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

(10) **DE 698 37 136 T2** 2007.12.06

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 917 320 B1**
(21) Deutsches Aktenzeichen: **698 37 136.4**
(96) Europäisches Aktenzeichen: **98 308 329.6**
(96) Europäischer Anmeldetag: **13.10.1998**
(97) Erstveröffentlichung durch das EPA: **19.05.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **21.02.2007**
(47) Veröffentlichungstag im Patentblatt: **06.12.2007**

(51) Int Cl.[8]: ***H04L 12/56*** (2006.01)
H04Q 7/22 (2006.01)
H04L 12/46 (2006.01)

(30) Unionspriorität:

61915 P	**14.10.1997**	**US**
138683	**24.08.1998**	**US**

(84) Benannte Vertragsstaaten:
DE, FR, GB, IT, SE

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

(74) Vertreter:
derzeit kein Vertreter bestellt

(72) Erfinder:
Chuah, Mooi Choo, Eaton Town, Monmouth, New Jersey 07724, US; Rai, Girish, Bartlett, Du Page, Illinois 60103, US

(54) Bezeichnung: **Optimierte Leitweglenkung**

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

Allgemeiner Stand der Technik

Gebiet der Erfindung

[0001] Die vorliegende Erfindung betrifft die Verwaltung von mobilen Endsystemen in einem paketvermittelten Datennetz, das Computerbenutzer unter Verwendung von Diensten virtueller Privatnetze über eine paketvermittelte drahtlose Hochgeschwindigkeitsdatenstrecke mit Fernzugang zum Internet und zu privaten Intranets versieht. Insbesondere betrifft die Erfindung die Optimierung der Leitweglenkung von mobilen Endsystemen zu gewünschten Kommunikationsservern.

Beschreibung des Standes der Technik

[0002] Fig. 1 stellt drei Wirtschaftseinheiten und deren Betriebsmittel dar, die in Zusammenarbeit normalerweise einen Internetfernzugang für Benutzercomputer **2** durch Benutzermodems **4** bereitstellen. Die Benutzercomputer **2** und die Modems **4** bilden Endsysteme.

[0003] Die erste Wirtschaftseinheit ist die Telefongesellschaft (Telco für engl. telephone company), die das normale alte Telefonwählsystem (POTS für engl. plain old telephone system) oder diensteintegrierende Datennetz (ISDN für engl. integrated services data network) besitzt und betreibt. Die Telco stellt die Medien in Form des öffentlichen Telefonwählnetzes (PSTN für engl. public switched telephone network) **6** bereit, über welches Bits (oder Pakete) zwischen Benutzern und den beiden anderen Wirtschaftseinheiten fließen können.

[0004] Die zweite Wirtschaftseinheit ist der Internetdiensteanbieter (ISP für engl. internet service provider). Der ISP verwendet und verwaltet einen oder mehr Übergabepunkte (POPs für engl. points of presence) **8** in seinem Dienstbereich, an welche Endbenutzer sich für Netzdienst anschließen. Ein ISP richtet normalerweise in jedem größeren Ortsanschlussbereich, in welchem der ISP erwartet, Kunden zu verpflichten, einen POP ein. Der POP wandelt den Nachrichtenverkehr vom PSTN, das von der Telco geführt wird, in eine digitale Form um, damit er über das Intranetbackbone **10** übertragen wird, das dem ISP gehört oder von einem Intranetbackbone-Anbieter wie der MCI, Inc. gemietet ist. Ein ISP mietet normalerweise fraktionale oder komplette T1-Leitungen oder fraktionale oder komplette T3-Leitungen von der Telco zur Verbindungsfähigkeit mit dem PSTN. Die POPs und das ISP-Medien-Datenzentrum **14** sind über das Intranetbackbone durch einen Router **12A** miteinander verbunden. Das Datenzentrum beherbergt die Webserver, Mailserver, Abrechnungs- und Registrierungsserver des ISPs und befähigt den ISP, Webinhalte, sowie E-Mail- und Webhosting-Dienste für Endbenutzer bereitzustellen. Zukünftige Mehrwertdienste können durch Einsetzen von zusätzlichen Arten von Servern im Datenzentrum hinzugefügt werden. Der ISP unterhält auch den Router **12A** zur Verbindung mit dem öffentlichen Internetbackbone **20**. Im aktuellen Modell für Fernzugang haben Endbenutzer Dienstverhältnisse mit ihrer Telco und ihrem ISP und erhalten für gewöhnlich getrennte Rechnungen von beiden. Endbenutzer greifen durch Anwählen des nächstgelegenen POPs und Ausführen eines Kommunikationsprotokolls, das als das Punkt-zu-Punkt-Protokoll oder PPP (für engl. Point-to-point protocol) der Arbeitsgruppe zur Entwicklung und Koordinierung von Internetprotokollen (IETF für engl. Internet Engineering Task Force) bekannt ist, auf den ISP und durch den ISP auf das öffentliche Internet **20** zu.

[0005] Die dritte Wirtschaftseinheit ist das Privatunternehmen, das aus Geschäftsgründen sein eigenes privates Intranet **18** besitzt und durch den Router **12B** betreibt. Firmenangestellte können durch Durchführen von POTS/ISDN-Anrufen (z.B. von Zuhause oder von unterwegs) zum Fernzugangsserver **16** der Firma und Ausführen des IETF-PPP-Protokolls auf das Firmennetz **18** zugreifen. Für den Firmenzugang zahlen Endbenutzer nur die Kosten für die Verbindung mit dem Fernzugangsserver **16** der Firma. Der ISP ist nicht beteiligt. Das Privatunternehmen unterhält den Router **12B**, um einen Endbenutzer entweder mit dem firmeneigenen Intranet **18** oder dem öffentlichen Internet **20** oder beiden zu verbinden.

[0006] Endbenutzer zahlen der Telco die Kosten für Telefonanrufe und die Kosten für eine Telefonleitung zu ihnen nach Hause. Endbenutzer bezahlen auch den ISP für den Zugang zum Netz und den Diensten des ISPs. Die vorliegende Erfindung kommt Drahtlosdiensteanbietern wie Sprint PCS, PrimeCo usw. zugute, und sie kommt auch Internetdiensteanbietern wie AOL, AT&T Worldnet usw. zugute.

[0007] Heutzutage bieten Internetdiensteanbieter Endbenutzern Internetzugangsdienste, Webinhaltsdienste, E-Mail-Dienste, Contenthosting-Dienste und Roaming an. Aufgrund kleiner Gewinnspannen und in Ermangelung eines Rahmens zur Durchführung einer Marktsegmentierung auf der Basis von Merkmalen und Preisen

suchen ISPs nach Mehrwertdiensten zur Verbesserung der Gewinnspannen. Kurzfristig werden Betriebsmittelhersteller imstande sein, den ISPs Lösungen anbieten, damit sie schnelleren Zugang, Vernetzung virtueller Privatnetze (was die Fähigkeit ist, öffentliche Netze sicher als Privatnetze zu verwenden und mit Intranets zu verbinden), Roaming-Konsortien, Push-Techniken und Dienstgüte anbieten können. Längerfristig werden auch Sprachübertragung über Internet und Mobilität angeboten. Die ISPs werden diese Mehrwertdienste verwenden, um der Zwangsjacke kleiner Gewinnspannen zu entrinnen. Viele dieser Mehrwertdienste fallen in die Kategorie von Netzdiensten und können nur durch die Netzinfrastrukturbetriebsmittel angeboten werden. Andere fallen in die Kategorie von Anwendungsdiensten, welche die Unterstützung von der Netzinfrastruktur benötigen, während andere keine Unterstützung von der Netzinfrastruktur benötigen. Dienste wie schnellerer Zugang, Vernetzung virtueller Privatnetze, Roaming, Mobilität, Sprache, Dienstgüte und dienstgütebasierte Abrechnung benötigen alle eine verbesserte Netzinfrastruktur. Die Erfindung, die hier beschrieben wird, stellt diese verbesserten Dienste entweder direkt bereit, oder sie stellt Gabeln bereit, damit diese Dienste als zukünftige Verbesserungen später hinzugefügt werden können. Drahtlosdiensteanbieter werden imstande sein, einen größeren Anteil am Ertragsstrom zu gewinnen. Der ISP wird imstande sein, mehr Dienste mit einer besseren Marktsegmentierung anzubieten.

[0008] Der Stand der Technik von Interesse, der mit dem erfinderischen Gegenstand in Beziehung steht, ist Folgender:
EP 0 697 798, eingereicht am 21. Februar 1996, offenbart eine Verbesserung für ein drahtloses Paketdatenübertragungssystem, indem einem Teilnehmer, der ein mobiles Endsystem (M-ES) (**205**) verwendet, die Möglichkeit gegeben wird, den Verbindungsnetzbetreiber (IXC) (**222** oder **224**) auszuwählen, der die Daten während einer bestimmten Kommunikationssitzung über jene Netzwege überträgt, für welche der Teilnehmer die Kosten trägt. Das System ermöglicht es dem Teilnehmer, einen bevorzugten Verbindungsnetzbetreiber in einem optionalen Bevorzugter-IXC-Feld, das einer Begrüßungsnachricht des Endsystems hinzugefügt wird, zu spezifizieren. Während der Registrierungs- und Berechtigungsprozeduren wird in einem Bevorzugter-IXC-Feld, das standardmäßigen Registrierungsprotokollnachrichten hinzugefügt wird, eine Kennung, die dem bevorzugten Verbindungsnetzbetreiber entspricht, zwischen einem versorgenden mobilen Datentransitsystem (MD-IS) (**220**) und einem Heimat-MD-IS (**240**) übertragen. Wenn der Teilnehmer in dem Bevorzugter-IXC-Feld einen bevorzugten Verbindungsnetzbetreiber spezifiziert hat, dann wird diesem bevorzugten Verbindungsnetzbetreiber eine höhere Priorität eingeräumt als einem vorgegebenen bevorzugten Verbindungsnetzbetreiber, der ausgewählt wird, wenn der Teilnehmer die Netzdienste abonniert. Jedes MD-IS wird mit einer neuen Datenbank (**221**, **241**) versehen, welche Verbindungsnetzbetreiberkennungen in eine entsprechende Grenzrouteradresse abbildet, die dem bevorzugten Verbindungsnetzbetreiber zugeordnet wird, um Datenpakete über den vom Teilnehmer bevorzugten IXC zu leiten. Demnach ermöglicht das System es, Daten auf einer Pro-Sitzung-Basis sowohl auf Wegen in der Vorwärts- als auch der Rückwärtsrichtung über den vom Teilnehmer bevorzugten Verbindungsnetzbetreiber zu senden.

[0009] WO 96/21983 offenbart eine protokollabhängige Leitweglenkung von Datenpaketen zwischen einer Mobilstation eines Paketfunknetzes und einem Gesprächspartner (Host), der mit einem externen Netz verbunden ist. Ein Datenpaket eines fremden Protokolls (IPX) wird durch ein Paketfunknetz, das ein zweites Protokoll (X.25) verwendet, als in einem Datenpaket gemäß dem zweiten Protokoll eingekapselt übertragen. Das übertragende Paketfunknetz braucht das Protokoll des übertragenen fremden Datenpakets demnach weder zu verstehen, noch muss es die Inhalte des Datenpakets interpretieren können. Ein Datenpaketnetz ist mit anderen Paketfunknetzen, Datennetzen oder dem Backbone-Netz zwischen Paketdatennetzen über einen Netzübergangsknoten (GPRS GSN) verbunden, welcher das netzinterne Protokoll (X.25) zum dedizierten Paketnetz und das Protokoll jedes Netzes zu anderen Netzen verwendet. Wenn ein Datenpaket über einen Netzübergangsknoten von einem Netz in ein anderes Netz übertragen wird, wird das Datenpaket in einem Paket gemäß dem Protokoll des neuen Netzes eingekapselt. Wenn das eingekapselte Datenpaket in einem Knoten ankommt, welcher das Protokoll des eingekapselten Datenpakets unterstützt, wird die Einkapselung abgestreift, und das Datenpaket wird gemäß dem Protokoll des Datenpakets weitergesendet.

KURZDARSTELLUNG DER ERFINDUNG

[0010] Ein Verfahren und eine Vorrichtung gemäß der vorliegenden Erfindung werden in den unabhängigen Ansprüchen dargelegt, auf welche der Leser nun verwiesen wird. Bevorzugte Merkmale werden in den abhängigen Ansprüchen angeführt.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0011] Die Erfindung wird in der folgenden Beschreibung von bevorzugten Ausführungsforen unter Bezug-

nahme auf die folgenden Figuren ausführlich beschrieben, wobei:

[0012] Fig. 1 ein Konfigurationsdiagramm einer bekannten Fernzugangsarchitektur durch ein öffentliches Telefonwählnetz ist;

[0013] Fig. 2 ein Konfigurationsdiagramm einer Fernzugangsarchitektur durch ein drahtloses paketvermitteltes Datennetz gemäß der vorliegenden Erfindung ist;

[0014] Fig. 3 eine Endsystemkonfiguration gemäß einer Ausführungsform der vorliegenden Erfindung veranschaulicht;

[0015] Fig. 4 eine andere Endsystemkonfiguration gemäß einer Ausführungsform der vorliegenden Erfindung veranschaulicht;

[0016] Fig. 5 eine andere Endsystemkonfiguration gemäß einer Ausführungsform der vorliegenden Erfindung veranschaulicht;

[0017] Fig. 6 ein Konfigurationsdiagramm von ausgewählten Teilen der Architektur des Netzes von Fig. 2 ist, das ein Roaming-Szenarium darstellt;

[0018] Fig. 7 ein Konfigurationsdiagramm einer Basisstation mit lokalen Zugangspunkten ist;

[0019] Fig. 8 ein Konfigurationsdiagramm einer Basisstation mit abgesetzten Zugangspunkten ist;

[0020] Fig. 9 ein Konfigurationsdiagramm einer Basisstation mit abgesetzten Zugangspunkten ist, von welchen einige unter Verwendung einer drahtlosen Trunk-Verbindung angeschlossen sind;

[0021] Fig. 10 ein Diagramm eines Protokollstapels für einen lokalen Zugangspunkt ist;

[0022] Fig. 11 ein Diagramm eines Protokollstapels für einen abgesetzten Zugangspunkt mit einem drahtlosen Trunk ist;

[0023] Fig. 12 ein Diagramm eines Protokollstapels für eine Relaisfunktion in der Basisstation zur Unterstützung von abgesetzten Zugangspunkten mit drahtlosen Trunks ist;

[0024] Fig. 13 ein Diagramm von Protokollstapeln zur Implementierung der Relaisfunktion ist, die in Fig. 12 dargestellt ist;

[0025] Fig. 14 ein Diagramm von Protokollstapeln für eine Relaisfunktion in der Basisstation zur Unterstützung von lokalen Zugangspunkten ist;

[0026] Fig. 15 ein Konfigurationsdiagramm von ausgewählten Teilen der Architektur des Netzes von Fig. 2 ist, das ein erstes Endsystem, das sich im Heimatnetznetz vom Heimatnetz registrieren lässt, und ein zweites System, das sich im Heimatnetz von einem Fremdnetz unter Verwendung einer Heimatnetzübergangsfunktion für einen Anker registrieren lässt, darstellt;

