorgenden LAC die Nr, Ns in ihre Werte Sr, Ss eingespeichert und auch sofern nötig die Empfangsfenstergröße aus der empfangenen CCRP-Nachricht gespeichert und eine CCCN-Nachricht (Continued-Call-Connect) zur Anker-LAC gesendet, wodurch die Weiterschaltung abgeschlossen wird.

[0066] Als Unterstützung für das oben beschriebene Weiterschaltungsmerkmal für ein PPP-Protokoll zeigt die Fig. 11 die oben erwähnten neuen Steuernachrichtentransaktionen gemäß den Grundsätzen der Erfindung. Nach der Darstellung in Fig. 11 wird eine CCRQ-Nachricht zur identifizierten Anker-LAC gesendet.

[0067] Eine CCRQ-Nachricht umfaßt folgende Felder:
- Assigned Cid (zugewiesene Cid),
- Call Serial No. (Verbindungs-Seriennr.),
- Bearer Type (Trägerart),
- Physical Channel ID (ID des physikalischen Kanals),
- Dialed No. (gewählte Nr.),
- Dialling No. (Wähl-Nr.),
- Sub-Address (Unteradresse),
- Anchor-LAC (Anker-LAC),
- Challenge (Abfrage),
- User AVP (Benutzer-AVP),
- Benutzername und
- MIN/Telefon des Benutzers.

[0068] Für das Anker-LAC-Feld wird angenommen, daß diese Information während der Weiterschaltung zur Verfügung steht (als Alternative muß das Weiterschaltungsverfahren, wenn es keine Informationen über die Anker-LAC für die neue versorgende LAC bereitstellt, genug Benutzerinformationen für die neue versorgende LAC bereitstellen, so daß die neue versorgende LAC mit Hilfe von einem Foreign Radius Server (fremder Radiusserver) nach dem Stand der Technik nach der Anker-LAC-Information suchen kann. Das heißt, die neue versorgende LAC fragt nach der Anker-LAC von einem Home Radius Server (Heimat-Radiusserver) über Radius Access/Response-Nachrichten).

[0069] Die Information Benutzer-AVP enthält Benutzerinformationen (wie beispielsweise den Benutzernamen) und sonstige Benutzerreferenzen, z.B. virtueller Mehrstrecken-Wähldienst, Benutzeridentität (MIN), Telefonnummer des Diensteanbieters usw.

[0070] Nach der CCRQ-Nachricht sendet die Anker-LAC eine Nachricht Call-Disconnect-Notify zur alten versorgenden LAC. Die Anker-LAC antwortet dann mit einer CCRP-Nachricht (Continued-Call-Reply), die die von ihr unterhaltenen aktuellen Sr-, Ss-werte enthält.

[0071] Eine CCRP-Nachricht umfaßt folgende Felder:
- Assigned Cid (zugewiesene Cid),
- Result-Code (Ergebniscode),
- Receive Window Size (Empfangsfenstergröße),
- PPD,
- Nr,
- Ns,
- Challenge (Abfrage) und
- Challenge Response (Abfrageantwort).

[0072] Abschließend antwortet die neue versorgende LAC mit einer CCCN-Nachricht (Continued Call Connect). Eine CCCN-Nachricht umfaßt folgende Felder:

– Connect Speed (Verbindungsgeschwindigkeit),
– Framing Type (Rahmenbildungsart),
– Receive Window Size (Empfangsfenstergröße),
– PPD, und
– Challenge Response (Abfrageantwort).

[0073] Uns nunmehr der Fig. 12 zuwendend, ist eine weitere Ausführungsform des erfinderischen Konzepts im Zusammenhang mit der Übertragung einer bestehenden PPP-Verbindung von einem NAS zu einem anderen NAS dargestellt, wo der alte NAS eine Verbindung zum LNS aufweist. (In diesem Beispiel gibt es keine versorgende LAC an sich, sondern einfach z.B. eine Anker-LAC, die eine bestehende PPP-Verbindung direkt unterstützt.) Fig. 12 ist der Fig. 8 ähnlich. Außer dem erfinderischen Konzept sind die Elemente wohlbekannt und werden nicht ausführlich beschrieben. Gleiche Ziffern zeigen gleiche Funktionen an und werden nur wo nötig weiter beschrieben.

[0074] In der Fig. 12 enthält der PC **805** (nicht gezeigte) Datenkommunikationseinrichtung zur Herstellung drahtlosen Zugriffs auf das Internet über das drahtlose PCS-Netz **910** (Personal Communication Service). Drahtlose PCS-Dienste sind in der Technik bekannt und werden nicht ausführlich beschrieben. Das drahtlose PCS-Netz **910** umfaßt eine Mehrzahl von durch Elemente **875** und **880** dargestellte Mobilvermittlungsstellen. Jede Vermittlungsstelle versorgt ein (nicht gezeigtes) geographisches Gebiet. Es wird angenommen, daß Elemente **875** und **880** einen NAS einschließen, z.B. versorgende LAC ähnlich der versorgenden LAC **115** der Fig. 1. Anfänglich wird angenommen, daß der entfernte Benutzer eine VPN-Sitzung zum Firmennetz unter Verwendung des oben beschriebenen Mehrstreckenverfahrens herstellt. Insbesondere befindet sich der entfernte Benutzer in einem geographischen Gebiet, so daß seine anfängliche Verbindung über Verbindungen **874** und **876** durch das Element **875** zum LNS **935** geleitet wird. Im Zusammenhang mit einer drahtlosen PCS-Anwendung besteht die anfängliche PPP-Verbindung zwischen dem Element **875** und dem PC **805**. (Obwohl der Einfachheit halber als Teil der Vermittlungselemente dargestellt, könnten die NAS-Funktionen auch in getrennten Einrichtungsstücken durchgeführt werden. Auf ähnliche Weise sind die anderen Elemente, wie beispielsweise ein Ortsnetz und Router, der Einfachheit halber nicht dargestellt.)

[0075] In dieser Ausführungsform wird die gleiche Weiterschaltungsprozedur für das Paar LAC/LNS ausgeführt, nur werden die oben beschriebenen CCRQ-, CCRP-, CCCN-Nachrichten zwischen der neuen LAC und dem LNS ausgetauscht. Gemäß dem erfinderischen Konzept ist in Fig. 13 ein beispielhafter Weiterschaltungsnachrichtenfluß dargestellt. Wie aus Fig. 13 ersichtlich, wird anfänglich ein (durch einen Tid-Wert identifizierter) Tunnel und eine (durch einen Cid-Wert identifizierte) Verbindung zwischen dem Element **875**, das eine LAC enthält, und dem LNS **935** hergestellt. Nach der Darstellung in Fig. 13 erlaubt das erfinderische Konzept der bestehenden LAC, die bestehende PPP-Verbindung zu einer neuen LAC, wie durch Element **880** dargestellt, zu übertragen.

[0076] Es ist nunmehr auf Fig. 14 Bezug zu nehmen, die ein beispielhaftes Flußdiagramm eines Verfahrens zur Verwendung bei der Bereitstellung eines „Weiterschaltungsmerkmals" ist. Wie bemerkt, wird angenommen, daß eine VPN-Sitzung zwischen PC **805** und dem Firmennetz über das Element **875**, das eine LAC enthält, besteht. Nach dem erfinderischen Konzept fügt das drahtlose PCS-Netz **910** den bestehenden Verbindungszustandsvariablen zusätzliche Variablen hinzu, die die Gegenwart (oder den Mangel) einer PPP-Verbindung für jede drahtlose Verbindung anzeigen und, wenn eine PPP-Verbindung besteht, PPP-Verbindungsinformationen, die die LNS-Kennung, z.B. die IP-Adresse der LNS, umfassen.

[0077] Im Schritt **505** der Fig. 14 erkennt das drahtlose PCS-Netz **910** das Erfordernis einer Weiterschaltung, da sich der PC **805** aus dem durch das Element **875** versorgten geographischen Gebiet in ein anderes geographisches Gebiet, z.B. das durch Element **880** versorgte Gebiet, bewegt hat, das eine weitere LAC enthält. Im Schritt **510** wird vom drahtlosen PCS-System das Element **880** über die bevorstehende Weiterschaltung benachrichtigt. (Das (die) durch ein drahtloses System zum Erkennen und Durchführen einer Weiterschaltung benutzte(n) Verfahren sind in der Technik bekannt und für das erfinderische Konzept bedeutungslos. Sie werden daher hier nicht beschrieben und sind durch den Signalisierungsweg **911** der Fig. 12 dargestellt.) Da die Verbindungszustandsinformationen nunmehr einen PPP-Sitzungsanzeiger und PPP-Verbindungsinformationen enthalten, wird die LNS von der neuen LAC (des Elements **880**) im Schritt **515** identifiziert. Im Schritt **520** überprüft die neue LAC (des Elements **880**), ob ein bestehender Tunnel zwischen ihr selbst und dem identifizierten LNS, hier LNS **935**, besteht.

[0078] Wenn kein Tunnel besteht, wird von der neuen LAC (wie vorher beschrieben) zuerst im Schritt **525** ein Tunnel hergestellt. Danach und erfindungsgemäß sendet die neue versorgende LAC eine CCRQ-Nachricht (Continued-Call-Request) zur LNS im Schritt **530**. Diese CCRQ-Nachricht enthält den der bestehenden PPP-Verbindung zugeordneten Benutzernamen, die für die übertragene (neue) PPP-Sitzung zu benutzenden Tid- und Cid-Werte.