[0027] Fig. 16 ein Konfigurationsdiagramm von ausgewählten Teilen der Architektur des Netzes von Fig. 2 ist, das ein erstes Endsystem, das sich im Heimatnetznetz vom Heimatnetz registrieren lässt, und ein zweites System, das sich im Heimatnetz von einem Fremdnetz unter Verwendung einer versorgenden Netzübergangsfunktion für einen Anker registrieren lässt, darstellt;

[0028] Fig. 17 ein Leiterdiagramm der Aufforderungs- und Antwortnachrichten zum Registrieren in einem Heimatnetz von einem Fremdnetz und Aufbauen, Authentifizieren und Konfigurieren einer Datenstrecke ist;

[0029] Fig. 18 ein Konfigurationsdiagramm von ausgewählten Teilen der Architektur des Netzes von Fig. 2 ist, das Registrierungsaufforderungen und -antworten zum Registrieren einer Mobileinheit in einem Heimatnetz vom Heimatnetz darstellt;

[0030] Fig. 19 ein Konfigurationsdiagramm von ausgewählten Teilen der Architektur des Netzes von Fig. 2 ist, das Registrierungsaufforderungen und -antworten zum Registrieren einer Mobileinheit in einem Heimatnetz

von einem Fremdnetz darstellt;

[0031] Fig. 20 ein Konfigurationsdiagramm von Protokollstapeln ist, das Kommunikationen zwischen einem Endsystem in einem Heimatnetz und einer Netzübergangsfunktion im Heimatnetz darstellt, wobei der Zellenstandort lokale Zugangspunkte aufweist;

[0032] Fig. 21 ein Konfigurationsdiagramm von Protokollstapeln ist, das Kommunikationen zwischen einem Endsystem in einem Heimatnetz und einer Netzübergangsfunktion im Heimatnetz darstellt, wobei der Zellenstandort abgesetzte Zugangspunkte aufweist, die durch einen drahtlosen Trunk mit einem drahtlosen Hub verbunden sind;

[0033] Fig. 22 ein Konfigurationsdiagramm von Protokollstapeln ist, das Kommunikationen zwischen einer Basisstation, die mit einem Gast-Endsystem gekoppelt ist, und einer Heimatnetzübergangsfunktion darstellt;

[0034] Fig. 23 ein Konfigurationsdiagramm von Protokollstapeln ist, das Kommunikationen eines Endsystems in einem Heimatnetz durch eine Netzübergangsfunktion im Heimatnetz mit einem Internetdiensteanbieter darstellt;

[0035] Fig. 24 ein Konfigurationsdiagramm von Protokollstapeln ist, das Kommunikationen zwischen einem Endsystem in einem Fremdnetz und einem Heimatregistrierungsserver in einem Heimatnetz während der Registrierungsphase darstellt;

[0036] Fig. 25 ein Verarbeitungsflussdiagramm ist, das die Verarbeitung von Abrechungsdaten durch das Kundengebührenverrechnungssystem darstellt;

[0037] Fig. 26 und Fig. 27 Leiterdiagramme sind, die den Registrierungsprozess für ein Endsystem in einem Heimatnetz beziehungsweise in einem Fremdnetz veranschaulichen;

[0038] Fig. 28 und Fig. 29 Protokollstapeldiagramme sind, die eine Endsystemverbindung in einem Heimatnetz darstellen, wobei ein PPP-Protokoll in einer Netzübergangsfunktion des Heimatnetzes endet beziehungsweise das PPP-Protokoll in einem ISP oder einem Intranet endet;

[0039] Fig. 30 und Fig. 31 Protokollstapeldiagramme sind, die eine Endsystemverbindung in einem Fremdnetz darstellen, wobei ein PPP-Protokoll in einer Netzübergangsfunktion des Fremdnetzes endet beziehungsweise das PPP-Protokoll in einem ISP oder einem Intranet endet;

[0040] Fig. 32, Fig. 33 und Fig. 34 Leiterdiagramme sind, die ein lokales Weiterschaltszenarium, ein Mikro-Weiterschaltszenarium beziehungsweise ein Makro-Weiterschaltszenarium veranschaulichen;

[0041] Fig. 35 ein Leiterdiagramm ist, das ein globales Weiterschaltszenarium veranschaulicht, wobei der fremde Registrierungsserver wechselt und wobei die Heimatnetzübergangsfunktion nicht wechselt;

[0042] Fig. 36 ein Leiterdiagramm ist, das ein globales Weiterschaltszenarium veranschaulicht, wobei sowohl der fremde Registrierungsserver als auch die Heimatnetzübergangsfunktion wechseln;

[0043] Fig. 37 und Fig. 38 Systemkonfigurationsdiagramme sind, welche mögliche Verbindungen veranschaulichen; und

[0044] Fig. 39 bis Fig. 42 verschiedene Weiterschaltszenarien veranschaulichen.

AUSFÜHRLICHE BESCHREIBUNG VON BEVORZUGTEN AUSFÜHRUNGSFORMEN

[0045] Die vorliegende Erfindung versieht Computerbenutzer mit Fernzugang zum Internet und zu privaten Intranets unter Verwendung von Diensten virtueller Privatnetze über eine paketvermittelte drahtlose Hochgeschwindigkeitsdatenstrecke. Diese Benutzer sind imstande, über eine drahtlose Verbindung auf das öffentliche Internet, private Intranets und ihre Internetdiensteanbieter zuzugreifen. Das Netz unterstützt Roaming, das heißt die Fähigkeit, auf das Internet und private Intranets unter Verwendung von Diensten virtueller Privatnetze von überall zuzugreifen, wo die Dienste, die durch die vorliegende Erfindung angeboten werden, verfügbar sind. Das Netz unterstützt auch Weiterschaltungen, das heißt die Fähigkeit, den Anschlusspunkt des Benutzers zum Netz zu wechseln, ohne die PPP-Verbindung zwischen dem PPP-Client und dem PPP-Server zu stö-

ren. Das Netz zielt auf Benutzer ab, die horizontale Internet- und Intranetanwendungen ausführen. Diese Anwendungen umfassen elektronische Post, Dateitransfer, browserbasierten WWW-Zugang und andere kommerzielle Anwendungen, die rund um das Internet eingerichtet sind. Da das Netz auf den IETF-Standards basieren wird, ist es möglich, Streaming-Media-Protokolle, wie RTP, und Konferenzprotokolle, wie H.323, über das Netz aus zuführen.

[0046] Andere Internetfernzugangstechniken, die bereits eingesetzt werden oder in verschiedenen Einsatzstufen sind, umfassen: Drahtleitungseinwahlzugang auf der Basis von POTS und ISDN, XDSL-Zugang, drahtlosen leitungsvermittelten Zugang auf der Basis von GSM/CDMA/TDMA, drahtlosen paketvermittelten Zugang auf der Basis von GSM/CDMA/TDMA, Kabelmodems und satellitenbasierte Systeme. Die vorliegende Erfindung bietet jedoch niedrige Einsatzkosten, Wartungsfreundlichkeit, einen umfassenden Merkmalssatz, Skalierbarkeit, eine Fähigkeit zum sanften Leistungsabfall unter Bedingungen starker Belastung und Unterstützung für verbesserte Netzdienste wie Vernetzung virtueller Privatnetze, Roaming, Mobilität und Dienstgüte zum jeweiligen Nutzen von Benutzern und Diensteanbietern.

[0047] Was Drahtlosdiensteanbieter betrifft, die ein persönliches Kommunikationssystemsspektrum (PCS für engl. personal communications system) besitzen, so befähigt die vorliegende Erfindung sie, drahtlose paketvermittelte Datenzugriffsdienste anzubieten, die mit den Diensten konkurrieren können, die durch die traditionellen Drahtleitungs-Telcos bereitgestellt werden, die das PSTN besitzen und betreiben. Drahtlosdiensteanbieter können auch beschließen, selbst Internetdiensteanbieter zu werden, in welchem Fall sie das ganze Netz besitzen und betreiben und für Benutzer Ende-zu-Ende-Dienste bereitstellen.

[0048] Was Internetdiensteanbieter betrifft, so ermöglicht die vorliegende Erfindung es ihnen, die Telcos zu umgehen (vorausgesetzt, sie kaufen oder mieten das Spektrum) und Benutzern direkte Ende-zu-Ende-Dienste anzubieten, vielleicht unter Einsparung von Zugangsgebühren für die Telcos, was in Zukunft noch zunehmen kann, da das Internet wächst, um noch größer zu werden, als es jetzt schon ist.

[0049] Die vorliegende Erfindung ist flexibel, so dass sie Drahtlosdiensteanbietern zugute kommen kann, die keine Internetdiensteanbieter sind und Endbenutzern nur ISP-, Internet- oder privaten Intranetzugang verschaffen. Die Erfindung kann auch Diensteanbietern zugute kommen, die für Endbenutzer drahtlosen Zugang und Internetdienste bereitstellen. Die Erfindung kann auch Diensteanbietern zugute kommen, die drahtlosen Zugang und Internetdienste bereitstellen, aber auch zulassen, den drahtlosen Abschnitt des Netzes zum Zugang zu anderen ISPs oder zu privaten Intranets zu verwenden.

[0050] In Fig. 2 schließen sich Endsysteme **32** (z.B. basierend auf einem Win **95** Personalcomputer) unter Verwendung von externen oder internen Modems an ein drahtloses Netz **30** an. Diese Modems ermöglichen es Endsystemen, Medienzugriffssteuerungs- oder MAC-Rahmen (MAC für engl. medium access control) über eine Luftverbindung **34** zu senden und zu empfangen. Externe Modems sind über eine drahtgebundene oder drahtlose Verbindung an den PC angeschlossen. Externe Modems sind ortsfest und zum Beispiel ortsgleich mit Richtantennen, die auf dem Dach montiert sind, untergebracht. Externe Modems können unter Verwendung jedes der folgenden Mittel mit dem PC eines Benutzers verbunden werden: 802.3, universeller serieller Bus, paralleler Port, Infrarot oder sogar eine ISM-Funkverbindung. Interne Modems sind vorzugsweise PCMCIA-Karten für Laptops und werden in die Rückwandplatine des Laptops gesteckt. Unter Verwendung von kleinen Allrichtungsantennen senden und empfangen sie MAC-Rahmen über die Luftverbindung.

[0051] Das Endsystem besteht aus den Betriebsmitteln, die sich am Aufenthaltsort des Teilnehmers befinden. Im Falle einer festen Installation besteht das Endsystem aus einer Dachantenne, Funkkomponenten, Digitalkomponenten und schließlich einem Tischcomputer. Es ist anzunehmen, dass ein Teilnehmer den Tischcomputer bereits besitzt, weshalb das drahtlose System durch Standardschnittstellen mit dem PC verbunden werden muss. Fig. 3 bis Fig. 5 veranschaulichen verschiedene Optionen für typische feste Installationen des drahtlosen Systems. Jede der Wahlmöglichkeiten, die in diesen Figuren umrissen werden, hat Konsequenzen, die damit verbunden sind und von den Installationskosten, den Betriebsmittelkosten und der praktischen Installation bis hin zu umgebungsbedingten bei der Installation reichen, was im Folgenden erörtert wird.

[0052] Die Installation, die in Fig. 3 dargestellt ist, ist gegenwärtig die billigste. Bei dieser Konfiguration ist nur eine Antenne **21** außen angeordnet, und ein HF-Kabel **22** ist mit dem Funkgerät **23** verbunden. Der Installierer, entweder der bezahlte Fachmann oder der Teilnehmer, muss nur die Antenne **21** auf dem Dach oder auf der Seite des Gebäudes installieren und ein billiges externes Kabel **22** entlang des Gebäudes zu einer Einführstelle hinab lassen, normalerweise durch ein Loch im Eck eines Fensterrahmens oder durch ein Loch in der Wand in der Nähe eines inneren Fußbodens. Das Funkgerät **23** ist extern vom Tischcomputer **24** mit einer PCM-

CIA-Schnittstelle zum PC **24**. Verluste bei langen HF-Kabelverläufen für Benutzer, die sich an entfernten Punkten vom Zugangspunkt befinden, können mit in Reihe geschalteten bidirektionalen HF-Verstärkern kompensiert werden. Benutzer in der Nähe des Zugangspunkts können die zusätzlichen Verluste von langen Kabelverläufen tolerieren, da ihre Ausbreitungsverluste nicht so groß wie bei Benutzern am Rand der Zelle sind.

[0053] Eine andere Anordnung, die in Fig. 4 veranschaulicht ist, bezieht die Integration der Funkelektronik und der Antenne in ein gemeinsames Gerät **25** ein. Die Verbindung mit dem PC **24** wäre durch eine proprietäre Schnittstelle und PCMCIA. Leistung würde dem Gerät von einem Wandtransformator **27** über eine mehrfach verdrillte Doppelleitung **26** zugeführt werden, welche sowohl Leistung als auch digitale Daten befördert. Die Schwierigkeiten beim Konstruieren eines integrierten Geräts umfassen Wetterfestigkeit, Erwärmung und Kühlung, sowie Servertemperaturextreme.

[0054] Eine andere Anordnung besteht aus einer Außenantenne und einer im Dachgeschoss montierten Teilnehmereinheit. Dies verringert einige der Anforderungen hinsichtlich niedriger Temperatur und Wetterfestigkeit, aber es muss eine Kühlung bereitgestellt werden. Die Teilnehmereinheit wird dann über ein Kabel mit dem PC verbunden.

[0055] Das letzte und teuerste Mittel, durch welches die digitalen Daten vom Funkgerät zu einem Computer oder mehreren Computern übertragen werden, ist die Verwendung eines ISM-Band-LANs, wie beispielsweise des WaveLANs, wie in Fig. 5 dargestellt. Die Antenne **21** befindet sich auf dem Dach, wie bei der vorherigen Installation, und das Funkgerät kann bei der Antenne oder sonst irgendwo angeordnet sein. Eine 802.3 Verbindung verbindet das Funkgerät mit einem Zugangspunkt des drahtlosen LANs. Jedes der abgesetzten Computergeräte innerhalb des Hauses hat nun Zugang zum drahtlosen LAN **28**. Idealerweise sollte die Antenne **29** des Zugangspunkts des drahtlosen LANs eine Richtantenne sein, die im Gebäude hoch angeordnet ist und nach unten zeigt, um eine Versorgung für das Haus bereitzustellen, während eine HF-Streuung außerhalb des Hauses minimiert wird. Das Anordnen der Antenne im Dachgeschoss wirft verschiedene Probleme von der Speisung des Geräts im Dachgeschoss bis hin zur Kühlung der LAN-Funkgeräte auf. In der Praxis scheint es, dass eine LAN-Antenne, die irgendwo im Haus angeordnet ist, akzeptabel ist, solange die Längen der LAN-Zugangspunktantennenkabel kurz sind.

[0056] Es kann eine Notwendigkeit bestehen, Gastteilnehmer zu versorgen, die entscheiden, ihren Laptopcomputer aus ihrem Heimatversorgungsbereich in einen anderen Versorgungsbereich mitzunehmen. Der Laptopbenutzer muss eine Flachplatten-Richtantenne verwenden, welche zu den Zugangspunkten gerichtet ist. Die Ausrichtung des Zugangspunkts ist für die Gewährleistung der Dienstgüte entscheidend. Als Teil der Laptopsoftware bietet ein Ausrichtungsindikator Führung beim Ausrichten der Antenne.

[0057] Es ist vorgesehen, dass die Antenne ungefähr ½ oder ¾ Inch dick ist und eine Öffnung von ungefähr derselben Größe wie der Laptop (8 ½" × 11") aufweist. Einige Mittel zum vorübergehenden Befestigen der Antennenplatte auf der Rückseite des Laptops, wie beispielsweise Klettverschlüsse, sind für den Transport der Antenne zweckmäßig. Sobald der Laptopbenutzer am Aufenthaltsort ankommt, wo der Zugang gewünscht wird, kann die Antenne entweder von der Rückseite des Laptops abgenommen und für die beste Leistung orientiert oder in Bereichen mit sehr starken Signalen am Laptop befestigt gelassen werden. Die Laptopantenne kann mit einem biaxialen Ausrichtungsmechanismus, welcher den Azimut und die Höhe der Antenne ändert, sogar gelenkig mit dem Laptop verbunden werden. Die Antennenplatten unterstützen eine 45° geneigte Doppelpolarisation mit konischen Strahlenformen, um jegliche Ausbreitungseffekte zu eliminieren, welche die Signalqualität beeinflussen können. Da außerdem die Strahlenformen bei Doppelpolarisation konisch sind, sollte die Lage der Antenne auf beiden Seiten die Signalqualität nicht ändern.

[0058] Eine weiträumige drahtlose Versorgung wird durch Basisstationen **36** bereitgestellt. Die Versorgungsreichweite, der durch die Basisstationen **36** bereitgestellt wird, hängt von Faktoren wie Streckenbilanz, Kapazität und Versorgungsgrad ab. Basisstationen werden durch Drahtlosdiensteanbieter von personenbezogenen Kommunikationsdiensten PCS (für engl. personal communication services) normalerweise in Zellenstandorten installiert. Basisstationen multiplexen den Endsystemverkehr von ihrem Versorgungsbereich über ein Drahtleitungs- oder Mikrowellen-Backhaul-Netz **38** zur Mobilvermittlungseinrichtung (MSC) **40** des Systems.

[0059] Die Erfindung ist von der MAC- und der (physikalischen) PHY-Schicht der Luftverbindung, sowie der Art des Modems unabhängig. Die Architektur ist auch von der physikalischen Schicht und der Topologie des Backhaul-Netzes **38** unabhängig. Die einzigen Anforderungen für das Backhaul-Netz sind, dass es zum Leiten von Internetprotokoll- oder IP-Paketen zwischen Basisstationen und der MSC mit einer angemessenen Leistung imstande sein muss. An der Mobilvermittlungseinrichtung **40** (MSC **40**) beendet eine Paketdaten-IWF

oder -Netzübergangsfunktion (IWF für engl. inter-working function) **52** die drahtlosen Protokolle für dieses Netz. Ein IP-Router **42** verbindet die MSC **40** mit dem öffentlichen Internet **44**, privaten Intranets **46** oder den Internetdiensteanbietern **46**. Abrechnungs- und Verzeichnisserver **48** in der MSC **40** speichern Abrechnungsdaten und Verzeichnisinformationen. Ein Elementverwaltungsserver **50** verwaltet die Betriebsmittel, welche die Basisstationen, die IWFs und die Abrechnungs/Verzeichnisserver umfassen.

[0060] Der Abrechnungsserver sammelt Abrechnungsdaten für Benutzer und sendet die Daten an das Gebührenverrechnungssystem des Diensteanbieters. Die Schnittstelle, die durch den Abrechnungsserver unterstützt wird, sendet Abrechnungsinformationen im Rechnungsprotokollformat des Amerikanischen Verbunds für Betriebsführung AMA (American Management Association) oder irgendeinem anderen geeigneten Rechnungsformat über eine Transportsteuerungsprotokoll/Internetprotokoll- oder TCP/IP-Übertragung (für engl. transport control protocol/internet protocol) an das Gebührenverrechnungssystem (das in der Figur nicht dargestellt ist).

[0061] Die Netzinfrastruktur versorgt Endsysteme mit einem PPP- oder Punkt-zu-Punkt-Dienst. Das Netz stellt (1) einen festen drahtlosen Zugang mit Roaming (Einloggen überall da, wo die drahtlose Versorgung verfügbar ist) für Endsysteme und (2) niedrigratige Mobilität und Weiterschaltungen bereit. Wenn ein Endsystem sich bei einem Netz anmeldet, kann es entweder einen festen Dienst (d.h. stationär und ohne Notwendigkeit von Weiterschaltdiensten) oder einen mobilen Dienst (d.h. mit der Notwendigkeit von Weiterschaltdiensten) anfordern. Ein Endsystem, das weder fest noch mobil spezifiziert, wird als den mobilen Dienst spezifizierend angesehen. Die tatsächliche Registrierung des Endsystems ist das Ergebnis einer Verhandlung mit einem Heimatregistrierungsserver auf der Basis der angeforderten Dienstklasse, der Dienstklasse, die vom Benutzer des Endsystems abonniert wurde, und der Dienstmerkmale, die im Netz verfügbar sind.

[0062] Wenn das Endsystem eine Festdienstregistrierung (d.h. ohne Weiterschaltdienste anzufordern) aushandelt und das Endsystem sich im Heimatnetz befindet, wird eine IWF (Netzübergangsfunktion) in der Basisstation implementiert, um den Verkehr zwischen dem Endbenutzer und einem Kommunikationsserver, wie beispielsweise einem PPP-Server (d.h. mit dem zu verbindenden Punkt, zum Beispiel einem ISP-PPP-Server oder einem PPP-Server des firmeneigenen Intranets oder einem PPP-Server, der durch den Drahtlosdiensteanbieter betrieben wird, um Kunden direkten Zugang zum öffentlichen Internet zu verschaffen), zu vermitteln. Es ist zu erwarten, dass vielleicht 80 % des Nachrichtenverkehrs von dieser Kategorie sein werden, weshalb diese Architektur die IWF-Verarbeitung an die Basisstationen verteilt und eine Nachrichtenverkehrsbehinderung in einer zentralen Mobilvermittlungseinrichtung vermeidet.

[0063] Wenn das Endsystem einen mobilen Dienst anfordert (von einem Heimatnetz oder einem Fremdnetz) oder wenn das Endsystem einen Roaming-Dienst (d.h. einen Dienst vom Heimatnetz durch ein Fremdnetz) anfordert, werden zwei IWFs eingerichtet: eine versorgende IWF, die normalerweise in der Basisstation des Netzes eingerichtet wird, an welches das Endsystem angeschlossen ist (sei es das Heimatnetz oder ein Fremdnetz), und eine Heimat-IWF, die normalerweise in der Mobilvermittlungseinrichtung MSC des Heimatnetzes eingerichtet wird. Da zu erwarten ist, dass diese Situation nur etwa 20 % des Nachrichtenverkehrs einbezieht, wird die Nachrichtenverkehrsbehinderung um die Mobilvermittlungseinrichtung minimiert. Die versorgende IWF und der drahtlose Hub können ortsgleich im selben Computersatz untergebracht sein oder sie können sogar im selben Computer programmiert sein, so dass kein Tunnel unter Verwendung eines XTunnel-Protokolls zwischen dem drahtlosen Hub und der versorgenden IWF hergestellt zu werden braucht.

[0064] Basierend auf den verfügbaren Dienstmerkmalen und der angeforderten Dienstart und Dienstgüte kann eine versorgende IWF in einem Fremdnetz alternativerweise aus Dienstmerkmalen in der fremden MSC gewählt werden. Im Allgemeinen wird die Heimat-IWF zu einem Ankerpunkt, der während der Kommunikationssitzung nicht gewechselt wird, während die versorgende IWF wechseln kann, wenn das Endsystem sich ausreichend bewegt.

[0065] Die Basisstation weist einen Zugangshub und wenigstens einen Zugangspunkt (sei er abgesetzt oder mit dem Zugangshub ortsgleich untergebracht) auf. Normalerweise versorgt der Zugangshub mehrere Zugangspunkte. Obwohl das Endsystem gemäß den Lehren dieser Erfindung an einen Zugangspunkt durch einen Draht oder ein Kabel angeschlossen werden kann, ist das Endsystem in einer bevorzugten Ausführungsform durch eine drahtlose „Luftverbindung" an den Zugangspunkt angeschlossen, in welchem Fall der Zugangshub zweckmäßig als drahtloser Hub bezeichnet wird. Es versteht sich von selbst, dass, obwohl der Zugangshub die ganze Beschreibung hindurch als „drahtloser Hub" bezeichnet wird, ein Endsystem, das durch einen Draht oder ein Kabel durch einen Zugangspunkt mit einem Zugangshub gekoppelt ist, eine gleichwertige Implementierung ist und durch den Begriff „Zugangshub" berücksichtigt ist.

[0066] In der Erfindung weist ein Endsystem einen Endbenutzerregistrierungsagenten (z.B. eine Software, die auf einem Computer des Endsystems, seines Modems oder beiden läuft) auf, der mit einem Zugangspunkt und durch den Zugangspunkt mit einem drahtlosen Hub kommuniziert. Der drahtlose Hub weist einen Proxy-Registrierungsagenten (z.B. eine Software, die auf einem Prozessor im drahtlosen Hub läuft) auf, der als ein Proxy für den Endbenutzerregistrierungsagenten fungiert. Ähnliche Konzepte, die zum Beispiel in dem von der IETF vorgeschlagenen Mobile-IP-Standard verwendet werden, werden allgemein als fremder Agent (FA) bezeichnet. Aus diesem Grund wird der Proxy-Registrierungsagent der vorliegenden Erfindung als fremder Agent bezeichnet, und Aspekte des fremden Agenten der vorliegenden Erfindung, die sich vom fremden Agenten des Mobile IPs unterscheiden, sind so, wie sie während dieser Beschreibung dargelegt werden.

[0067] Bei Verwenden des Proxy-Registrierungsagenten (d.h. des fremden Agenten) in einer Basisstation ist der Benutzerregistrierungsagent eines Endsystems imstande, einen Anschlusspunkt ans Netz zu ermitteln und sich bei einem Registrierungsserver in der MSC (Mobilvermittlungseinrichtung) des Heimatnetzes registrieren zu lassen. Der Heimatregistrierungsserver stellt die Verfügbarkeit jedes der mehreren Netzübergangsfunktionsmodule (IWFs) im Netz (eigentlich Softwaremodule, die auf Prozessoren sowohl in der MSC als auch dem drahtlosen Hub laufen) fest und ordnet dem registrierten Endsystem IWF(s) zu. Für jedes registrierte Endsystem wird ein Tunnel (unter Verwendung des XTunnel-Protokolls) zwischen dem drahtlosen Hub in der Basisstation und einer Netzübergangsfunktion (IWF) in der Mobilvermittlungseinrichtung (MSC) erzeugt, wobei dieser Tunnel PPP-Rahmen zwischen dem Endsystem und der IWF transportiert.

[0068] Wie hierin verwendet, ist das XTunnel-Protokoll ein Protokoll, das einen In-Folge-Transport von PPP-Datenrahmen mit Flusssteuerung bereitstellt. Dieses Protokoll kann über standardmäßige IP-Netze oder über Punkt-zu-Punkt-Netze oder über vermittelte Netze wie ATM-Datennetze oder Rahmenweiterleitungsdatennetze laufen. Solche Netze können auf T1- oder T3-Verbindungen basieren, oder sie können auf Funkverbindungen, seien sie land- oder weltraumgestützt, basieren. Das XTunnel-Protokoll kann durch Anpassen von Algorithmen vom Schicht-2-Tunnelprotokoll L2TP (für engl. layer 2 tunneling protocol) gebildet werden. In Netzen, die auf Verbindungen basieren, in welchen verlorene Datenpakete gefunden werden können, kann ein Wiederholungssendungsmerkmal eine wünschenswerte Option sein.

[0069] Der PPP-Partner (d.h. ein Kommunikationsserver) des Endsystems kann in der IWF oder einem firmeneigenen Intranet oder einem ISP-Netz sitzen. Wenn der PPP-Partner in der IWF sitzt, wird ein Endsystem mit einem direkten Internetzugang versehen. Wenn der PPP-Partner in einem Intranet oder ISP sitzt, wird ein Endsystem mit einem Intranetzugang oder einem Zugang zu einem ISP versehen. Um einen Intranet- oder ISP-Zugang zu unterstützen, verwendet die IWF das Schicht-zwei-Tunnelprotokoll (L2TP) zur Verbindung mit dem Intranet- oder ISP-PPP-Server. Vom Gesichtspunkt des Intranet- oder ISP-PPP-Servers sieht die IWF wie ein Netzugangsserver (NAS für engl. network access server) aus. Der PPP-Verkehr zwischen dem Endsystem und der IWF wird durch den fremden Agenten in der Basisstation weitergeleitet.

[0070] In der Rückwärtsrichtung (Aufwärtsstrecke) werden PPP-Rahmen, die sich vom Endsystem zur IWF fortpflanzen, über die MAC- und Luftverbindung zur Basisstation gesendet. Die Basisstation leitet diese Rahmen unter Verwendung des XTunnel-Protokolls zur IWF in der MSC weiter. Die IWF stellt sie einem PPP-Server zur Verarbeitung zu. Für den Internetzugang kann der PPP-Server in derselben Maschine wie die IWF sein. Für einen ISP- oder Intranetzugang ist der PPP-Server in einem privaten Netz, und die IWF verwendet das Schicht-zwei-Tunnelprotokoll (L2TP) zur Verbindung damit.

[0071] In der Vorwärtsrichtung (Abwärtsstrecke) werden PPP-Rahmen vom PPP-Server durch die IWF unter Verwendung des XTunnel-Protokolls zur Basisstation weitergeleitet. Die Basisstation enttunnelt Abwärtsstreckenrahmen und leitet sie über die Luftverbindung zum Endsystem weiter, wo sie durch die PPP-Schicht des Endsystems verarbeitet werden.

[0072] Die Unterstützung der Mobilität umfasst die Unterstützung von Weiterschaltungen. Die MAC-Schicht hilft der Mobilitätsverwaltungssoftware in der Basisstation und dem Endsystem bei der wirksamen Durchführung von Weiterschaltungen. Weiterschaltungen werden von den PPP-Partnerinstanzen und dem L2TP-Tunnel transparent abgewickelt. wenn ein Endsystem sich von einer Basisstation zu einer anderen bewegt, wird ein neuer XTunnel zwischen der neuen Basisstation und der ursprünglichen IWF erzeugt. Der alte XTunnel von der alten Basisstation wird gelöscht. PPP-Rahmen durchlaufen den neuen Weg transparent.