[0079] Im Schritt **535** wird vom LNS der Benutzername aus der empfangenen CCRQ-Nachricht wiedergewonnen und diese Information zur Bestimmung der IP-Adresse der alten LAC benutzt (diese wiedergewonnene Information könnte auch die jeweilige UDP-Anschlußnummer (User Datagram Protocol) enthalten). In diesem Schritt sendet der LNS eine Nachricht Call-Disconnect-Notify (z.B. siehe L2TP) zur alten LAC und identifiziert auch in z.B. einer der in Tabelle 4 gezeigten Verbindungstabelle ähnlichen Tabelle, aber ohne die Information über versorgende LAC usw., die dieser PPP-Verbindung zum entfernten Benutzer zugeordneten bestehenden Verbindungsvariablen wie beispielsweise alte Tunnel-ID und alte Verbindungs-ID. (Wenn andererseits die Continued-Call-Request vom LNS abgewiesen werden sollte, sendet der neue LAC entweder ein Zeichen zurück zum Benutzer, so daß die bestehende PPP-Sitzung abgebrochen werden kann und eine neue PPP-Sitzung eingeleitet werden kann, oder die PPP-Sitzung wird einfach abgeworfen (nicht gezeigte Schritte).)

[0080] Im Schritt **540** antwortet der LNS mit einer CCRP-Nachricht (Continued-Call-Reply) mit einer entsprechenden Empfangsfenstergröße. Die CCRP-Nachricht enthält Informationen über die aktuellen Nr- und Ns-Werte. Im Schritt **545** wird vom LNS die Verbindungstabelle durch Ersetzen der Einträge für die (in Schritt **535** identifizierten) Bilder für die Tid, Cid und LAC-IP-Adresse durch die neuen Verbindungsinformationen für die bestehende PPP-Verbindung aktualisiert. Im Schritt **550** wird von der neuen LAC sofern nötig die Nr, Ns und Empfangsfenstergröße aus der empfangenen CCRP-Nachricht aktualisiert und eine CCCN-Nachricht (Continued-Call-Connect) zum LNS gesendet, womit die Weiterschaltung abgeschlossen wird.

[0081] Zur Unterstützung des oben beschriebenen Weiterschaltungsmerkmals für ein PPP-Protokoll zeigt die Fig. 15 die obenerwähnten neuen Steuernachrichtentransaktionen gemäß den Grundsätzen der Erfindung. Nach der Darstellung in Fig. 15 wird eine CCRQ-Nachricht zum identifizierten LNS gesendet. (Als Alternative muß das Weiterschaltungsverfahren, wenn es keine Informationen über den LNS für die neue LAC bereitstellt, dann genügend Benutzerinformationen für die neue LAC bereitstellen, so daß die neue LAC mit Hilfe von einem Foreign Radius Server nach dem Stand der Technik nach den LNS-Informationen suchen kann. Das heißt, die neue LAC fragt nach dem LNS bei einem Home Radius Server über Radius Access/Response-Nachrichten). Nach der CCRQ-Nachricht sendet der LNS eine Nachricht Call-Disconnect-Notify zur alten LAC. Der LNS antwortet dann mit einer CCRP-Nachricht (Continued-Call Reply), die die von ihm unterhaltenen aktuellen Sr-, Ss-Werte enthält. Abschließend antwortet die neue LAC mit einer CCCN-Nachricht (Continued-Call Connect).

[0082] Wie oben beschrieben, wird eine PPP-Verbindung von einem NAS zu einem anderen NAS übertragen. Zur Unterstützung der neu definierten Nachrichten werden zusätzliche Verbindungszustände für den jeweiligen NAS, wie in Tabellen 5 und 6 unten dargestellt, definiert.

Verbindungs-zustand	Ereignis	Handlung	Neuer Zustand
Frei	Weiterschaltungs-benachrichtigung	CCRQ senden	CCRP-Antwort erwarten
CCRP-Antwort erwarten	CCRP empfangen, nicht angenommen	Aufräumen	Frei
CCRP-Antwort erwarten	CCRP empfangen, angenommen	CCCN senden	Hergestellt

Tabelle 5 – Neuer LAC (bzw. NAS)

[0083] Wie ersichtlich ist, ist der zusätzliche oder neue Verbindungszustand für mL2TP, der der neuen LAC (oder NAS) für eine Verbindungsfortführung zugeordnet ist, der Zustand CCRP-Antwort erwarten.

[0084] Es ist zu bemerken, daß für die alte LAC (oder den alten NAS) eine CDN-Nachricht (Call-Discon-

nect-Notify) empfangen wird, während sie sich im hergestellten Zustand befindet. Als Antwort räumt die alte LAC auf und trennt die Verbindung und kehrt zum Ruhezustand zurück.

Verbindungs-zustand	Ereignis	Handlung	Neuer Zustand
Hergestellt	CCRQ empfangen, nicht angenommen	CCRP senden mit Fehlercode, CDN zum LNS senden	Frei
Hergestellt	CCRP empfangen, angenommen	CDN zur alten LAC senden CCRP zur neuen LAC senden	CCCN erwarten
CCCN erwarten	CCCN empfangen	Bereitmachen für Daten	Hergestellt
CCCN erwarten	CDN empfangen	Aufräumen	Frei

Tabelle 6 – Anker-LAC bzw. LNS

[0085] Wie ersichtlich, ist der zusätzliche oder neue Verbindungszustand für mL2TP, der der Anker-LAC oder dem LNS für eine Verbindungsfortführung zugeordnet ist, der Zustand CCCN erwarten.

Nutzlastnachrichtenübersichten und Laststeuerung für mL2TP

[0086] Hinsichtlich der Nutzlastnachrichten für mL2TP werden von der versorgenden LAC und dem LNS L2TP-Prozeduren befolgt. Von der Anker-LAC wird die Tid und Cid für die Nutzlastpakete ausgetauscht. Von der Anker-LAC werden auch die durch die versorgende LAC gesendeten Werte (Nr, Ns) überwacht. (Es ist zu bemerken, daß, da Paketverluste zwischen der versorgenden LAC und der Anker-LAC auftreten könnten, erwartet wird, daß sowohl Sr- als auch Ss-Werte an der Anker-LAC den an der versorgenden LAC unterhaltenen Werten nachlaufen können.) von der Anker-LAC werden (Nr, Ns) der Nutzlastpakete in beiden Richtungen nicht geändert. Die Anker-LAC benutzt nur ihre eigenen Sr-, Ss-Werte, wenn sie eine Nachricht Continued-Call Request von einer neuen versorgenden LAC empfängt.

[0087] Hinsichtlich der Laststeuerung gelten die L2TP-Erfordernisse darüber, wann der Empfangsfenstergröße zu entsprechen ist, wann Nr/Ns zu senden sind und wann eine ACK zu senden ist, für mL2TP. Zusätzlich weist mL2TP auch die folgenden zusätzlichen Erfordernisse für die versorgende LAG und die Anker-LAC auf.

[0088] Die Anker-LAC muß den durch die versorgende LAC gesendeten Wert (Nr, Ns) überwachen. Von der Anker-LAC sollte der von ihr unterhaltene Wert (Sr, Ss) in die Nachricht Continued-Call-Reply eingefügt werden, wenn sie auf die von ihr von einer versorgenden LAC empfangene Nachricht Continued-Call-Connect antwortet. Da ein Netz zwischen der versorgenden LAC und einer Anker-LAC verlustbehaftet ist, kann der durch eine Anker-LAC unterhaltene Sr-Wert der versorgenden LAC nachlaufen.

[0089] Zusätzlich wird von der versorgenden LAC anstelle eines einfachen Empfängers ein vollständiger Empfänger entsprechend der Bezeichnung in der Technik implementiert. Durch dieses Erfordernis soll die neue versorgende LAC daran gehindert werden, Pakete außer Reihenfolge oder duplizierte Pakete zu oberen Schichten weiterzugeben, wenn während der Lebensdauer einer PPP-Sitzung ein Wechsel versorgender LAC stattfindet.

[0090] Uns kurz der Fig. 16 zuwendend, ist ein höheres Blockdiagramm eines beispielhaften NAS dargestellt.

Ein NAS ist eine speicherprogrammierte Prozessorarchitektur unterteilt in Prozessor **650**, den Speicher **660** (zum Speichern von Programmanweisungen und Daten, z.B. die oben erwähnten Verbindungstabellen usw.) und Kommunikationsschnittstelle(n) **665** zum Ankoppeln an eine oder mehrere Kommunikationseinrichtungen wie durch den Weg **666** dargestellt.

[0091] Durch das Obige werden nur die Grundsätze der Erfindung dargestellt, und es ist daher ersichtlich, daß der Fachmann zahlreiche alternative Anordnungen ausarbeiten kann. Beispielsweise könnte, anstatt daß die Herstellung eines Mehrstreckentunnels für ankommende Verbindungen durch einen versorgenden NAS eingeleitet wird, die Herstellung einer Mehrstreckenfolge für abgehende Verbindungen durch den LNS eingeleitet werden. Solche Abänderungen sind einfach und werden hier nicht beschrieben, wie durch Fig. 17-Fig. 18 dargestellt.

Patentansprüche

1. Verfahren zur Bereitstellung eines Benutzerzugangs zu einem VPN-Dienst an einem anderen Ort als dem Ankerort des Benutzers, mit folgenden Schritten:
Annehmen von Punkt-zu-Punkt-Protokoll-Verbindungen (**1**) mit Benutzern zum Zugreifen auf den VPN-Dienst, wobei diese Punkt-zu-Punkt-Verbindungen eine VPN-Verbindung zwischen dem Benutzer und einer versorgenden LAC-Vorrichtung (**115**) zum Ermöglichen eines alternativen VPN-Verbindungsorts herstellen; und
Veranlassen der Herstellung durch Verwendung eines Schicht-2-Tunnelprotokolls einer ersten Pakettunnels (**2**) zwischen einer Anker-LAC-Vorrichtung (**155**) und der versorgenden LAC-Vorrichtung und eines zweiten Pakettunnels (**3**) zwischen der Anker-LAC-Vorrichtung und einem Endpunkt-Paketserver (**135**), so daß die Anker-LAC-Vorrichtung zwischen dem ersten und zweiten Pakettunnel eingeordnet ist und Nachrichten zwischen diesen weiterleitet, und wobei mindestens einige durch das Schicht-2-Tunnelprotokoll hergestellte Nachrichten durch die Anker-LAC-Vorrichtung vor ihrer Weitergabe abgeändert werden.

2. Verfahren nach Anspruch 1, weiterhin mit dem Schritt des Verfolgens von Verbindungsinformationen, die einen Tunnelidentifikationswert für den ersten Pakettunnel und einen Tunnelidentifikationswert für den zweiten Pakettunnel enthalten.

3. Verfahren nach Anspruch 1, wobei die Abänderung mindestens einiger der Nachrichten die Abänderung von Tunnelidentifikationsinformationen enthält.

4. Verfahren nach Anspruch 1, wobei die Abänderung mindestens einiger der Nachrichten die Abänderung von in irgendwelchen der Nachrichten enthaltenen Paketverarbeitungsverzögerungsinformationen umfaßt, um eine Paketverarbeitungsverzögerung für die Anker-LAC-Vorrichtung einzuschließen.

5. Verfahren nach Anspruch 1, wobei die Anker-LAC-Vorrichtung und der Endpunktpaketserver ein Übertragungsprotokoll benutzen, das mehrere Tunnel unterstützt.

6. Verfahren nach Anspruch 5, wobei das Übertragungsprotoll das Schicht-2-Tunnelprotokoll ist.

7. Anker-LAC-Vorrichtung (**155**) zur Herstellung einer VPN-Verbindung mit einer versorgenden LAC-Vorrichtung (**115**) zum Ermöglichen eines alternativen Orts einer VPN-Verbindung mit einem Benutzer, mit folgendem:
einem Verarbeitungselement (**650**) zum Veranlassen der Herstellung durch Verwendung eines Schicht-2-Tunnelprotokolls eines ersten Pakettunnels (**2**) zwischen der Anker-LAC-Vorrichtung und der versorgenden LAC-Vorrichtung und eines zweiten Pakettunnels (**3**) zwischen der Anker-LAC-Vorrichtung und einem Endpunktpaketserver (**135**), wobei mindestens einige durch das Schicht-2-Tunnelprotokoll hergestellte Nachrichten durch die Anker-LAC-Vorrichtung vor ihrer Weitergabe zwischen dem ersten und zweiten Pakettunnel abgeändert werden; und
einem Speicherelement (**660**) zum Speichern von Verbindungsinformationen, die die zwei Pakettunnel in Verbindung miteinander bringen, wobei der erste Pakettunnel das Auftreten der VPN-Verbindung durch die versorgende LAC ermöglicht.

8. Anker-LAC-Vorrichtung nach Anspruch 7, wobei die Abänderung mindestens einiger der Nachrichten eine Abänderung von Tunnelidentifikationsinformationen umfaßt.

9. Anker-LAC-Vorrichtung nach Anspruch 7, wobei die Abänderung mindestens einiger der Nachrichten eine Abänderung von in irgendwelchen der Nachrichten enthaltenen Paketverarbeitungsverzögerungsinforma-

tion umfaßt, um eine Paketverarbeitungsverzögerung für die Anker-LAC-Vorrichtung einzuschließen.

10. Anker-LAC-Vorrichtung nach Anspruch 7, wobei die Anker-LAC-Vorrichtung und der Endpunktpaketserver zur Verwendung eines Übertragungsprotokolls geeignet sind, das mehrere Tunnel unterstützt.