[0073] Das Netz unterstützt Roaming (d.h., wenn der Endbenutzer sich durch einen fremden Drahtlosdiensteanbieter mit seinem Heimat-Drahtlosdiensteanbieter in Verbindung setzt). Durch Verwenden dieses Merkmals sind Endsysteme imstande, vom Heimatnetz in ein Fremdnetz zu wandern und dennoch versorgt zu wer-

den, vorausgesetzt natürlich, dass der fremde Drahtlosdiensteanbieter und der Heimat-Drahtlosdiensteanbieter des Endsystems eine Dienstvereinbarung haben.

[0074] In Fig. 6 hat sich ein Gast-Endsystem **60** zu einem Aufenthaltsort begeben, an welchem ein fremder Drahtlosdiensteanbieter **62** die Versorgung bereitstellt. Das Gast-Endsystem **60** hat jedoch ein Teilnehmerverhältnis mit dem Heimat-Drahtlosdiensteanbieter **70**. In der vorliegenden Erfindung hat der Heimat-Drahtlosdiensteanbieter **70** ein Vertragsverhältnis mit dem fremden Drahtlosdiensteanbieter **62**, um Zugangsdienste bereitzustellen. Daher setzt sich das Gast-Endsystem **60** über die Luftverbindung mit der Basisstation **64** des fremden Drahtlosdiensteanbieters **62** in Verbindung. Dann werden Daten vom Gast-Endsystem **60** durch die Basisstation **64** durch die versorgende IWF **66** des fremden Drahtlosdiensteanbieters **62** zur Heimat-IWF **72** des Heimat-Drahtlosdiensteanbieters **70** oder möglicherweise durch die Heimat-IWF **72** des Heimat-Drahtlosdiensteanbieters **70** zum Internetdiensteanbieter **74** weitergeleitet.

[0075] Eine diensteüberschreitende Anbieterschnittstelle, genannt I-Schnittstelle, wird für Kommunikationen über Drahtlosdiensteanbieter- oder WSP-Grenzen (WSP für engl. wireless service provider) zur Unterstützung von Roaming verwendet. Diese Schnittstelle wird zum Authentifizieren, Registrieren und Transportieren der PPP-Rahmen des Endsystems zwischen dem fremden WSP und dem Heimat-WSP verwendet.

[0076] PPP-Rahmen in der Aufwärtsstrecken- und in der Abwärtsstreckenrichtung pflanzen sich durch den Heimat-Drahtlosdiensteanbieter (WSP) des Endsystems fort. Alternativerweise laufen PPP-Rahmen vom fremden WSP direkt zum Bestimmungsnetz durch. Die Basisstation im fremden WSP ist der Anschlusspunkt des Endsystems im Fremdnetz. Diese Basisstation sendet (und empfängt) PPP-Rahmen zu (und von) einer versorgenden IWF in der Mobilvermittlungseinrichtung des fremden WSPs. Die versorgende IWF setzt sich unter Verwendung eines Schicht-zwei-Tunnels über die I-Schnittstelle mit der Heimat-IWF in Verbindung, um die PPP-Rahmen des Endsystems in beiden Richtungen zu transportieren. Die versorgende IWF im fremden WSP sammelt Abrechnungsdaten zur Rechnungsprüfung. Die Heimat-IWF im Heimat-WSP sammelt Abrechnungsdaten für die Gebührenverrechnung.

[0077] Die versorgende IWF im fremden WSP kann mit der Basisstation im selben System verknüpft sein, wodurch die Notwendigkeit des X-Tunnels eliminiert wird.

[0078] Während der Registrierungsphase stellt ein Registrierungsserver im fremden WSP die Identität des Heimatnetzes des Gast-Endsystems fest. Unter Verwendung dieser Informationen kommuniziert der fremde Registrierungsserver mit dem Heimatregistrierungsserver, um das Endsystem zu authentifizieren und zu registrieren. Diese Registrierungsnachrichten fließen über die I-Schnittstelle. Sobald das Endsystem authentifiziert und registriert wurde, wird unter Verwendung des XTUNNEL-Protokolls ein Schicht-zwei-Tunnel zwischen der Basisstation und der versorgenden IWF erzeugt, und ein anderer Schicht-zwei-Tunnel wird zwischen der versorgenden IWF und der Heimat-IWF über den I-XTunnel erzeugt. Die Heimat-IWF setzt sich wie zuvor unter Verwendung des L2TPs (Schicht-2-Tunnelprotokolls) mit dem PPP-Partner in Verbindung. während der Weiterschaltungen bleibt der Aufenthaltsort der Heimat-IWF und des L2TP-Tunnels fest. Wenn das Endsystem sich von einer Basisstation zu einer anderen Basisstation bewegt, wird ein neuer Tunnel zwischen der neuen Basisstation und der versorgenden IWF erzeugt, und der alte Tunnel zwischen der alten Basisstation und der versorgenden IWF wird gelöscht. Wenn das Endsystem sich weit genug bewegt, so dass eine neue versorgende IWF benötigt wird, wird ein neuer I-XTunnel zwischen der versorgenden IWF und der Heimat-IWF erzeugt. Der alte Tunnel zwischen der alten versorgenden IWF und der Heimat-IWF wird gelöscht.

[0079] Zur Unterstützung des Roaming unterstützt die I-Schnittstelle die Authentifizierung, Registrierung und Datentransportdienste über Drahtlosdiensteanbietergrenzen. Authentifizierungs- und Registrierungsdienste werden unter Verwendung des IETF Radius-Protokolls unterstützt. Datentransportdienste zum Übertragen von PPP-Rahmen über einen Schicht-zwei-Tunnel werden unter Verwendung des I-XTunnel-Protokolls unterstützt. Dieses Protokoll basiert auf dem IETF L2TP-Protokoll.

[0080] Wie in dieser Beschreibung verwendet, bezieht sich der Begriff Heimat-IWF auf die IWF im Heimatnetz des Endsystems. Der Begriff versorgende IWF bezieht sich auf die IWF im Fremdnetz, welches das Endsystem vorübergehend versorgt. Ähnlich bezieht sich der Begriff Heimatregistrierungsserver auf den Registrierungsserver im Heimatnetz des Endsystems, und der Begriff fremder Registrierungsserver bezieht sich auf den Registrierungsserver im Fremdnetz, durch welchen sich das Endsystem registrieren lässt, während es wandert.

[0081] Das Netz unterstützt sowohl eine feste als auch eine dynamische IP-Adresszuordnung für Endsysteme. Es gibt zwei Arten von IP-Adressen, die in Betracht zu ziehen sind. Die erste ist die Identität des Endsys-

tems in seinem Heimatnetz. Diese kann ein strukturierter Benutzername im Format user@domain sein. Diese unterscheidet sich von der Heimat-IP-Adresse, die im Mobile IP verwendet wird. Die zweite Adresse ist die IP-Adresse, die dem Endsystem über das PPP-IPC-Adressprotokoll zugeordnet wird. Das Domänenteilfeld der Heimatadresse wird verwendet, um die Heimatdomäne des Benutzers zu identifizieren, und ist ein voll qualifizierter Domänenname. Das Benutzerteilfeld der Heimatadresse wird verwendet, um den Benutzer in der Heimatdomäne zu identifizieren. Der User-Name wird auf dem Endsystem und in der Teilnehmerdatenbank an der MSC gespeichert, und er wird dem Benutzer zugeordnet, wenn er den Dienst abonniert. Das Domänenteilfeld des User-Name wird während des Roamings verwendet, um Roaming-Verhältnisse und den Heimatregistrierungsserver zum Zwecke der Registrierung und Authentifizierung zu identifizieren. Anstelle des strukturierten Benutzernamens kann eine andere eindeutige Kennung verwendet werden, um das Heimatnetz des Benutzers und der Identität des Benutzers im Heimatnetz zu identifizieren. Diese Kennung wird in der Registrierungsaufforderung durch das Endsystem gesendet.

[0082] Das PPP-IPCP wird verwendet, um die IP-Adresse für das Endsystem auszuhandeln. Durch Verwenden des IP-Konfigurationsprotokolls IPCP ist das Endsystem imstande, eine feste oder dynamische IP-Adresse auszuhandeln.

[0083] Obwohl die Verwendung des strukturierten Benutzernamensfeldes und die Nichtverwendung einer IP-Heimatadresse ein Merkmal ist, welches die vorliegende Erfindung gegenüber einem bekannten Mobile IP kennzeichnet, kann das Netz verbessert werden, um auch Endsysteme zu unterstützen, die keinen Benutzernamen und nur eine Nicht-Null-Heimat-IP-Adresse haben, wenn das Mobile IP und seine Verwendung in Verbindung mit PPP-Endsystemen gängig wird. Der PPP-Server kann durch den Diensteanbieter so konfiguriert werden, dass er während der IPCP-Adresszuordnungsphase IP-Adressen zuordnet, welche gleich sind wie die Heimat-IP-Adresse des Endsystems. In diesem Fall sind die Heimatadresse und die durch das IPCP zugeordnete IP-Adresse identisch.

[0084] In Fig. 7 bilden die Basisstation **64** und Luftverbindungen von Endsystemen ein drahtloses Teilnetz **80**, das die Luftverbindungen für den Endbenutzerzugang, wenigstens eine Basisstation (z.B. Station **64**) und wenigstens ein Backhaul-Netz (z.B. **38** von Fig. 2) von der Basisstation zur MSC **40** (Fig. 2) aufweist. Die Architektur des drahtlosen Teilnetzes von zum Beispiel einer Basisstation mit drei Sektoren weist die folgenden logischen Funktionen auf:

1. Zugangspunktfunktion. Zugangspunkte **82** führen MAC-Schicht-Überbrückungs- und MAC-Schicht-Assoziations- und -Dissoziationsprozeduren durch. Ein Zugangspunkt weist einen Prozessor (vorzugsweise in Form einer kundenanwendungsspezifischen integrierten Schaltung ASIC), eine Verbindung zu einem drahtlosen Hub (vorzugsweise in Form einer Ethernet-Verbindung auf einer Karte oder in die ASIC eingebaut), eine Verbindung zu einer Antenne (vorzugsweise in Form einer Karte mit einem Datenmodulator/demodulator und einem Sender/Empfänger) und die Antenne, an welche das Endsystem gekoppelt ist. Der Prozessor führt eine Software aus, um eine Datenüberbrückungsfunktion und verschiedene andere Funktionen zur Unterstützung von Registrierung und Mobilitätsweiterschaltungen, wie hierin näher beschrieben wird, auszuführen. Siehe Erörterung in Bezug auf Fig. 10, Fig. 11 und Fig. 14.
   Zugangspunkte (APs für engl. access points) nehmen MAC-Schicht-Rahmen von der Luftverbindung und leiten sie an einen drahtlosen Hub weiter und umgekehrt. Die MAC-Schicht-Assoziations- und – Dissoziationsprozeduren werden durch die APs verwendet, um eine Liste von Endsystem-MAC-Adressen in ihrer MAC-Adressen-Filtertabelle zu führen. Ein AP kann eine MAC-Schicht-Überbrückung nur für Endsysteme durchführen, deren MAC-Adressen in der Tabelle vorhanden sind. Ein Zugangspunkt und sein zugehöriger drahtloser Hub sind normalerweise ortsgleich untergebracht. In seiner einfachsten Form ist nur Zugangspunkt ein Port in einen drahtlosen Hub. Wenn die APs und der drahtlose Hub ortsgleich im selben Zellenstandort untergebracht sind, können sie über eine IEEE 802.3 Verbindung miteinander verbunden werden. Manchmal sind Zugangspunkte abgesetzt vom drahtlosen Hub angeordnet und über eine Weitverkehrsverbindung, wie einen drahtgebundenen T1-Trunk oder auch einen drahtlosen Trunk, angeschlossen. Für Zellen mit mehreren Sektoren werden mehrere Zugangspunkte (d.h. einer pro Sektor) verwendet.
2. Drahtloshubfunktion. Der drahtlose Hub **84** führt Fremdagent- oder FA-Prozeduren, Backhaul-Lastausgleich (z.B. über mehrere T1), Backhaul-Netzanbindungen und die XTunnel-Prozeduren durch. Wenn eine Unterstützung für Dienstgüte (QOS) vorhanden ist, implementiert der drahtlose Hub die Unterstützung für QOS durch Ausführen des XTunnel-Protokolls über Backhauls mit verschiedenen QOS-Attributen. In einem Zellenstandort mit mehreren Sektoren wird eine einzige Drahtloshubfunktion normalerweise durch mehrere Zugangspunkte gemeinsam benutzt.
   Ein drahtloser Hub weist einen Prozessor, eine Verbindung zu einem oder mehr Zugangspunkten (vorzugsweise in Form einer Ethernet-Verbindung auf einer Karte oder in eine ASIC eingebaut) und eine Verbindung zu einer Backhaul-Leitung auf. Die Backhaul-Leitung ist normalerweise eine T1- oder T3-Kommunikations-

leitung, die in der Mobilvermittlungseinrichtung des Drahtlosdiensteanbieters endet. Die Verbindung zur Backhaul-Leitung formatiert Daten in ein bevorzugtes Format, zum Beispiel ein Ethernet-Format, ein Rahmenweiterleitungsformat oder ein ATM-Format. Der Prozessor des drahtlosen Hubs führt eine Software aus, um eine Datenüberbrückung und verschiedene andere Funktionen, wie hierin beschrieben, zu unterstützen. Siehe Erörterung in Bezug auf Fig. 12. Fig. 13 und Fig. 14.

[0085] Die Basisstationskonstruktion unterstützt die folgenden Arten von Zellarchitekturen:

1. Architektur mit lokalen APs. In einer Architektur mit lokalen APs haben Zugangspunkte eine große (normalerweise >= 2 km) Reichweite. Sie sind im Zellenstandort ortsgleich mit dem drahtlosen Hub untergebracht (Fig. 4). Zugangspunkte können unter Verwendung eines IEEE 802.3 Netzes mit dem drahtlosen Hub verbunden sein, oder sie können direkt in der Rückwandplatine des drahtlosen Hubs angesteckt sein oder unter Verwendung irgendeines anderen Mechanismus (z.B. universeller serieller Bus, Druckeranschluss, Infrarot usw.) mit dem drahtlosen Hub verbunden sein. Es wird vorausgesetzt, dass die erste Alternative für den Rest dieser Erörterung verwendet wird. Der Zellenstandort kann rundstrahlend oder durch Hinzufügen von mehreren Zugangspunkten und sektorierten Antennen zu einem drahtlosen Hub sektoriert sein.
2. Architektur mit abgesetzten APs. In einer Architektur mit abgesetzten APs weisen Zugangspunkte normalerweise eine sehr kleine Reichweite, normalerweise ungefähr 1 km Radius, auf. Sie sind vom drahtlosen Hub (entweder außen oder innen) abgesetzt angeordnet. Ein T1- oder ein drahtloser Trunk verbindet vorzugsweise Zugangspunkte mit dem Zellenstandort, wo der drahtlose Hub angeordnet ist. Vom Zellenstandort wird normalerweise ein Drahtleitungs-Backhaul oder eine Mikrowellenstrecke zur Verbindung mit der IWF in der MSC verwendet. Wenn ein drahtloses Trunking zwischen dem abgesetzten AP und dem drahtlosen Hub verwendet wird, werden rundstrahlende oder sektorierte Funkgeräte für das Trunking verwendet. Die Geräte für das Trunking zu abgesetzten Zugangspunkten sind vorzugsweise ortsgleich mit dem drahtlosen Hub untergebracht und können unter Verwendung eines IEEE 802.3 Netzes damit verbunden sein, oder sie können direkt in der Rückwandplatine des drahtlosen Hubs angesteckt sein. Diese Geräte werden mit dem Begriff Trunk-AP bezeichnet.
3. Architektur mit gemischten APs. In einer Mischarchitektur muss das drahtlose Teilnetz abgesetzte und lokale Zugangspunkte unterstützen. Abgesetzte Zugangspunkte können zur Lochfüllung und aus anderen Kapazitätsgründen hinzugefügt werden. Wie bereits erwähnt, können T1- oder drahtlose Trunks verwendet werden, um den abgesetzten AP mit dem drahtlosen Hub zu verbinden.