11. Anker-LAC-Vorrichtung nach Anspruch 10, wobei das Übertragungsprotokoll das Schicht-2-Tunnelprotokoll ist.

Es folgen 15 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

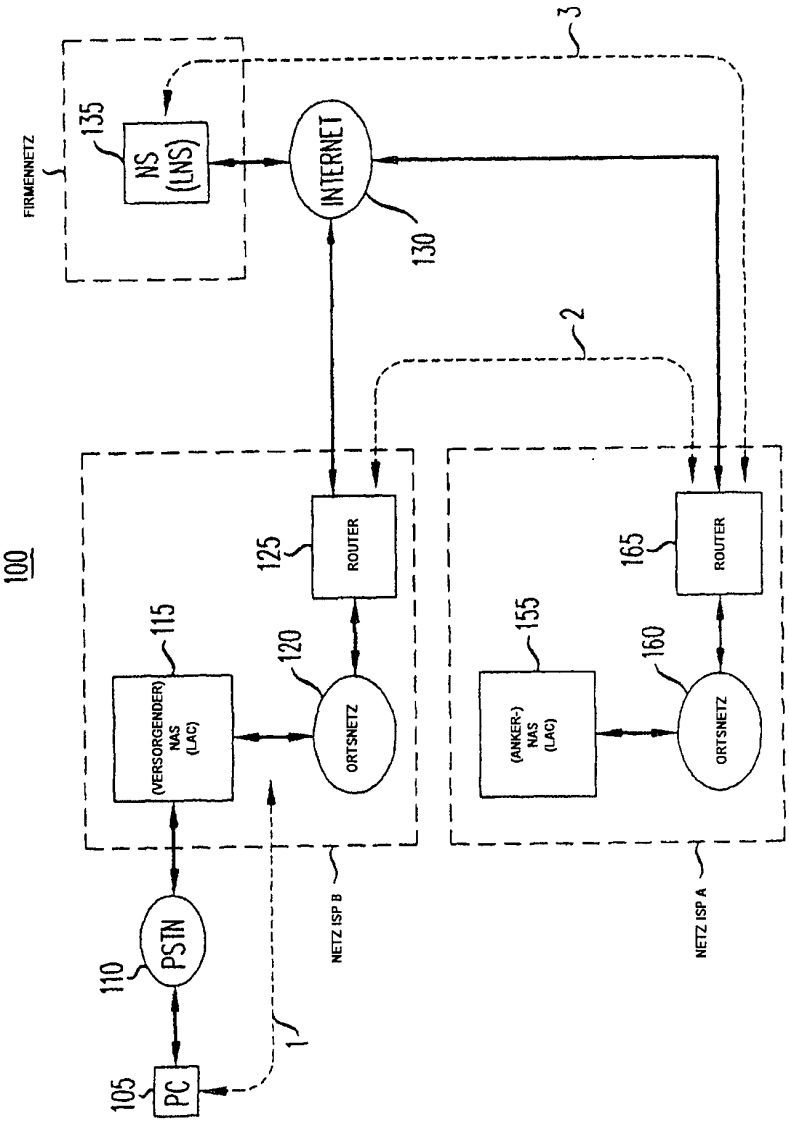


FIG. 2

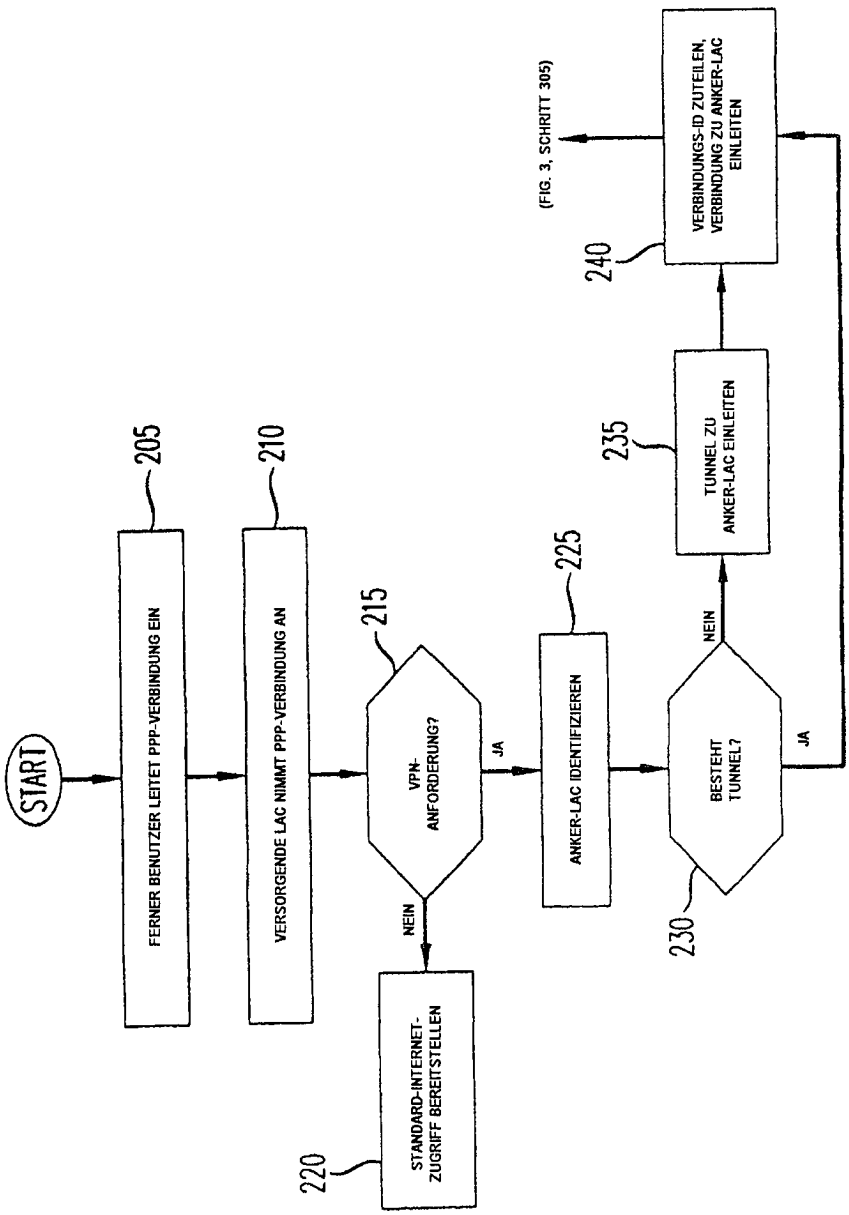

START
205
FERNER BENUTZER LEITET PPP-VERBINDUNG EIN
210
VERSORGENDE LAC NIMMT PPP-VERBINDUNG AN
215
VPN-ANFORDERUNG?
JA
NEIN
220
STANDARD-INTERNET-ZUGRIFF BEREITSTELLEN
225
ANKER-LAC IDENTIFIZIEREN
230
BESTEHT TUNNEL?
NEIN
JA
235
TUNNEL ZU ANKER-LAC EINLEITEN
240
VERBINDUNGS-ID ZUTEILEN, VERBINDUNG ZU ANKER-LAC EINLEITEN
(FIG. 3, SCHRITT 305)

FIG. 3

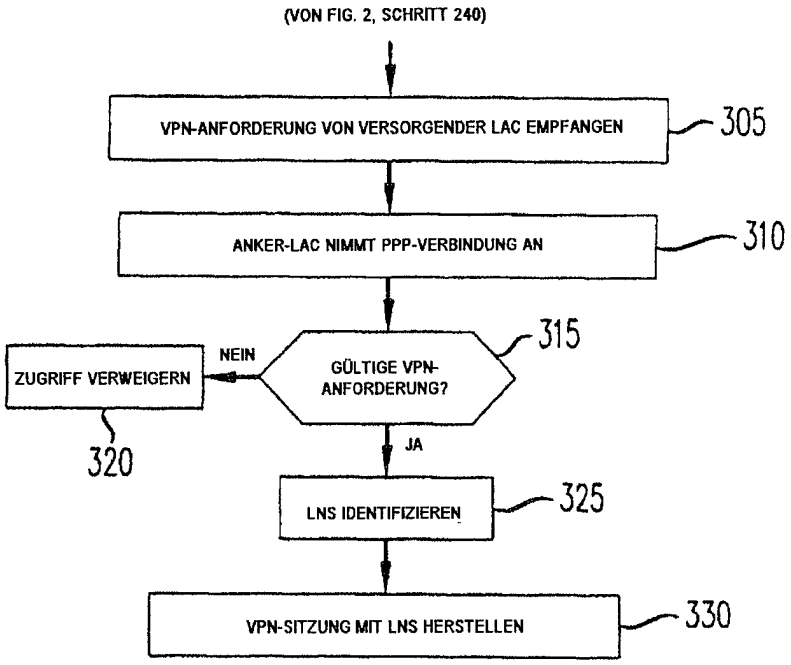

(VON FIG. 2, SCHRITT 240)
VPN-ANFORDERUNG VON VERSORGENDER LAC EMPFANGEN
305
ANKER-LAC NIMMT PPP-VERBINDUNG AN
310
GÜLTIGE VPN-ANFORDERUNG?
315
NEIN
ZUGRIFF VERWEIGERN
320
JA
LNS IDENTIFIZIEREN
325
VPN-SITZUNG MIT LNS HERSTELLEN
330

FIG. 4


VERSORGENDE LAC
Tid=2
Cid=5
ANKER-LAC
Tid=1
Cid=3
LNS-

FIG. 5

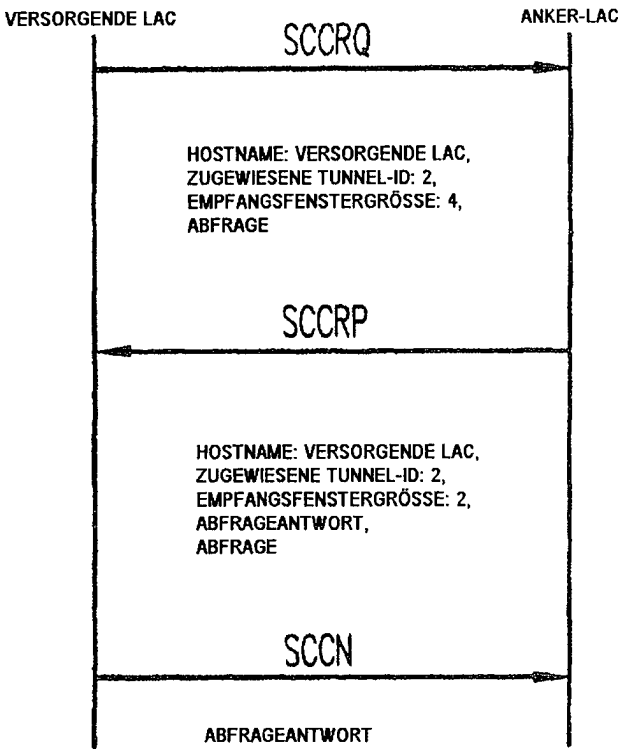

VERSORGENDE LAC
ANKER-LAC
SCCRQ
HOSTNAME: VERSORGENDE LAC,
ZUGEWIESENE TUNNEL-ID: 2,
EMPFANGSFENSTERGRÖSSE: 4,
ABFRAGE
SCCRP
HOSTNAME: VERSORGENDE LAC,
ZUGEWIESENE TUNNEL-ID: 2,
EMPFANGSFENSTERGRÖSSE: 2,
ABFRAGEANTWORT,
ABFRAGE
SCCN
ABFRAGEANTWORT

FIG. 6

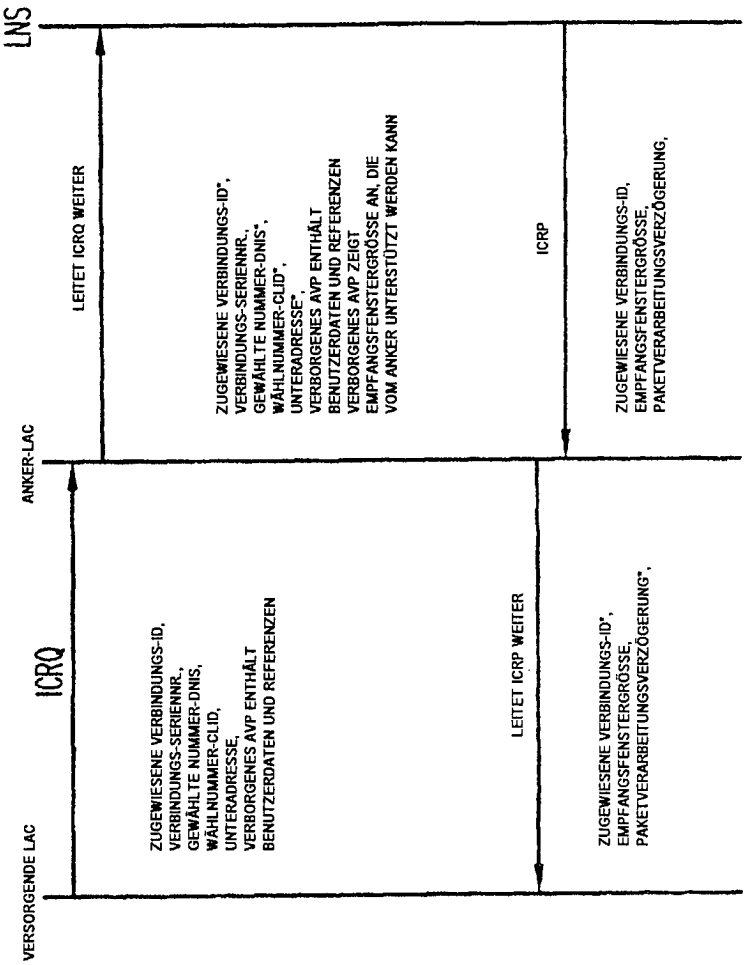
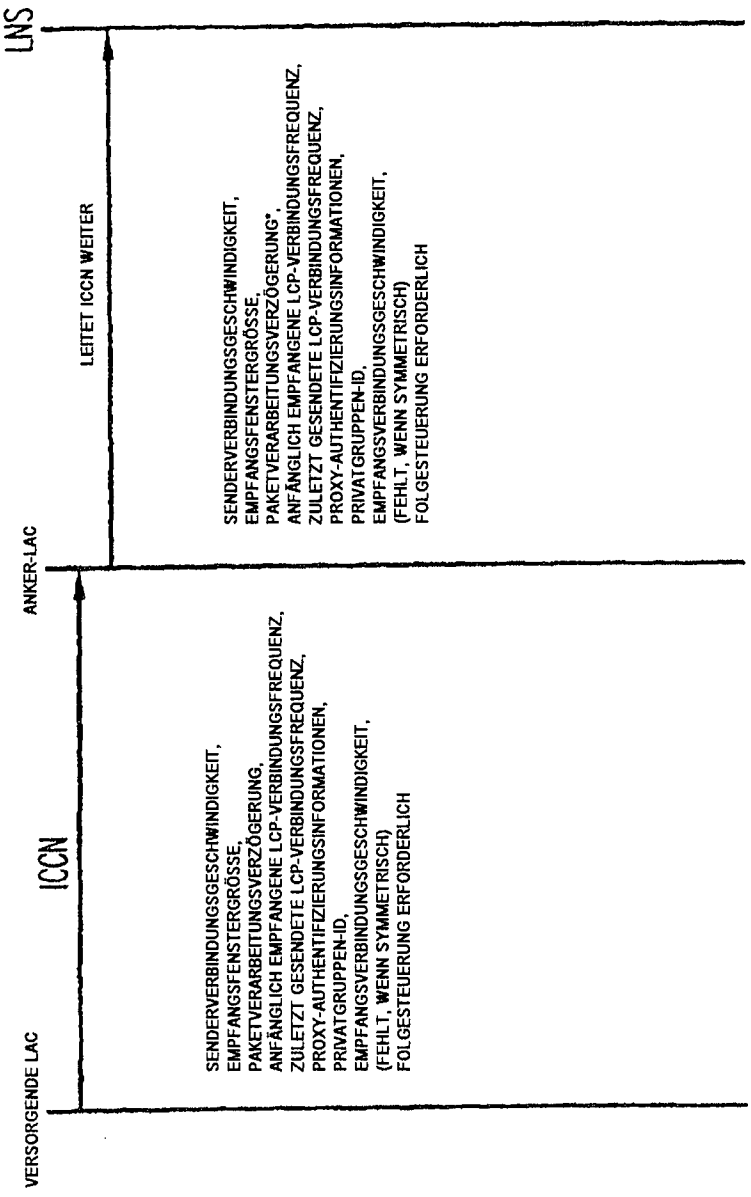

VERSORGENDE LAC
ANKER-LAC
LNS
ICRQ
ZUGEWIESENE VERBINDUNGS-ID,
VERBINDUNGS-SERIENNR.,
GEWÄHLTE NUMMER-DNIS,
WÄHLNUMMER-CLID,
UNTERADRESSE,
VERBORGENES AVP ENTHÄLT
BENUTZERDATEN UND REFERENZEN
LEITET ICRQ WEITER
ZUGEWIESENE VERBINDUNGS-ID",
VERBINDUNGS-SERIENNR.,
GEWÄHLTE NUMMER-DNIS",
WÄHLNUMMER-CLID",
UNTERADRESSE",
VERBORGENES AVP ENTHÄLT
BENUTZERDATEN UND REFERENZEN
VERBORGENES AVP ZEIGT
EMPFANGSFENSTERGRÖSSE AN, DIE
VOM ANKER UNTERSTÜTZT WERDEN KANN
LEITET ICRP WEITER
ICRP
ZUGEWIESENE VERBINDUNGS-ID",
EMPFANGSFENSTERGRÖSSE,
PAKETVERARBEITUNGSVERZÖGERUNG",
ZUGEWIESENE VERBINDUNGS-ID,
EMPFANGSFENSTERGRÖSSE,
PAKETVERARBEITUNGSVERZÖGERUNG,

FIG. 7


VERSORGENDE LAC
ICCN
ANKER-LAC
LNS
LEITET ICCN WEITER
SENDERVERBINDUNGSGESCHWINDIGKEIT,
EMPFANGSFENSTERGRÖSSE,
PAKETVERARBEITUNGSVERZÖGERUNG,
ANFÄNGLICH EMPFANGENE LCP-VERBINDUNGSFREQUENZ,
ZULETZT GESENDETE LCP-VERBINDUNGSFREQUENZ,
PROXY-AUTHENTIFIZIERUNGSINFORMATIONEN,
PRIVATGRUPPEN-ID,
EMPFANGSVERBINDUNGSGESCHWINDIGKEIT,
(FEHLT, WENN SYMMETRISCH)
FOLGESTEUERUNG ERFORDERLICH
SENDERVERBINDUNGSGESCHWINDIGKEIT,
EMPFANGSFENSTERGRÖSSE,
PAKETVERARBEITUNGSVERZÖGERUNG',
ANFÄNGLICH EMPFANGENE LCP-VERBINDUNGSFREQUENZ,
ZULETZT GESENDETE LCP-VERBINDUNGSFREQUENZ,
PROXY-AUTHENTIFIZIERUNGSINFORMATIONEN,
PRIVATGRUPPEN-ID,
EMPFANGSVERBINDUNGSGESCHWINDIGKEIT,
(FEHLT, WENN SYMMETRISCH)
FOLGESTEUERUNG ERFORDERLICH

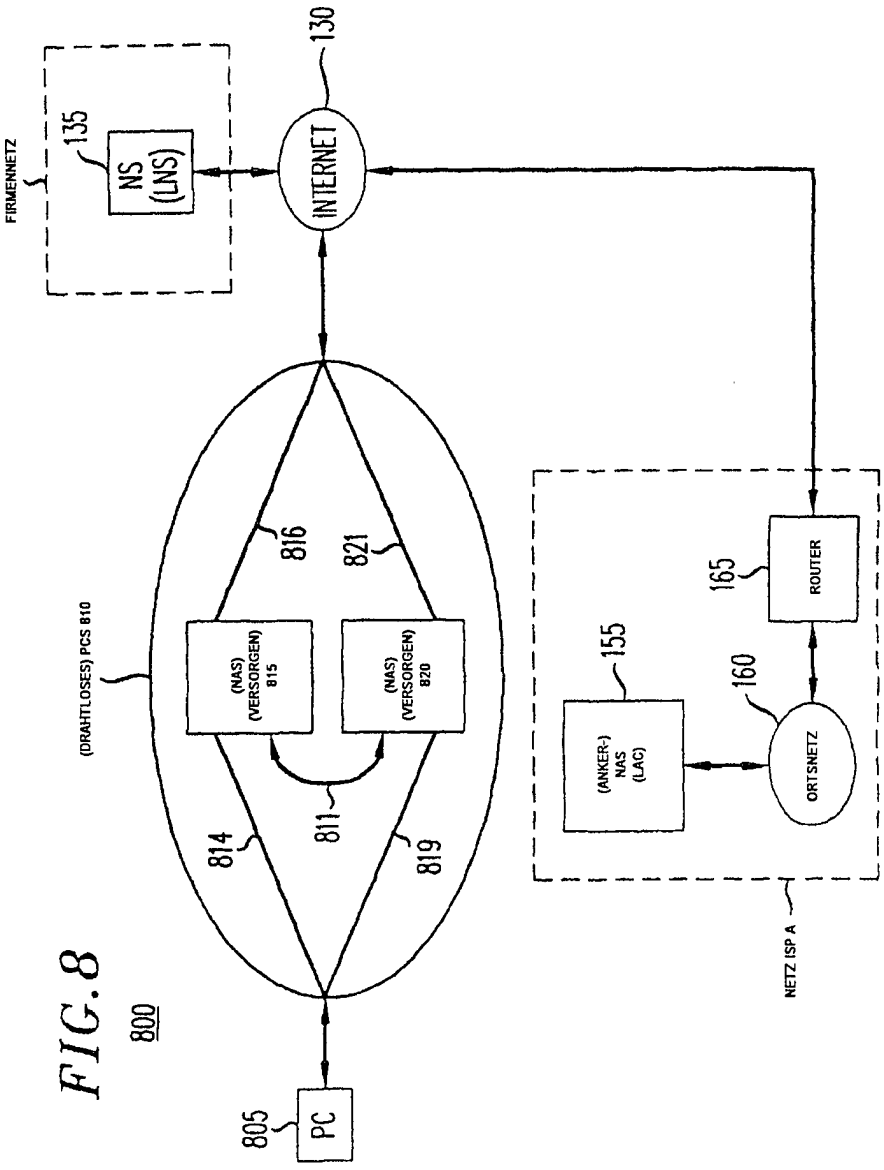

FIRMENNETZ
135
NS
(LNS)
130
INTERNET
816
821
(NAS)
(VERSORGEN)
815
(NAS)
(VERSORGEN)
820
(DRAHTLOSES) PCS 810
811
814
819
805
PC
165
ROUTER
155
160
(ANKER-)
NAS
(LAC)
ORTSNETZ
NETZ ISP A