[0086] Fig. 37 und Fig. 38 sind Systemkonfigurationsdiagramme, welche mögliche Verbindungen veranschaulichen. Für Fall (i) ist die IWF1 die Anker-IWF und dient als der Heimatagent, während der WH1 als der fremde Agent dient. Ein XTunnel wird zwischen dem WH1 und der IWF1 verwendet, und der Schicht-2-Tunnelprotokoll- oder L2TP-Tunnel wird zwischen der IWF1 und dem PPP-Server verwendet. Für Fall (ii) sind der WH und die versorgende IWF ortsgleich untergebracht. Die IWF1 ist die Anker-IWF und die versorgende IWF IWF2 dient als der fremde Agent. Ein I-XTunnel wird zwischen IWF und IWF2 verwendet, und ein L2TP-Tunnel wird zwischen IWF1 und dem PPP-Server verwendet. Für Fall (iii) ist die versorgende IWF IWF3, und die Anker-IWF ist IWF1. Ein XTunnel wird zwischen WH3 und IWF3 verwendet, ein I-XTunnel wird zwischen IWF3 und IWF1 verwendet, und ein L2TP-Tunnel wird zwischen IWF1 und dem PPP-Server verwendet.

[0087] Fig. 38 veranschaulicht die Hinzufügung eines drahtlosen Abschnitts (Trunk-AP), wobei der Trunk-AP mit dem WH ortsgleich untergebracht sein kann. Für diesen Fall können neben den zuvor beschriebenen drei Möglichkeiten auch die folgenden Möglichkeiten vorkommen. Für Fall (i) ist der Trunk-AP1 der fremde Agent, und IWF1 ist die Anker-IWF. Ein XTunnel wird zwischen dem Trunk-AP1 und der Anker-IWF verwendet, und ein L2TP-Tunnel wird zwischen der Anker-IWF und dem PPP-Server verwendet. Für Fall (ii) ist die versorgende IWF2 der fremde Agent. Ein XTunnel wird zwischen dem Trunk-AP2 und der IWF2 verwendet, ein I-XTunnel wird zwischen der IWF2 und der Anker-IWF1 verwendet, und ein L2TP-Tunnel wird zwischen der Anker-IWF und dem PPP-Server verwendet. Für Fall (iii) ist die versorgende IWF der fremde Agent. Ein XTunnel wird zwischen dem Trunk-AP3 und der IWF3 verwendet, ein I-XTunnel wird zwischen IWF3 und der Anker-IWF1 verwendet, und ein L2TP-Tunnel wird zwischen der Anker-IWF1 und dem PPP-Server verwendet.

[0088] Fig. 39 bis Fig. 42 veranschaulichen mehrere Weiterschaltungsszenarien, sowie verschiedene Verbindungen zwischen den Elementen des Systems.

[0089] Fig. 8 stellt eine Zelle mit drei Sektoren dar, die nur lokale APs verwenden. Die Zugangspunkte und der drahtlose Hub sind ortsgleich in der Basisstation untergebracht und mit 802.3 Verbindungen miteinander verbunden.

[0090] Fig. 9 stellt die Architektur mit abgesetzten Zugangspunkten **82** dar, die unter Verwendung von drahtlosen Trunks **86** mit dem drahtlosen Hub **84** verbunden sind. Jeder Trunk-Zugangspunkt in der Basisstation stellt eine drahtlose Punkt-zu-Mehrpunkt-Funkverbindung zu abgesetzten Mikro-Zugangspunkten (R-AP in der Figur) bereit. Die abgesetzten Zugangspunkte stellen einen Luftverbindungsdienst zu Endsystemen bereit. Der drahtlose Hub und die Trunk-Zugangspunkte sind ortsgleich in der Bassstation untergebracht und über 802.3 Verbindungen miteinander verbunden. Diese Figur stellt auch abgesetzte Zugangspunkte **82R** dar, die über Punkt-zu-Punkt-T1-Verbindungen mit dem drahtlosen Hub verbunden sind. In diesem Szenarium sind keine Trunk-APs erforderlich.

[0091] Zur Unterstützung aller zuvor beschriebenen Zellarchitekturen und der verschiedenen Arten von Zugangspunkten, die jede Zelle verwenden könnte, befolgt die Netzarchitektur folgende Regeln:

1. Zugangspunkte fungieren als MAC-Schicht-Brücken. Abgesetzte Zugangspunkte führen eine MAC-Überbrückung zwischen der Luftverbindung zu den Endsystemen und dem drahtlosen oder T1-Trunk zum Zellenstandort durch. Lokale Zugangspunkte führen eine MAC-Überbrückung zwischen der Luftverbindung zu den Endsystemen und dem drahtlosen Hub durch.
2. Trunk-Zugangspunkte fungieren ebenfalls als MAC-Schicht-Brücken. Sie führen eine MAC-Überbrückung zwischen dem Trunk (welcher zu den Zugangspunkten geht) und dem drahtlosen Hub durch.
3. Der drahtlose Hub wird mit allen ortsgleich untergebrachten MAC-Brücken (d.h. lokalen Zugangspunkten oder Trunk-Zugangspunkten) verbunden, wobei anfänglich eine 802.3 Verbindung verwendet wird.

[0092] Wenn lokale Zugangspunkte oder abgesetzte Zugangspunkte mit T1-Trunks verwendet werden, werden außerdem die folgenden Regeln befolgt:

1. Lokale Zugangspunkte werden mit dem drahtlosen Hub ortsgleich untergebracht und unter Verwendung von 802.3 Punkt-zu-Punkt-Verbindungen oder einem gemeinsam benutzten 802.3 Netz damit verbunden. Abgesetzte Zugangspunkte werden unter Verwendung von Punkt-zu-Punkt-T1-Trunks mit dem drahtlosen Hub verbunden.
2. Die Sektorisierung wird durch Hinzufügen von Zugangspunkten mit sektorierten Antennen zum Zellenstandort unterstützt.
3. Für jeden Zugangspunkt, der mit dem drahtlosen Hub verbunden ist, gibt es einen fremden Agenten, der im drahtlosen Hub läuft, der an der Endsystemregistrierung teilnimmt. MAC-Schicht-Assoziationsprozeduren werden verwendet, um die MAC-Adressen-Filtertabellen der Zugangspunkte auf dem Laufenden zu halten und die MAC-Schicht-Überbrückung wirksam durchzuführen. Der drahtlose Hub nimmt an den MAC-Assoziationsfunktionen teil, so dass nur gültige MAC-Adressen den MAC-Adressen-Filtertabellen der Zugangspunkte hinzugefügt werden.
4. Der drahtlose Hub leitet Rahmen von den Zugangspunkten unter Verwendung des XTunnel-Protokolls zur MSC-IWF und umgekehrt, sofern die IWF nicht mit dem drahtlosen Hub ortsgleich untergebracht ist. Die MAC-Adressen-Filtertabelle wird verwendet, um jene Punkt-Punkt-MAC-Kommunikationsdatenrahmen auszufiltern, deren MAC-Adressen in der Tabelle nicht vorhanden sind. Die APs senden MAC-Rundsenderahmen und MAC-Rahmen, die mit der Endsystemregistrierungsfunktion verbunden sind, stets ungeachtet der Inhalte der MAC-Adressen-Filtertabelle weiter.
5. Lokale Zugangspunkte verwenden das ARP zur Auflösung von MAC-Adressen, um den IP-Verkehr zum drahtlosen Hub zu leiten. Umgekehrt verwendet auch der drahtlose Hub das ARP, um IP-Pakete zu Zugangspunkten zu leiten. Das UDP/IP wird zur Netzverwaltung von Zugangspunkten verwendet.
6. Abgesetzte Zugangspunkte, die über T1 angeschlossen sind, verwenden kein ARP, da die Verbindung eine Punkt-zu-Punkt-Verbindung ist.
7. Die Unterstützung für Weiterschaltungen erfolgt mit Hilfe von der MAC-Schicht.

[0093] In einer Zellarchitektur, die drahtlose Trunks und Trunk-APs verwendet, werden die folgenden Regeln befolgt

1. Trunk-Zugangspunkte werden ortsgleich mit dem drahtlosen Hub untergebracht und unter Verwendung von 802.3 Punkt-zu-Punkt-Verbindungen oder anderen geeigneten Mitteln damit verbunden.
2. Die Sektorisierung drahtloser Trunks wird durch Hinzufügen von Trunk-Zugangspunkten mit sektorierten Antennen zum Zellenstandort unterstützt.
3. Weiterschaltungen über Backhaul-Sektoren erfolgen unter Verwendung des fremden Agenten im drahtlosen Hub. Für jeden Backhaul-Sektor gibt es einen fremden Agenten, der im drahtlosen Hub läuft.
4. Die Trunk-APs brauchen nicht an den MAC-Schicht-Endsystem-Assoziations- und -Weiterschaltungsprozeduren teilzunehmen. Ihre MAC-Adressen-Filtertabellen werden durch den drahtlosen Hub dynamisch programmiert, wenn Endsysteme sich beim Netz registrieren lassen. Die MAC-Adressen-Filtertabelle wird verwendet, um Punkt-Punkt-MAC-Kommunikationsrahmen auszufiltern. MAC-Rundesenderahmen oder MAC-Rahmen, die Registrierungspakete enthalten, werden stets durchgelassen.

5. Trunk-APs verwenden das ARP zur Auflösung von MAC-Adressen, um den IP-Verkehr zum drahtlosen Hub zu leiten. Umgekehrt verwendet der drahtlose Hub das ARP, um IP-Pakete zu Trunk-APs zu leiten. Das UDP/IP wird zur Netzverwaltung von Trunk-APs verwendet.
6. In einem einzelnen drahtlosen Trunk-Sektor erfolgen MAC-Assoziation und -Weiterschaltungen von einem Zugangspunkt zu einem anderen unter Verwendung der MAC-Schicht mit Unterstützung des fremden Agenten im drahtlosen Hub. Durch Verwenden dieser MAC-Schicht-Prozeduren assoziieren Endsysteme sich mit Zugangspunkten. Wenn Endsysteme sich von einem Zugangspunkt zu einem anderen Zugangspunkt bewegen, verwenden die Zugangspunkte ein MAC-Weiterschaltungsprotokoll, um ihre MAC-Adressen-Filtertabellen zu aktualisieren. Der drahtlose Hub am Zellenstandort unterstützt die Zugangspunkte bei der Durchführung dieser Funktion. Diese Unterstützung umfasst das Weiterleiten von MAC-Schicht-Weiterschaltungsnachrichten (da Zugangspunkte nicht imstande sind, direkt über die MAC-Schicht miteinander zu kommunizieren) und Authentifizieren des Endsystems zur MAC-Schicht-Registrierung und -Weiterschaltung und zur Aktualisierung der MAC-Adressen-Filtertabellen der Zugangspunkte.
7. Der fremde Agent für einen drahtlosen Trunk-Sektor ist für die Weiterleitung von Rahmen von seinem Trunk-AP zur MSC und umgekehrt unter Verwendung des XTunnel-Protokolls verantwortlich. Demnach interessiert sich der fremde Agent für einen Trunk-AP nicht für den Aufenthaltsort des Endsystems in Bezug auf Zugangspunkte innerhalb dieses drahtlosen Trunk-Sektors. In der Abwärtsstreckenrichtung übermittelt er nur Rahmen vom Mobile-IP-Tunnel an den entsprechenden Trunk-AP, welcher eine MAC-Schicht-Überbrückung verwendet, um die Rahmen an alle abgesetzten Zugangspunkte zu senden, die an diesen Backhaul-Sektor angeschlossen sind. Die Zugangspunkte konsultieren ihre MAC-Adressen-Filtertabellen und leiten die MAC-Rahmen entweder über das Zugangsnetz weiter oder löschen die MAC-Rahmen. Wie bereits erwähnt, werden die MAC-Adressen-Filtertabellen unter Verwendung der MAC-Schicht-Assoziations- und -Weiterschaltungsprozeduren auf dem Laufenden gehalten. In der Aufwärtsstreckenrichtung werden MAC-Rahmen durch die Zugangspunkte zur Backhaul-Brücke weitergesendet, welche sie unter Verwendung der 802.3 Verbindung an den fremden Agenten im drahtlosen Hub übermittelt.
8. Das ARP wird nicht zum Senden oder Empfangen von IP-Paketen zu den abgesetzten Zugangspunkten verwendet. Die Trunk-Zugangspunkte stellen die MAC-Adresse des drahtlosen Hubs unter Verwendung von BOOTP-Prozeduren fest. Umgekehrt ist der drahtlose Hub mit der MAC-Adresse von abgesetzten Zugangspunkten konfiguriert. Das UDP/IP wird zur Netzverwaltung von Zugangspunkten und für Endsystem-Assoziations- und -Weiterschaltungsnachrichten verwendet.

[0094] IEEE 802.3 Srecken im Zellenstandort können durch schnellere Verbindungen ersetzt werden.

[0095] Fig. 10 stellt den Protokollstapel für einen lokalen Zugangspunkt dar. An der Basis des Stapels ist die physikalische Schicht PHY. Die physikalische Schicht PHY überträgt Daten zu und von einem Endsystem über die Luft unter Verwendung von Funkwellen als ein Beispiel.

[0096] Wenn von einem Endsystem empfangen, empfängt der AP Daten von der physikalischen Schicht und packt sie aus den MAC-Rahmen (der MAC-Schicht) aus. Die Endsystemdatenrahmen werden dann wieder in ein physikalisches Ethernet-Schichtformat (IEEE 802.3 Format) verpackt, wobei sie über die Ethernet-Verbindung zum drahtlosen Hub gesendet werden. Wenn der AP-Prozessor Daten vom drahtlosen Hub über seine Ethernet-Verbindung (d.h. die physikalische Schicht), die Daten, die an ein Endsystem zu übertragen sind, empfängt, verpackt der AP die Daten in ein Medienzugriffssteuerungs- oder MAC-Format und sendet die MAC-Schicht-Daten an seinen Modulator, damit sie unter Verwendung der PHY-Schicht an das Endsystem übertragen werden.

[0097] In Fig. 11 sind die MAC- und die PHY-Schicht zum/vom Endsystem von Fig. 10 durch eine MAC und eine PHY für den Trunk zum Zellenstandort für einen abgesetzten Zugangspunkt ersetzt. Konkret wird für einen T1-Trunk vorzugsweise das höhere Datenübertragungssteuerungs- oder HDLC-Protokoll (für engl. high level data link control protocol) über die T1 verwendet.