FIG. 8

800

FIG. 9

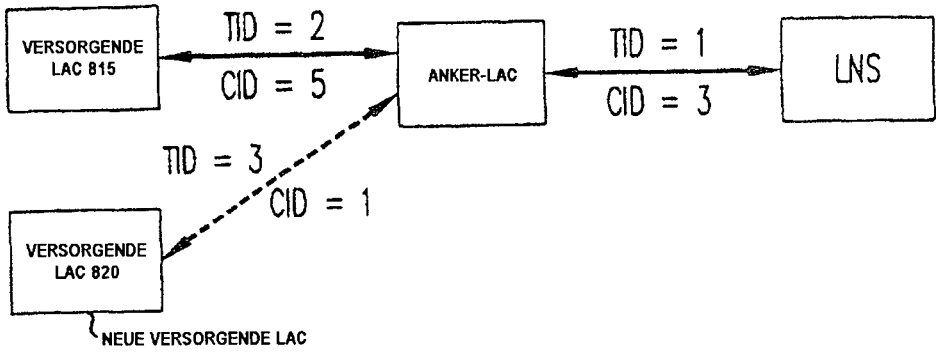


FIG. 13

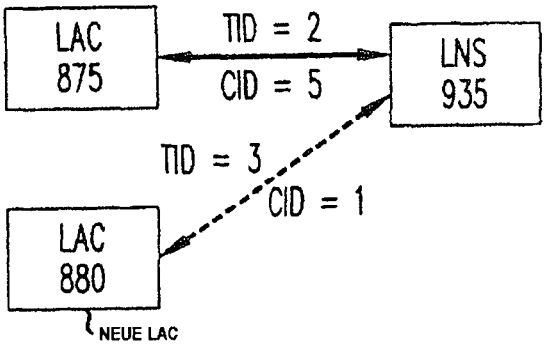


FIG. 16

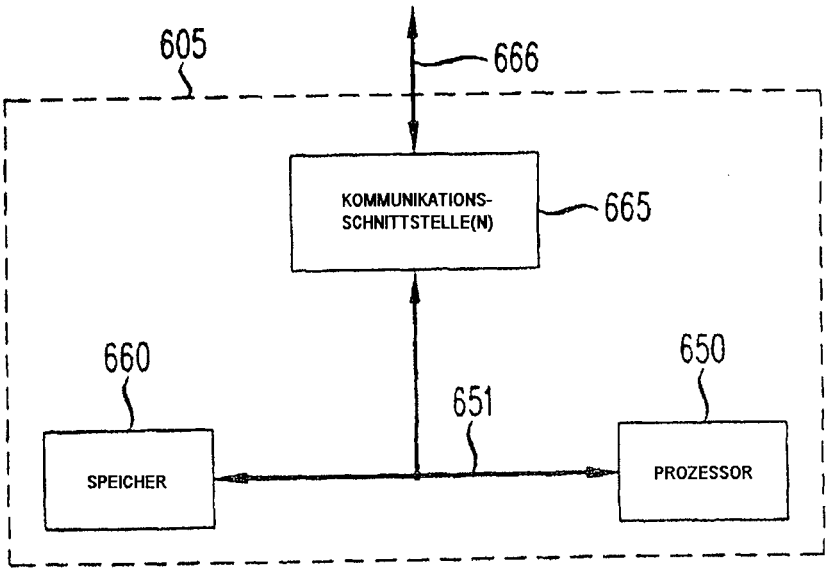


FIG. 10

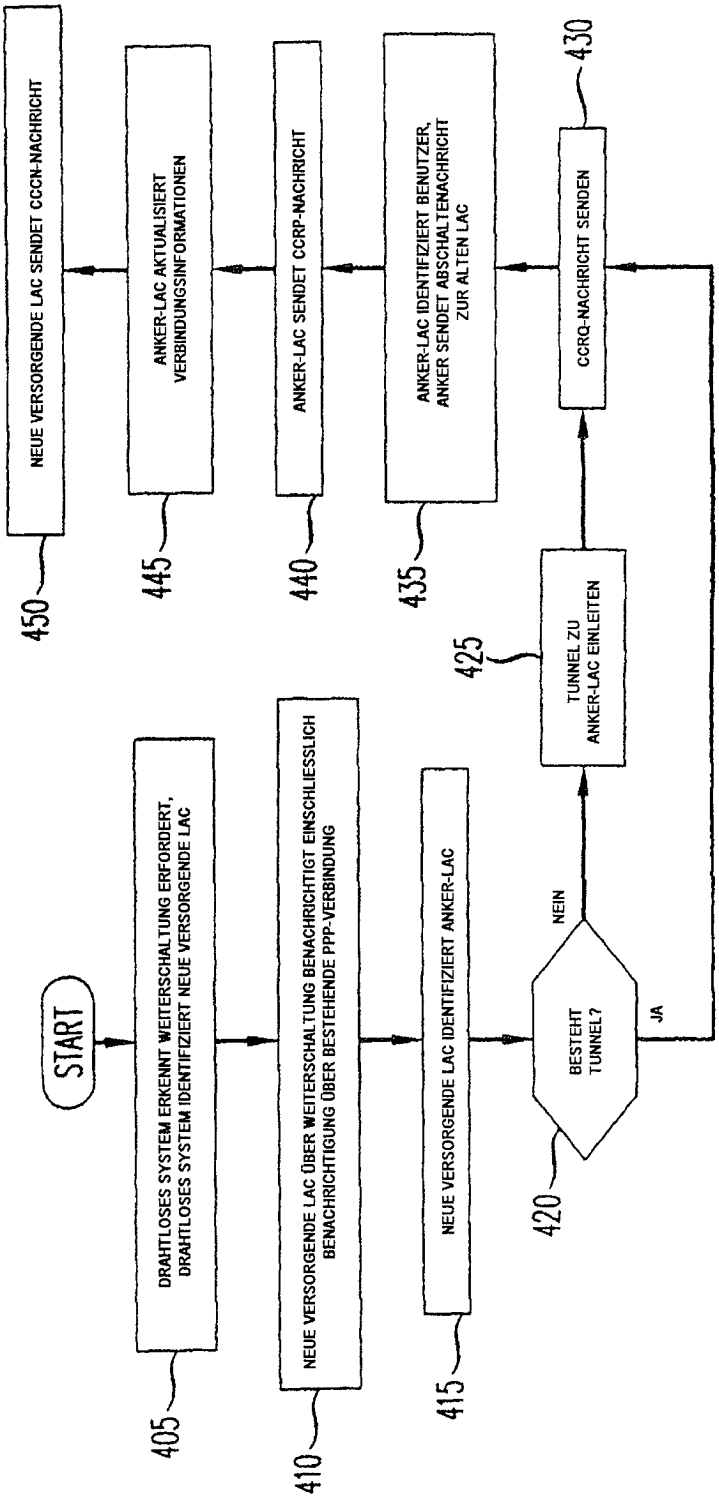

START
DRAHTLOSES SYSTEM ERKENNT WEITERSCHALTUNG ERFORDERT, DRAHTLOSES SYSTEM IDENTIFIZIERT NEUE VERSORGENDE LAC
NEUE VERSORGENDE LAC ÜBER WEITERSCHALTUNG BENACHRICHTIGT EINSCHLIESSLICH BENACHRICHTIGUNG ÜBER BESTEHENDE PPP-VERBINDUNG
NEUE VERSORGENDE LAC IDENTIFIZIERT ANKER-LAC
BESTEHT TUNNEL?
NEIN
JA
TUNNEL ZU ANKER-LAC EINLEITEN
CCRQ-NACHRICHT SENDEN
ANKER-LAC IDENTIFIZIERT BENUTZER, ANKER SENDET ABSCHALTENACHRICHT ZUR ALTEN LAC
ANKER-LAC SENDET CCRP-NACHRICHT
ANKER-LAC AKTUALISIERT VERBINDUNGSINFORMATIONEN
NEUE VERSORGENDE LAC SENDET CCCN-NACHRICHT
405
410
415
420
425
430
435
440
445
450