[0098] Fig. 12 zeigt den Protokollstapel für den drahtlosen Hub, der die Backhaul-Leitung und den Trunk zum abgesetzten Zugangspunkt zusammenschaltet. Der Trunk zu den abgesetzten Zugangspunkten wird nur zur Unterstützung von abgesetzten Zugangspunkten benötigt (im Unterschied zum Ethernet, das mit Zugangspunkten gekoppelt ist). Die MAC- und die PHY-Schicht für den drahtlosen Trunk zu den abgesetzten APs stellen eine Punkt-zu-Mehrpunkt-Verbindung bereit, so dass ein Trunk verwendet werden kann, um mit vielen abgesetzten APs im selben Sektor zu kommunizieren.

[0099] Der drahtlose Hub schaltet den Trunk zu den abgesetzten APs und die Backhaul-Leitung (z.B. T1 oder T3) zur Mobilvermittlungseinrichtung (MSC) des Netzes zusammen.

[0100] Der Protokollstapel im drahtlosen Hub implementiert MAC- und PHY-Schichten zur MSC, worüber eine IP-Schicht (Internetprotokoll) implementiert ist, worüber eine universelle Datagrammprotokoll- oder UDP-Schicht (für engl. Universelles Datagrammprotokoll) zur Netzverwaltung implementiert ist (die zusammen als UDP/IP bezeichnet werden), worüber ein XTunnel-Protokoll implementiert ist. Das XTunnel-Protokoll ist ein neues Format, das Aspekte von Mobilität (z.B. wie im Mobile IP) und Aspekte des Schicht-2-Tunnelprotokolls (L2TP) umfasst. Das XTunnel-Protokoll wird verwendet, um vom drahtlosen Hub mit der MSC und zwischen Netzübergangsfunktionen (IWFs) in verschiedenen Netzen oder demselben Netz zu kommunizieren.

[0101] In Fig. 13 ist der Protokollstapel für die Relaisfunktion in der Basisstation zur Unterstützung von abgesetzten Zugangspunkten dargestellt. Die Relaisfunktion weist eine Schnittstelle mit der Backhaul-Leitung (dargestellt als der drahtlose Hub) und eine Schnittstelle mit dem abgesetzten AP (dargestellt als ein Trunk-AP) auf. Vom Gesichtspunkt des drahtlosen Hubs verhält sich der Trunk-AP (dargestellt in Fig. 13) eigentlich wie ein AP, der in Fig. 10 dargestellt ist. Vorzugsweise werden die Basisstationsprotokollstapel in einen drahtlosen Hub und einen Trunk-AP mit einem Ethernet dazwischen aufgeteilt. In einem drahtlosen Trunk mit N Sektoren gibt es N drahtlose Trunk-APs im Zellenstandort und einen drahtlosen Hub.

[0102] In Fig. 14 ist der Basisstationsprotokollstapel für eine Zellarchitektur dargestellt, die einen lokalen AP verwendet. Die Relaisfunktion weist eine Schnittstelle mit der Backhaul-Leitung (dargestellt als der drahtlose Hub) und eine Luftverbindungsschnittstelle mit dem Endsystem (dargestellt als ein AP) auf. Vom Gesichtspunkt des drahtlosen Hubs verhält sich der AP (dargestellt in Fig. 11 und Fig. 14) eigentlich wie der Trunk-AP, der in Fig. 11 dargestellt ist. Vorzugsweise werden die Basisstationsprotokollstapel in einen drahtlosen Hub und einen Trunk-AP mit einem Ethernet dazwischen aufgeteilt. In einer Zelle mit N Sektoren gibt es N Zugangspunkte und einen einzigen drahtlosen Hub.

[0103] Das Backhaul-Netz von der Basisstation zur MSC hat die folgenden Attribute:

1. Das Netz ist zum Weiterleiten von IP-Datagrammen zwischen der Basisstation und der MSC imstande.
2. Das Netz ist sicher. Es ist kein öffentliches Netz. Auf dem Netz ist nur Verkehr von zuverlässigen Knoten erlaubt, da das Netz nicht nur zum Transportieren von Endsystemverkehr, sondern auch zum Transportieren von Authentifizierungs-, Abrechnungs-, Registrierungs- und Verwaltungsverkehr verwendet wird.
3. Das Netz weist die notwendigen Leistungscharakteristiken auf.
4. Die Basisstationen unterstützen IP über Ethernet-Verbindungen.

[0104] In einer typischen Anwendung ist der Diensteanbieter für die Installation und die Wartung des Backhaul-Netzes, auf welchem die Betriebsmittel installiert sind, verantwortlich.

[0105] Die Basisstationen unterstützen die folgenden Backhaul-Schnittstellen zum Kommunizieren mit der MSC:

1. Die Basisstationen unterstützen IP über PPP mit HDLC-Verbindungen unter Verwendung von Punkt-zu-Punkt-T1- oder fraktionalen T3-Verbindungen.
2. Die Basisstationen unterstützen IP über Rahmenweiterleitung unter Verwendung von T1- oder fraktionalen T3-Verbindungen.
3. Die Basisstationen unterstützen IP über AAL5/ATM unter Verwendung von T1- oder fraktionalen T3-Verbindungen.

[0106] Da alle der zuvor erwähnten Schnittstellen auf IETF-Standardkapselungen basieren, können handelsübliche Router in der MSC verwendet werden, um die physikalischen Verbindungen des Backhaul-Netzes zu beenden. Höhere Schichten werden durch die verschiedenen Server und andere Prozessoren weitergegeben und verarbeitet.

[0107] Endsystemregistrierungsprozeduren über die MAC-Schicht werden unterstützt. Im Folgenden werden Endsystemregistrierungsprozeduren auf der MAC-Schicht ignoriert, ausgenommen, sie beeinflussen die Schichten darüber.

[0108] Endsysteme können sich für einen Dienst auf ihrem Heimatnetz oder von einem Fremdnetz registrieren lassen. In beiden Szenarien verwendet das Endsystem einen fremden Agenten (FA) in der Basisstation, um einen Anschlusspunkt ans Netz zu ermitteln und sich registrieren zu lassen. Im ersteren Fall ist der FA im Heimatnetz des Endsystems. Im letzteren Fall ist der FA in einem Fremdnetz. In jedem Fall verwendet das Netz eine IWF im Heimatnetz des Endsystems als einen Ankerpunkt (d.h. unveränderlich während der ganzen Sitzung trotz Mobilität). PPP-Rahmen zum und vom Endsystem pflanzen sich über den FA in der Basisstation zur IWF im Heimatnetz fort. Wenn das Endsystem zu Hause ist, wird die Heimat-IWF mittels des XTunnel-Proto-

kolls direkt mit der Basisstation verbunden. Es ist zu erwähnen, dass die Heimat-IWF mit der Basisstation auf dieselbe Weise verknüpft werden kann. Wenn das Endsystem wandert, wird eine versorgende IWF im Fremdnetz über eine I-Schnittstelle mit der Heimat-IWF verbunden. Die versorgende IWF leitet Rahmen zwischen der Basisstation und der Heimat-IWF weiter. Es ist zu erwähnen, dass auch die versorgende IWF mit der Basisstation auf dieselbe Weise verknüpft werden kann. von der Heimat-IWF werden Daten unter Verwendung des L2TP-Protokolls an einen PPP-Server, der in derselben IWF sitzen kann, oder an einen getrennten Server gesendet. Der getrennte Server kann einem Privatnetzbetreiber (z.B. ISP oder firmeneigenem Intranet) gehören und von diesem betrieben werden, der vom Drahtlosdiensteanbieter verschieden ist. Für die Dauer der Sitzung bleibt der Aufenthaltsort der Heimat-IWF und des PPP-Servers fest. Wenn das Endsystem sich während der Verbindung bewegt, muss es sich mit einem neuen fremden Agenten neu registrieren lassen. Es werden jedoch weiter dieselbe Heimat-IWF und derselbe PPP-Server verwendet. Ein neuer XTunnel wird zwischen dem neuen FA und der IWF erzeugt, und der alte XTunnel zwischen dem alten fremden Agenten und der IWF wird zerstört.

[0109] Fig. 15 stellt diese Netzkonfiguration für zwei Endsysteme A und B dar, deren beider drahtloses Heimatnetz der Drahtlosdiensteanbieter A (WSP-A) ist. Ein Endsystem wird vom drahtlosen Heimatnetz registriert, und das andere von einem drahtlosen Fremdnetz. Die Heimat-IWF im WSP-A dient als der Ankerpunkt für beide Endsysteme. Für beide Endsysteme werden Daten zur Heimat-IWF weitergeleitet. Die Heimat-IWF setzt sich mit einem Internetdiensteanbieter-PPP-Server in Verbindung, welcher dem ISP-A gehört.

[0110] Hierbei wird vorausgesetzt, dass beide Endsysteme ein Abonnement beim selben ISP haben. Wenn dies nicht der Fall wäre, dann würde die Heimat-IWF so dargestellt, dass sie auch mit einem anderen ISP verbunden wäre.

[0111] Innerhalb des Netzes eines Drahtlosdiensteanbieters werden Daten zwischen Basisstationen und der IWF unter Verwendung des XTunnel-Protokolls übertragen. Daten zwischen der IWF und dem PPP-Server werden unter Verwendung des Schicht-2-Tunnelprotokolls (L2TP) übertragen. Daten zwischen der versorgenden IWF und der Heimat-IWF werden unter Verwendung des I-XTunnel-Protokolls übertragen.

[0112] In einem einfachen Szenarium kann für einen Benutzer in seinem Heimatnetz, der einen festen Dienst anfordert, die Heimat-IWF-Funktion in der Basisstation dynamisch ausgelöst werden. Außerdem kann die versorgende IWF-Funktion für einen Gastbenutzer in der Basisstation aktiviert werden.

[0113] Stets eine IWF im Heimatnetz zu verwenden, hat seine Vor- und Nachteile. Ein offensichtlicher Vorteil ist Einfachheit. Ein Nachteil ist, dass ständig Daten zu und von einer möglicherweise entfernten Heimat-IWF weitergeleitet werden müssen. Die Alternative ist, sämtliche notwendigen Informationen an die versorgende IWF zu senden, damit sie sich mit dem ISP/Intranet des Endsystems in Verbindung setzen kann, und damit die versorgende IWF Abrechnungsinformationen in Fastechtzeit zurück zum Abrechnungsserver im Heimatnetz senden kann. Diese Funktionalität ist komplexer zu implementieren, aber wirksamer, da sie die Notwendigkeit verringert, Daten über potenziell lange Entfernungen vom Fremdnetz zum Heimatnetz weiterleiten zu müssen.

[0114] Man betrachte zum Beispiel den Fall eines Benutzers, der von Chicago nach Hongkong wandert. Wenn das Heimatnetz des Benutzers in Chicago ist und der Benutzer sich unter Verwendung eines Drahtlosdienstanbieters in Hongkong registrieren lässt, dann ist in der ersten Konfiguration die Heimat-IWF in Chicago der Ankerpunkt, und alle Daten müssen von Hongkong nach Chicago und umgekehrt weitergeleitet werden. Die Heimat-IWF in Chicago setzt sich mit dem ISP des Benutzers in Chicago in Verbindung. Bei der zweiten Konfiguration wird dem Endsystembenutzer ein ISP in Hongkong zugeordnet. Demnach müssen die Daten nicht ständig zwischen Chicago und Hongkong hin- und hergeleitet werden. In der zweiten Konfiguration dient die versorgende IWF als der Anker und ändert sich für die Dauer der Sitzung nie, selbst wenn das Endsystem sich bewegt. Der Aufenthaltsort des FAs kann sich jedoch infolge einer Endsystembewegung in Hongkong ändern.

[0115] Fig. 16 stellt die zweite Konfiguration dar. In dieser Figur ist WSP-A das Heimatnetz für das Endsystem A und B. Das Endsystem A lässt sich von seinem Heimatnetz unter Verwendung seiner Heimat-IWF als Ankerpunkt registrieren und setzt sich unter Verwendung des ISP-PPP-Servers auch mit seinem ISP-A in Verbindung. Das Endsystem B lässt sich vom Fremdnetz von WSP-B registrieren und verwendet eine versorgende IWF, welche als der Ankerpunkt dient und das Endsystem unter Verwendung des ISP-PPP-Servers mit einem ISP verbindet. In dieser Konfiguration müssen Daten für das Endsystem B nicht vom Fremdnetz zum Heimatnetz und umgekehrt weitergeleitet werden.

[0116] Damit diese Konfiguration funktioniert, muss es nicht nur Roaming-Vereinbarungen zwischen den fremden und Heimat- Drahtlosdiensteanbietern geben, sondern es muss auch Vereinbarungen zwischen dem fremden Drahtlosdiensteanbieter und dem Internetdiensteanbieter des Endsystems direkt oder durch einen Vermittler geben. In dem zuvor dargelegten Beispiel muss nicht nur der Drahtlosdiensteanbieter in Hongkong eine Geschäftsvereinbarung mit dem Drahtlosdiensteanbieter in Chicago haben, sondern der WSP in Hongkong muss auch eine Geschäftsvereinbarung mit dem Chicagoer ISP des Benutzers und Zugang zum Chicagoer ISP-PPP-Server in Hongkong oder eine Geschäftsvereinbarung mit einem anderen ISP vor Ort in Hongkong haben, der eine Geschäftsvereinbarung für Roaming mit dem Chicagoer ISP des Benutzers hat. Außerdem muss der WSP in Hongkong imstande sein, diese Roaming-Verhältnisse dynamisch zu ermitteln, um eine Benutzer-Authentifizierung und -Abrechnung durchzuführen und die geeigneten Tunnel aufzubauen.

[0117] Es ist schwierig für diese Unternehmen, die im Internetinfrastrukturgeschäft sind, geeignete Standards in der IETF für all diese Szenarien auszuarbeiten. Demnach ist eine bevorzugte Ausführungsform für die vorliegende Erfindung, die einfachere, potenziell weniger wirksame Konfiguration zu implementieren, wobei die IWF im Heimatnetz stets als der Ankerpunkt verwendet wird. Bei Vorhandensein einer geeigneten Industriestandardisierung von Protokollen für das Internet-Roaming sollte die zweite Konfiguration als gleichwertige oder alternative Ausführungsform betrachtet werden.

[0118] Ein Endsystem muss sich beim drahtlosen Netz registrieren lassen, bevor es das PPP starten und Daten senden und empfangen kann. Das Endsystem durchläuft zuerst die FA-Ermittlungs- und -Registrierungsphasen. Diese Phasen authentifizieren und registrieren das Endsystem für den Drahtlosdiensteanbieter. Sobald diese Phasen vorüber sind, startet das Endsystem das PPP. Dies umfasst die PPP-Verbindungsherstellungsphase, die PPP-Authentifizierungsphase und die PPP-Netzsteuerungsprotokollphase. Sobald diese Phasen vorüber sind, ist das Endsystem imstande, IP-Pakete unter Verwendung des PPPs zu senden und zu empfangen.

[0119] Die folgende Erörterung geht davon aus, dass das Endsystem wandert und sich von einem Fremdnetz registrieren lässt. Während der FA-Ermittlungsphase wartet das Endsystem (durch seinen Benutzerregistrierungsagenten) auf eine Ankündigung vom fremden Agenten oder ruft sie bei diesem ab. Der Benutzerregistrierungsagent verwendet Ankündigungsnachrichten, die durch einen nahe gelegenen fremden Agenten gesendet werden, um die Identität des FAs zu ermitteln, und zum Registrieren. Während dieser Phase wählt der Benutzerregistrierungsagent des Endsystems einen FA aus und gibt eine Registrierungsaufforderung an ihn aus. Der FA, der als ein Proxy-Registrierungsagent agiert, übermittelt die Registrierungsaufforderung an seinen Registrierungsserver (den Registrierungsserver im fremden WSP). Der Registrierungsserver verwendet den User-Name aus der Aufforderung des Benutzerregistrierungsagenten, um das Heimatnetz des Endsystems zu bestimmen, und übermittelt die Registrierungsaufforderung zur Authentifizierung an einen Registrierungsserver im Heimatnetz. Nach Empfang der Registrierungsaufforderung, die durch den fremden Registrierungsserver weitergeleitet wurde, authentifiziert der Heimatregistrierungsserver die Identität des fremden Registrierungsservers, und er authentifiziert auch die Identität des Endsystems. Wenn die Authentifizierung und die Registrierung erfolgreich sind, wählt der Heimatregistrierungsserver eine IWF im Heimatnetz aus, um eine I-XTunnel-Verbindung zwischen der Heimat-IWF und der versorgenden IWF (im fremden WSP) zu erzeugen. Die IWF im Heimatnetz dient für die Dauer der PPP-Sitzung als der Ankerpunkt.

[0120] Sobald die Authentifizierungs- und Registrierungsphasen vorüber sind, werden die verschiedenen PPP-Phasen gestartet. Beim Start des PPPs wird zwischen der Heimat-IWF und dem angeforderten ISP/Intranet-PPP-Server eine L2TP-Verbindung hergestellt. In der PPP-Authentifizierungsphase werden unter Verwendung von PAP oder CHAP PPP-Passwörter ausgetauscht, und der ISP- oder Intranet-PPP-Server authentifiziert unabhängig die Identität des Endsystems.

[0121] Sobald dies gelingt, wird die PPP-Netzsteuerungsphase gestartet. In dieser Phase wird eine IP-Adresse ausgehandelt und durch den PPP-Server dem Endsystem zugeordnet, und es wird die Verwendung einer TCP/IP-Kopf-Kompression ausgehandelt. Wenn dies abgeschlossen ist, ist das Endsystem imstande, IP-Pakete unter Verwendung des PPPs zu seinem ISP oder einem firmeneigenes Intranet zu senden und zu empfangen.

[0122] Es ist zu erwähnen dass zwei Authentifizierungsstufen durchgeführt werden. Die Authentifizierung authentifiziert die Identität des Endsystems für den Registrierungsserver im Heimatnetz und die Identitäten des Fremdnetzes und des Heimatnetzes untereinander. Zur Durchführung dieser Funktion übermittelt der fremde Agent die Registrierungsaufforderung des Endsystems zum Beispiel unter Verwendung eines IETF Radius-Protokolls in einem Radius Access-Request- oder Radius-Zugangsanforderungs-Paket an einen Registrie-

rungsserver in seiner lokalen MSC. Durch Verwenden des Domänennamens des Endsystems bestimmt der fremde Registrierungsserver die Identität des Heimatnetzes und des Heimatregistrierungsservers des Endsystems und verkapselt und übermittelt als ein Radius-Proxy agierend die Anforderung an den Heimatregistrierungsserver des Endsystems. Wenn der fremde Registrierungsserver die Identität der Heimat des Endsystems nicht feststellen kann, kann er die Radius-Anforderung optional an einen Registrierungsserver übermitteln, der wie ein Makler agiert (z.B. einer, der einem Konsortium von Drahtlosdiensteanbietern gehört), welcher die Radius Access-Request seinerseits zum Endheimatregistrierungsserver durchreicht. Wenn der lokale Registrierungsserver außerstande ist, die Registrierungsaufforderung lokal oder durch Durchreichen zu versorgen, dann weist er die Registrierungsaufforderung des fremden Agenten ab, und der fremde Agent weist die Registrierungsaufforderung des Endsystems ab. Bei Empfang der Radius Access-Request führt der Heimatregistrierungsserver die erforderliche Authentifizierung der Identitäten des Fremdnetzes und des Endsystems durch. Wenn die Authentifizierung und die Registrierung erfolgreich sind, antwortet der Heimatregistrierungsserver mit einem Radius Access-Response-Radius-Zugangsantwort-Paket an fremden Registrierungsserver, der eine Antwort an den fremden Agenten sendet, so dass ein Umlauf abgeschlossen werden kann. Die Registrierungsaufforderung wird abgewiesen, wenn der Heimatregistrierungsserver aus irgendeinem Grund außerstande ist, zu entsprechen.

[0123] Die zweite Authentifizierungsstufe überprüft die Identität des Endsystems für den Intranet- oder ISP-PPP-Server. Eine von der Mobilitätsauthentifizierung getrennte PPP-Authentifizierung ermöglicht es, die Infrastrukturbetriebsmittel getrennt vom ISP einzusetzen und zu besitzen.

[0124] Fig. 17 ist ein Leiterdiagramm, das die Registrierungsfolge für ein Gast-Endsystem darstellt. Es wird davon ausgegangen, dass der PPP-Server und die Heimat-IWF im selben Server sind und kein L2TP benötigt wird. Man beachte die Interaktionen mit Abrechnungsservern, um mit der Abrechnung für das zu registrierende Endsystem zu beginnen, sowie mit Verzeichnisservern, um die Identität des Heimatregistrierungsserver zu bestimmen und die Identität des Endsystems zu authentifizieren. Nähere Informationen über Abrechnung, Gebührenverrechnung, Roaming (zwischen Diensteanbietern) und Zahlung werden im Folgenden bereitgestellt.

[0125] MAC-Schicht-Nachrichten vom Benutzerregistrierungsagenten des Endsystems können verwendet werden, um einen Agent Solicitation oder Agentenabruf einzuleiten. Die MAC-Schicht-Nachrichten sind der Klarheit halber nicht dargestellt.

[0126] In Fig. 17 ruft das Endsystem (Mobileinheit) anfänglich eine Ankündigung ab, und der fremde Agent antwortet mit einer Ankündigung, die das Endsystem mit Informationen über das Netz, zu welchem der fremde Agent gehört, einschließlich einer Gastadresse des fremden Agenten versieht. Alternativerweise kann diese Phase weggelassen werden, und sämtliche Netzankündigungen können durch eine kontinuierlich ausgegebene MAC-Schicht-Bakennachricht erfolgen. In diesem Fall wird davon ausgegangen, dass das Netz ein fremder Drahtlosdiensteanbieter ist. Dann nimmt ein Benutzerregistrierungsagent (im Endsystem) die Informationen über den fremden Agenten (welche den Benutzernamen und andere Sicherheitsnachweise enthalten) und sein Netz in eine Aufforderung auf und sendet die Aufforderung an den fremden Agenten. Der fremde Agent als ein Proxy-Registrierungsagent leitet die Aufforderung an den fremden Registrierungsserver (d.h. den Registrierungsserver für den fremden Drahtlosdiensteanbieter) weiter. Dann greift der fremde Registrierungsserver, der erkennt, dass es sich nicht um das Heimatverzeichnis handelt, auf den fremden Verzeichnisserver mit dem FDD im fremden Drahtlosdiensteanbieter zu, um zu erfahren, wie er die Registrierungsaufforderung zum Heimatregistrierungsserver des Drahtlosdiensteanbieter, zu welchem das Endsystem gehört, leiten soll. Der fremde Registrierungsserver antwortet mit den erforderlichen Übermittlungsnachrichten. Dann kapselt der fremde Registrierungsserver die Registrierungsaufforderung des Endsystems in einer Radius-Zugangsanforderung ein und leitet die eingekapselte Anforderung an den Heimatregistrierungsserver des Drahtlosdiensteanbieters, zu welchem das Endsystem gehört. Der Heimatregistrierungsserver greift auf den Heimatverzeichnisserver mit dem HDD des Heimatregistrierungsservers zu, um wenigstens Authentifizierungsinformationen über den fremden Diensteanbieter zu erfahren. Optional greift der Heimatregistrierungsserver auf das Teilnehmerverzeichnis zu, um detaillierte Teilnehmerdienstprofilinformationen (z.B. abonnierte Dienstgüteoptionen usw.) zu erfahren. Wenn alle Partner authentifiziert sind, sendet der Heimatregistrierungsserver eine IWF-Start-Aufforderung an die Heimat-IWF und den PPP-Server. Die Heimat-IWF und der PPP-Server starten den Heimatabrechnungsserver und senden dann eine IWF-Start-Antwort an den Heimatregistrierungsserver. Der Heimatregistrierungsserver sendet dann eine Radius-Zugangsantwort an den fremden Registrierungsserver. Der fremde Registrierungsserver sendet dann eine IWF-Start-Aufforderung an den Server der versorgenden IWF. Der Server der versorgenden IWF startet den versorgenden Abrechnungsserver und sendet dann eine IWF-Start-Antwort an den fremden Registrierungsserver. Der fremde Registrierungsserver sendet eine Registrierungsantwort an den fremden Agenten, und der fremde Agent leitet die Registrierungsantwort an das Endsystem weiter.

[0127] Eine Übertragungssteuerungsprotokoll- oder LCP-Konfigurationsaufforderung (LCP für engl. link control protocol) wird vom Endsystem durch den fremden Registrierungsserver an die Heimat-IWF und den PPP-Server gesendet. Die Heimat-IWF und der PPP-Server senden eine LCP-Konfigurationsbestätigung durch den fremden Registrierungsserver an das Endsystem.

[0128] Ähnlich wird eine Passwortauthentifizierungsprotokoll- oder PAP-Authentifizierungsaufforderung durch die Heimat-IWF und den PPP-Server gesendet und bestätigt.

[0129] Alternativerweise kann ein Abfrageauthentifizierungsprotokoll (CHAP für engl. challenge authentication protocol) zur Authentifizierung verwendet werden. Beide Protokolle können zur Authentifizierung verwendet werden, oder diese Phase kann übersprungen werden.

[0130] Ähnlich wird eine IP-Konfiguratonsprotokoll- oder IPCP-Konfigurationsaufforderung durch die Heimat-IWF und den PPP-Server gesendet und bestätigt.

[0131] Die Verbindung mit dem Endsystem kann aus irgendeinem der folgenden Gründe beendet werden:

1. Vom Benutzer eingeleitete Beendigung. Gemäß diesem Szenarium beendet das Endsystem als Erstes das PPP auf gleitende Weise. Dies umfasst das Beenden des PPP-Netzsteuerungsprotokolls (IPCP), worauf das PPP-Verbindungsprotokoll beendet wird. Sobald dies geschehen ist, lässt sich das Endsystem aus Netzregister löschen, worauf die Funkverbindung mit dem Zugangspunkt beendet wird.
2. Unterbrechung der drahtlosen Verbindung. Dieses Szenarium wird vom Modem erkannt und dem Modemtreiber im Endsystem gemeldet. Die oberen Schichten der Software werden informiert, um die Stapel zu beenden und den Benutzer zu benachrichtigen.
3. Unterbrechung der Verbindung mit dem fremden Agenten. Dieses Szenarium wird vom Mobilitätstreiber im Endsystem erkannt. Nach dem Versuch und Fehlschlag, mit einem (potenziell neuen) fremden Agenten Kontakt neu herzustellen, sendet der Treiber eine entsprechende Mitteilung den Protokollstapel hinauf und signalisiert auch der Modemhardware unten, die drahtlose Verbindung zu beenden.
4. Unterbrechung der Verbindung mit der IWF. Hier gilt im Wesentlichen dasselbe wie für die Unterbrechung mit dem fremden Agenten.
5. Beendigung von PPP durch IWF oder PPP-Server. Dieses Szenarium wird durch die PPP-Software im Endsystem erkannt. Der PPP-Treiber des Endsystems wird von diesem Ereignis unterrichtet. Er leitet eine Löschung aus dem Netzregister ein, worauf die drahtlose Verbindung mit dem Zugangspunkt beendet wird.

[0132] Endsystemdienstkonfiguration bezieht sich auf das Konzept des Konfigurierens des Netzdienstes für ein Endsystem basierend auf dem Teilnehmerdienstprofil. Das Teilnehmerdienstprofil ist in einem Teilnehmerverzeichnis gespeichert. Das Dienstprofil enthält Informationen, um die Software zu befähigen, den drahtlosen Datendienst für den Teilnehmer kundenspezifisch einzustellen. Es umfasst Informationen, um das Endsystem zu authentifizieren, dem Endsystem zu erlauben, zu wandern, und Verbindungen mit dem Internetdiensteanbieter des Endsystems herzustellen. Vorzugsweise umfassen diese Informationen auch andere Parameter wie Dienstgüte. Zusätzlich zum Teilnehmerverzeichnis werden ein Heimatdomänenverzeichnis (HDD für engl. home domain directory) und ein Fremddomänenverzeichnis (FDD für engl. foreign domain directory) für das Roaming und zur Authentifizierung des fremden und des Heimatregistrierungsservers untereinander verwendet. Das HDD speichert Informationen über das Heimatnetz des Endsystems, und das FDD speichert Informationen über Fremdnetze, die ein Teilnehmer besuchen könnte.

[0133] Fig. 18 zeigt, wie diese Verzeichnisse in die Netzarchitektur abbilden und während der Registrierung für ein Endsystem verwendet werden, das sich zu Hause registrieren lässt. Bei Schritt 0 ruft das Endsystem (Mobileinheit) eine Ankündigung ab und empfängt sie vom fremden Agenten, um das Endsystem mit Informationen über das Netz zu versehen, zu welchem der fremde Agent gehört. In diesem Fall ist das Netz der Heimat-Drahtlosdiensteanbieter. Bei Schritt 1 nimmt der Benutzerregistrierungsagent (im Endsystem) die Informationen über den fremden Agenten, sein Netz und seine Sicherheitsnachweise in eine Aufforderung auf und sendet die Aufforderung an den fremden Agenten. Bei Schritt 2 leitet der fremde Agent als ein Proxy-Registrierungsagent die Aufforderung an den Heimatregistrierungsserver weiter. Bei Schritt 3 greift der Heimatregistrierungsserver auf das HDD des Heimat-Drahtlosdiensteanbieters zu, um wenigstens Authentifizierungsinformationen zu erfahren. Bei Schritt 4 greift der Heimatregistrierungsserver auf das Teilnehmerverzeichnis zu, um detaillierte Teilnehmerdienstprofilinformationen (z.B. abonnierte Dienstgüteoptionen usw.) zu erfahren. Bei Schritt 5 teilt der Heimatregistrierungsserver dem fremden Agenten die Zugangsantwort mit. Bei Schritt 6 und 7 teilt der fremde Agent dem Endsystem (d.h. der Mobileinheit) die Registrierungsantwort mit.