FIG. 11

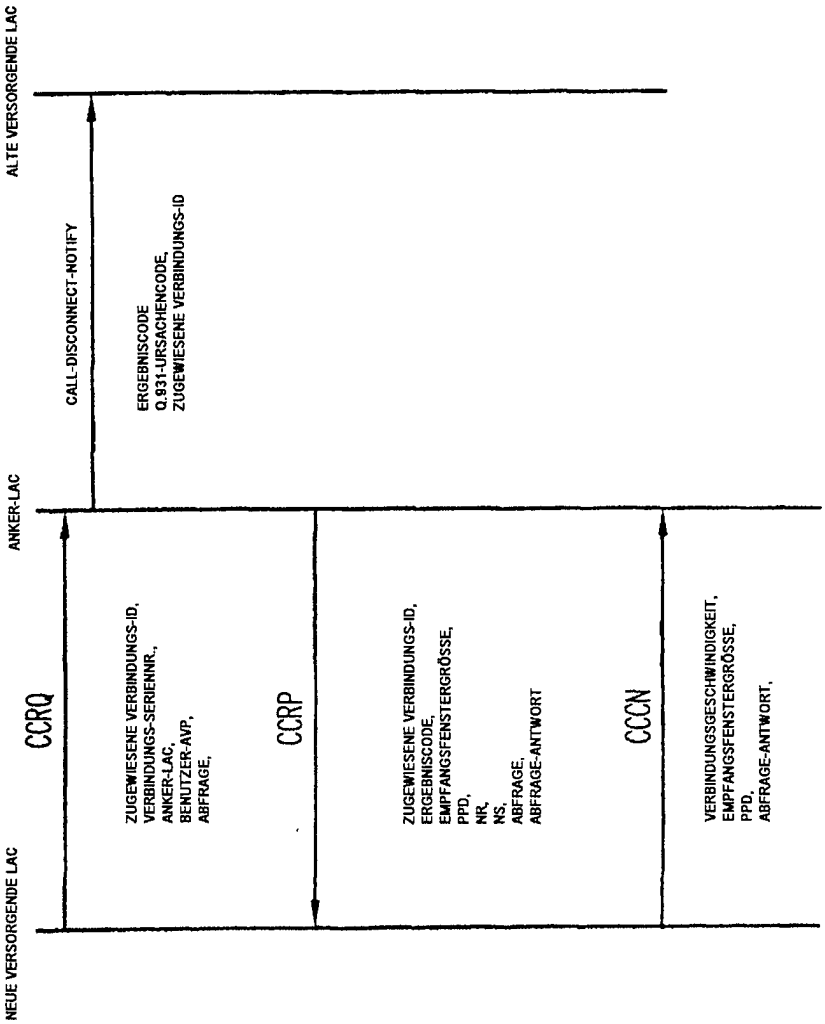

ALTE VERSORGENDE LAC
ANKER-LAC
NEUE VERSORGENDE LAC
CALL-DISCONNECT-NOTIFY
ERGEBNISCODE
Q.931-URSACHENCODE,
ZUGEWIESENE VERBINDUNGS-ID
CCRQ
ZUGEWIESENE VERBINDUNGS-ID,
VERBINDUNGS-SERIENNR.,
ANKER-LAC,
BENUTZER-AVP,
ABFRAGE,
CCRP
ZUGEWIESENE VERBINDUNGS-ID,
ERGEBNISCODE,
EMPFANGSFENSTERGRÖSSE,
PPD,
NR,
NS,
ABFRAGE,
ABFRAGE-ANTWORT
CCCN
VERBINDUNGSGESCHWINDIGKEIT,
EMPFANGSFENSTERGRÖSSE,
PPD,
ABFRAGE-ANTWORT,

FIG. 12

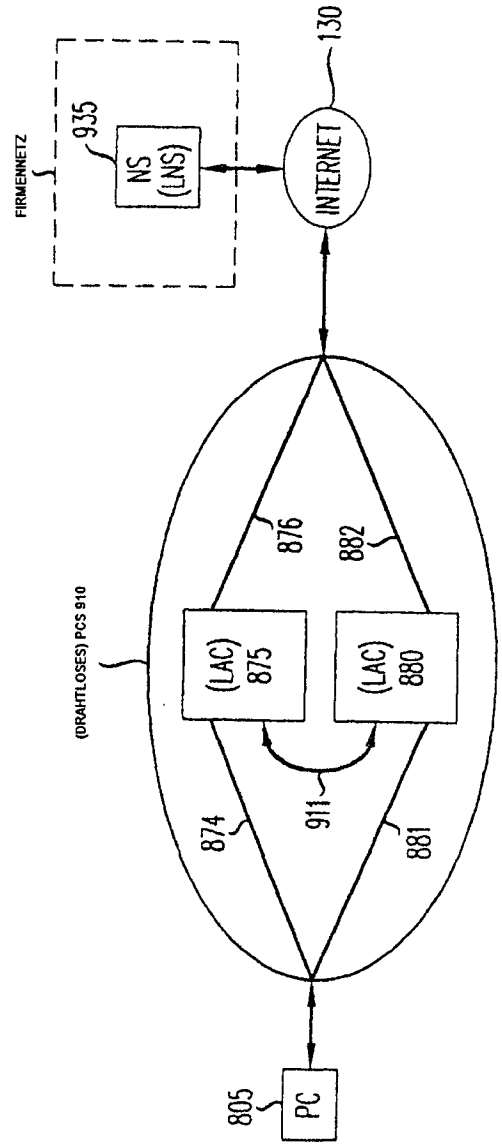

130
INTERNET
FIRMENNETZ
935
NS
(LNS)
(DRAHTLOSES) PCS 910
876
882
(LAC)
875
(LAC)
880
874
911
881
805
PC

FIG. 14

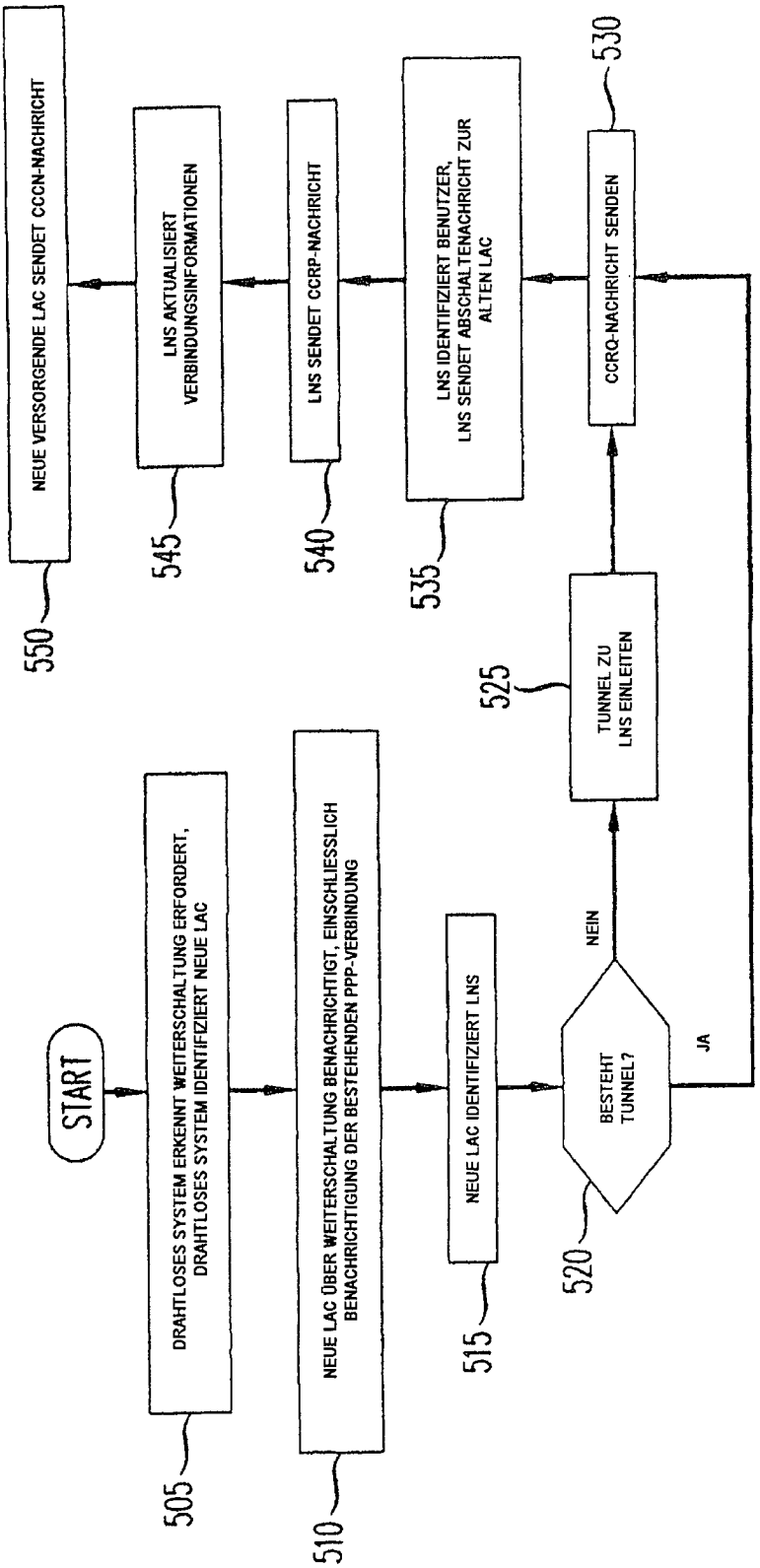

START
DRAHTLOSES SYSTEM ERKENNT WEITERSCHALTUNG ERFORDERT, DRAHTLOSES SYSTEM IDENTIFIZIERT NEUE LAC
505
NEUE LAC ÜBER WEITERSCHALTUNG BENACHRICHTIGT, EINSCHLIESSLICH BENACHRICHTIGUNG DER BESTEHENDEN PPP-VERBINDUNG
510
NEUE LAC IDENTIFIZIERT LNS
515
BESTEHT TUNNEL?
520
NEIN
JA
TUNNEL ZU LNS EINLEITEN
525
LNS IDENTIFIZIERT BENUTZER, LNS SENDET ABSCHALTENACHRICHT ZUR ALTEN LAC
535
LNS SENDET CCRP-NACHRICHT
540
LNS AKTUALISIERT VERBINDUNGSINFORMATIONEN
545
NEUE VERSORGENDE LAC SENDET CCCN-NACHRICHT
550
CCRQ-NACHRICHT SENDEN
530

FIG. 15

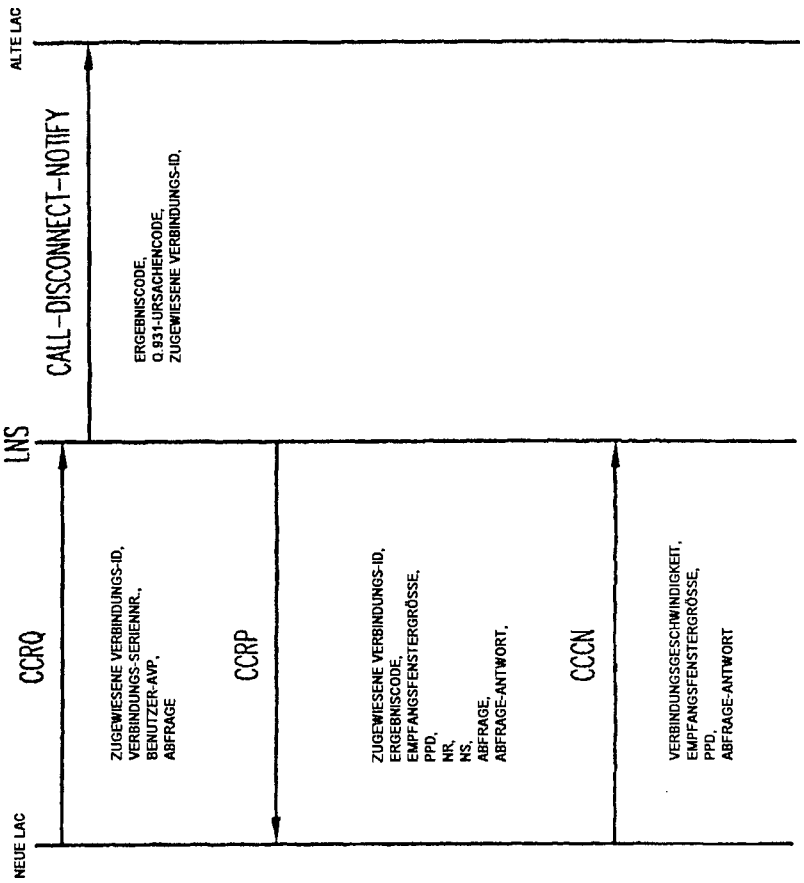

ALTE LAC
LNS
NEUE LAC
CALL-DISCONNECT-NOTIFY
ERGEBNISCODE,
Q.931-URSACHENCODE,
ZUGEWIESENE VERBINDUNGS-ID,
CCRQ
ZUGEWIESENE VERBINDUNGS-ID,
VERBINDUNGS-SERIENNR.,
BENUTZER-AVP,
ABFRAGE
CCRP
ZUGEWIESENE VERBINDUNGS-ID,
ERGEBNISCODE,
EMPFANGSFENSTERGRÖSSE,
PPD,
NR,
NS,
ABFRAGE,
ABFRAGE-ANTWORT,
CCCN
VERBINDUNGSGESCHWINDIGKEIT,
EMPFANGSFENSTERGRÖSSE,
PPD,
ABFRAGE-ANTWORT

FIG. 17

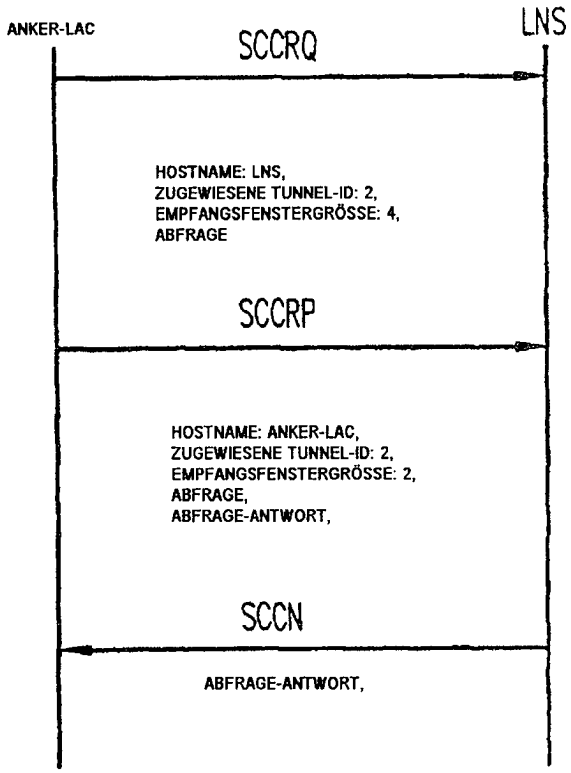
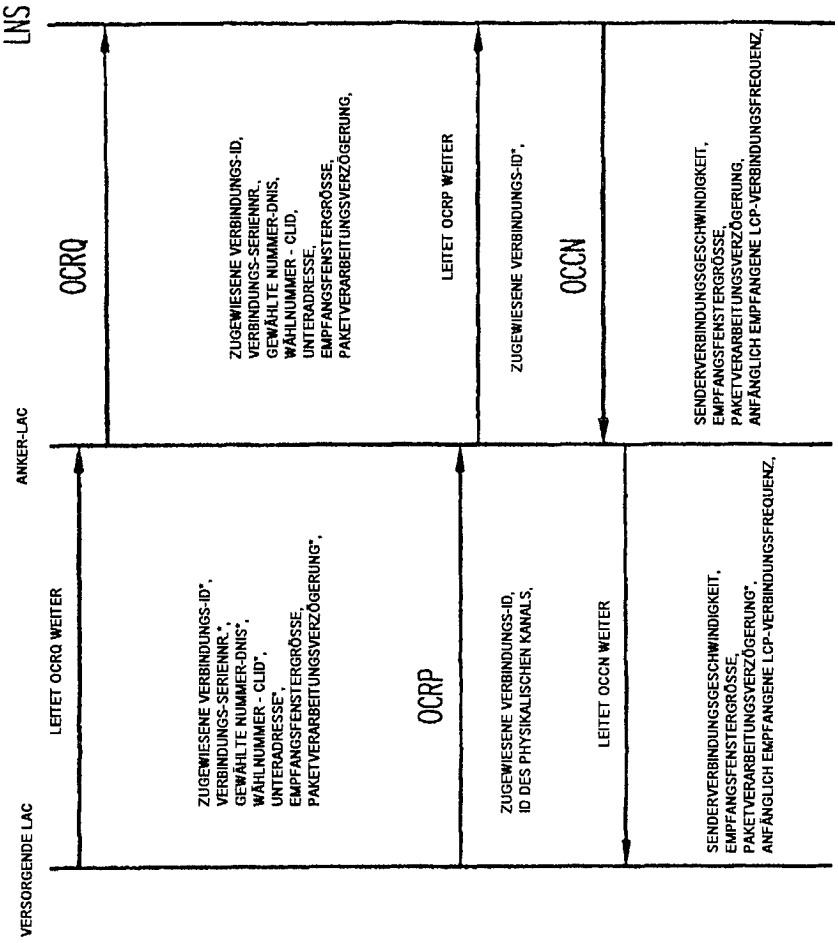

ANKER-LAC
LNS
SCCRQ
HOSTNAME: LNS,
ZUGEWIESENE TUNNEL-ID: 2,
EMPFANGSFENSTERGRÖSSE: 4,
ABFRAGE
SCCRP
HOSTNAME: ANKER-LAC,
ZUGEWIESENE TUNNEL-ID: 2,
EMPFANGSFENSTERGRÖSSE: 2,
ABFRAGE,
ABFRAGE-ANTWORT,
SCCN
ABFRAGE-ANTWORT,

FIG. 18


VERSORGENDE LAC
ANKER-LAC
LNS
LEITET OCRQ WEITER
OCRQ
ZUGEWIESENE VERBINDUNGS-ID,
VERBINDUNGS-SERIENNR.,
GEWÄHLTE NUMMER-DNIS,
WÄHLNUMMER - CLID,
UNTERADRESSE,
EMPFANGSFENSTERGRÖSSE,
PAKETVERARBEITUNGSVERZÖGERUNG,
ZUGEWIESENE VERBINDUNGS-ID*,
VERBINDUNGS-SERIENNR.*,
GEWÄHLTE NUMMER-DNIS*,
WÄHLNUMMER - CLID*,
UNTERADRESSE*,
EMPFANGSFENSTERGRÖSSE,
PAKETVERARBEITUNGSVERZÖGERUNG*,
LEITET OCRP WEITER
OCRP
ZUGEWIESENE VERBINDUNGS-ID*,
OCCN
ZUGEWIESENE VERBINDUNGS-ID,
ID DES PHYSIKALISCHEN KANALS,
LEITET OCCN WEITER
SENDERVERBINDUNGSGESCHWINDIGKEIT,
EMPFANGSFENSTERGRÖSSE,
PAKETVERARBEITUNGSVERZÖGERUNG,
ANFÄNGLICH EMPFANGENE LCP-VERBINDUNGSFREQUENZ,
SENDERVERBINDUNGSGESCHWINDIGKEIT,
EMPFANGSFENSTERGRÖSSE,
PAKETVERARBEITUNGSVERZÖGERUNG*,
ANFÄNGLICH EMPFANGENE LCP-VERBINDUNGSFREQUENZ,