[0134] Fig. 19 stellt die Verzeichnisnutzung für ein Endsystem dar, das sich von einem Fremdnetz registrieren

lässt. Bei Schritt 0 ruft das Endsystem (Mobileinheit) eine Ankündigung ab, und der fremde Agent kündigt an, was das Endsystem mit Informationen über das Netz versieht, zu welchem der fremde Agent gehört. In diesem Fall ist das Netz ein fremder Drahtlosdiensteanbieter. Bei Schritt 1 nimmt der Benutzerregistrierungsserver (im Endsystem) die Informationen über den fremden Agenten, sein Netz und seine Sicherheitsnachweise in eine Aufforderung auf und sendet die Aufforderung an den fremden Agenten. Bei Schritt 2 leitet der fremde Agent als ein Proxy-Registrierungsagent die Aufforderung an den fremden Registrierungsserver (d.h. den Registrierungsserver für den fremden Drahtlosdiensteanbieter) weiter. Bei Schritt 3 greift der fremde Registrierungsserver auf das HDD des fremden Drahtlosdiensteanbieters zu, um zu erfahren, zu welchem Netz das Endsystem gehört. Bei Schritt 4 übermittelt der fremde Registrierungsserver die Aufforderung des Endsystems an den Heimatregistrierungsserver des Heimat-Drahtlosdiensteanbieters des Endsystems. Bei Schritt 5 greift der Heimatregistrierungsserver auf das FDD des Heimatregistrierungsservers zu, um wenigstens Authentifizierungsinformationen über den fremden Diensteanbeiter zu erfahren. Bei Schritt 6 greift der Heimatregistrierungsserver auf das Teilnehmerverzeichnis zu, um detaillierte Teilnehmerdienstprofilinformationen (z.B. abonnierte Dienstgüteoptionen usw.) zu erfahren. Bei Schritt 7 teilt der Heimatregistrierungsserver dem fremden Registrierungsserver die Zugangsantwort mit. Bei Schritt 8 übermittelt der fremde Registrierungsserver die Zugangsantwort an den fremden Agenten. Bei Schritt 9 teilt der fremde Agent dem Endsystem (d.h. der Mobileinheit) die Registrierungsantwort mit.

[0135] Protokollabwicklungsszenarien zum Bearbeiten von Trägerdaten und die zugehörigen Stapel zum Transportieren von Trägerdaten zu und von einem Endsystem, die Protokollstapel für die Zellarchitekturen, die lokale APs (**Fig. 20**) und abgesetzte APs (**Fig. 21**) verwenden.

[0136] **Fig. 20** stellt Protokollstapel zum Abwickeln von Kommunikationen zwischen einem Endsystem (in seinem Heimatnetz) und einer Heimat-IWF für End system@Home dar. **Fig. 20** zeigt die Protokollabwicklung für eine Zellarchitektur, in welcher der Zugangspunkt und der drahtlose Hub ortsgleich untergebracht sind.

[0137] **Fig. 21** zeigt die Protokollabwicklung für eine Zellarchitektur, in welcher der Zugangspunkt abgesetzt vom drahtlosen angeordnet ist. Wie dargestellt, endet das PPP in der IWF, und die Konfiguration stellt einen direkten Internetzugang bereit. Die Konfiguration für den Fall, in dem der PPP-Server von der IWF getrennt ist, wird später beschrieben.

[0138] In **Fig. 21** werden PPP-Rahmen für das Endsystem in Funkverbindungsprotokoll- oder RLP-Rahmen (für engl. radio link protocol) eingekapselt, welche am abgesetzten Zugangspunkt zur Kommunikation mit dem Trunk-Zugangspunkt (d.h. einem Zugangspunkt, der physisch in der Nähe des drahtlosen Hubs angeordnet ist) in MAC-Rahmen eingekapselt werden, wobei der abgesetzte Zugangspunkt zum Beispiel durch einen drahtlosen Trunk mit dem Zugangspunkt verbunden ist. Der Zugangspunkt fungiert als eine MAC-Schicht-Brücke und leitet Rahmen von der Luftverbindung an den fremden Agenten im drahtlosen Hub weiter. Der fremde Agent entkapselt die RLP-Rahmen aus den MAC-Rahmen und leitet die RLP-Rahmen unter Verwendung des XTunnel-Protokolls an die IWF weiter. Ein ähnlicher, obgleich umgekehrter Prozess findet bei der Übertragung von Rahmen von der IWF zum Endsystem statt.

[0139] Wenn das Endsystem sich zu einem anderen fremden Agenten bewegt, dann wird automatisch ein neuer XTunnel zwischen dem neuen fremden Agenten und der IWF erzeugt, damit der PPP-Verkehr dazwischen weiter ohne Unterbrechung fließt.

[0140] In der Zellarchitektur mit abgesetztem AP (**Fig. 21**), die drahtlose Trunks zwischen dem abgesetzten AP und dem Trunk-AP verwendet, kann die Luftverbindung zwischen dem Endsystem und dem Zugangspunkt gegenüber der Frequenz (f2) und der Funktechnik des Trunks auf einer anderen Frequenz (f1) arbeiten und eine andere Funktechnik verwenden.

[0141] **Fig. 22** stellt die Protokollstapel für ein Gast-Endsystem dar. Die versorgende IWF verwendet das I-XTunnel-Protokoll zwischen der versorgenden IWF und der Heimat-IWF. Der Rest des Protokollstapels bleibt unverändert und ist nicht dargestellt. Diese Architektur kann durch Einfügen der versorgenden IWF in die Basisstation vereinfacht werden, wodurch das XWD-Protokoll eliminiert wird.

[0142] Die RLP-Schicht verwendet Folgenummern, um doppelte PPP-Datagramme zu löschen und eine In-Folge-Zustellung von PPP-Datagrammen zwischen dem Endsystem und der IWF bereitzustellen. Sie stellt auch einen konfigurierbaren Keep-alive-Mechanismus bereit, um die Streckenverbindungsfähigkeit zwischen dem Endsystem und IWF zu überwachen. Außerdem stellt die RLP-Schicht in einer alternativen Ausführungsform auch Wiederholungssendungs- und Flusssteuerungsdienste bereit, um die Gesamtbitfehlerrate der Ver-

bindung zwischen dem Endsystem und der IWF zu verringern. Das RLP zwischen dem Endsystem und der IWF wird am Beginn der Sitzung gestartet und bleibt während der ganzen Sitzung und selbst über Weiterschaltungen aktiv.

[0143] Im Gegensatz zur Spezifikation im Mobile IP RFC (RFC **2003**) wird keine IP-in-IP-Kapselung zum Tunneln zwischen dem fremden Agenten und der Heimat-IWF verwendet. Stattdessen wird ein neues Tunnelprotokoll verwendet, das über dem UDP implementiert wird. Dieses Tunnelprotokoll ist eine vereinfachte Version des L2TP-Protokolls. Die Gründe für diese Wahl sind Folgende:

1. Das Kapselungsprotokoll, das in RFC 2003 spezifiziert ist, stellt keine Flusssteuerung oder In-Folge-Zustellung von Paketen bereit. Das gegenwärtig beschriebene Netz benötigt diese Dienste möglicherweise im Tunnel über den Backhaul. Eine Flussteuerung kann erforderlich sein, um die Menge von Wiederholungssendungen über die Luftverbindung aufgrund von Paketverlust infolge von Flusssteuerungsproblemen über das Netz zwischen der Basisstation und der MSC oder aufgrund von Flussteuerungsproblemen in der Basisstation oder der IWF zu verringern.
2. Durch Verwenden eines UDP-basierten Tunnelprotokolls kann die Implementierung auf der Benutzerebene erfolgen und dann aus Leistungsgründen nach seiner Entstörung in den Kernel gesetzt werden.
3. Bei Verwenden von RFC 2003 gibt es keine leichte Möglichkeit, Tunnel unter Berücksichtigung von Dienstgüte und Lastausgleich zu erzeugen. Um die QOS zu berücksichtigen, sollte es möglich sein, Tunnel über Verbindungen aufzubauen, welche die erforderliche QOS bereits vorsehen. Zweitens gibt es bei Verwenden von RFC 2003 keine leichte Möglichkeit, einen Lastausgleich bereitzustellen, um die Trägerverkehrslast über mehrere Verbindungen zwischen der Basisstation und der MSC zu verteilen.
4. Um eine IP-in-IP-Kapselung zu implementieren, wie in RFC 2003 spezifiziert, benötigen die Entwickler Zugang zum IP-Quellcode. In kommerziellen Betriebssystemen ist der Quellcode für den TCP/IP-Stapel im Allgemeinen das Eigentum anderer Gerätehersteller. Der Erwerb des TCP/IP-Stapels von einem Hersteller und die Vornahme von Änderungen an der IP-Schicht, um den Mobile-IP-Tunnelaufbau zu unterstützen, würden von einem Entwickler verlangen, eine abweichende Version des TCP/IP-Stapels zu unterstützen. Dies fügt Kosten und Risiko hinzu.

[0144] Obwohl zu beachten ist, dass das Tunnelprotokoll zwischen der Basisstation und der IWF nicht standardmäßig ist und dass der Drahtlosdiensteanbieter nicht imstande ist, Betriebsmittel von verschiedenen Herstellern zu kombinieren und anzupassen, ist die Verwendung eines nicht standardmäßigen Tunnelprotokolls innerhalb eines einzelnen Drahtlosdiensteanbieternetzes für Endsysteme und Betriebsmittel von anderen Herstellern transparent.

[0145] Das neue Tunnelprotokoll basiert auf dem L2TP. Das L2TP an sich ist ein stark belastetes Tunnelprotokoll, so dass das L2TP einen hohen Zusatzaufwand in Verbindung mit der Tunnelerzeugung und Authentifizierung hat. Das neue Tunnelprotokoll der vorliegenden Erfindung hat weniger Zusatzaufwand. Das neue XTunnel- und I-XTunnel-Protokoll kann die folgenden Merkmale aufweisen:

1. Die XTunnel- und I-XTunnel-Erzeugung fügt den Radius Access Request- und Radius Access Response-Nachrichten zwischen der Basisstation und dem Registrierungsserver herstellerspezifische Erweiterungen hinzu. Diese Erweiterungen verhandeln Tunnelparameter und, um den Tunnel zu erzeugen.
2. Der Registrierungsserver ist imstande, die tatsächliche Arbeit des Tunnelaufbaus und der Weiterleitung von Paketen an verschiedene IP-Adressen und daher an einen anderen Server in der MSC delegieren. Dies ermöglicht es dem Registrierungsserver, einen Lastausgleich über mehrere IWF-Server durchzuführen und eine unterschiedliche QOS für verschiedene Benutzer bereitzustellen.
3. Das XTunnel- und I-XTunnel-Protokoll unterstützt Inband-Steuernachrichten zur Tunnelverwaltung. Diese Nachrichten umfassen Echoabfrage/antwort zum Prüfen der Tunnelverbindungsfähigkeit, Trennungs-Anforderung/Antwort/Meldung zum Trennen des Tunnels und Fehlermeldung für Fehlermitteilungen. Diese Nachrichten werden über die Tunnelmedien, zum Beispiel UDP/IP, gesendet.
4. Das XTunnel- und I-XTunnel-Protokoll sendet Nutzdaten über die Tunnelmedien, zum Beispiel UDP/IP. Das XTunnel- und I-XTunnel-Protokoll unterstützt Flusssteuerung und In-Folge-Paketzustellung.
5. Das XTunnel- und I-XTunnel-Protokoll kann über andere Medien als UDP/IP für Dienstgüte implementiert werden.

[0146] Das Netz unterstützt eine direkte Internetverbindungsfähigkeit, indem das PPP in der Heimat-IWF beendet wird und IP-Pakete von der IWF zum Internet über einen Router weitergeleitet werden, der standardmäßige IP-Leitweglenkungsprotokolle verwendet. Vorzugsweise führt die IWF das RIP aus, und der Router führt ebenfalls das RIP und möglicherweise andere Leitweglenkungsprotokolle wie OSPF aus.

[0147] Das Netz unterstützt eine erste Konfiguration für einen Drahtlosdiensteanbieter, der auch ein Internet-

diensteanbieter ist. In dieser Konfiguration fungiert die Heimat-IWF in der MSC auch als ein PPP-Server. Diese IWF führt auch Internetleitweglenkungsprotokolle wie RIP aus und verwendet einen Router, um sich ans Backbone-Netz des Internetdiensteanbieters anzuschließen.

[0148] Das Netz unterstützt eine zweite Konfiguration für einen Drahtlosdiensteanbieter, der wünscht, es Endsystemen zu ermöglichen, sich an einen oder mehr Internetdiensteanbieter anzuschließen, weil der WSP entweder selbst kein ISP ist oder weil der WSP Vereinbarungen mit anderen ISPs hat, um Endbenutzern Zugang zu verschaffen. Zum Beispiel kann ein Drahtlosdiensteanbieter sich dafür entscheiden, einem Endbenutzer Zugang anzubieten, und er kann eine Vereinbarung mit einem Fremd-ISP haben, um dem Benutzer, der auch ein Konto beim Fremd-ISP hat, den Zugang zum ISP vom WSP-Netz zu ermöglichen. In dieser Konfiguration läuft der PPP-Server nicht in der Heimat-IWF, die in der MSC installiert ist. Stattdessen wird ein Tunnelprotokoll, wie L2TP (Schicht-zwei-Tunnelprotokoll), zum Zurücktunneln zum PPP-Server des ISPs verwendet. Fig. 10 stellt die Protokollstapel für diese Konfiguration für ein Endsystem dar, das zu Hause ist.

[0149] Der Aufenthaltsort der Heimat-IWF und des ISP-PPP-Servers bleibt während der ganzen PPP-Sitzung fest. Außerdem bleibt der L2TP-Tunnel zwischen der IWF und dem ISP-PPP-Server während der ganzen PPP-Sitzung aufrecht. Die physikalische Strecke zwischen der IWF und dem PPP-Server ist über einen Router, der ein dediziertes T1- oder T3-, ein Rahmenweiterleitungs- oder ein ATM-Netz verwendet. Die tatsächliche Beschaffenheit der physikalischen Strecke ist vom Gesichtspunkt der Architektur nicht wichtig.

[0150] Diese Konfiguration unterstützt auch den Intranetzugang. Für den Intranetzugang sitzt der PPP-Server im firmeneignen Intranet, und die Heimat-IWF verwendet das L2TP, um zu ihm zu tunneln.

[0151] Für ein festes Endsystem ist die Protokollabwicklung für den Intranet- oder ISP-Zugang so, wie in Fig. 23 dargestellt, mit dem Unterschied, dass das Gast-Endsystem eine versorgende IWF verwendet, um sich mit seiner Heimat-IWF in Verbindung setzen. Die Protokollabwicklung zwischen einer versorgenden IWF und einer Heimat-IWF wurde bereits beschrieben. In Fig. 23 kann die Heimat-IWF in den drahtlosen Hub eingefügt werden, wodurch das XTunnel-Protokoll eliminiert wird. Auch die versorgende IWF kann in den drahtlosen Hub eingefügt werden, wodurch das XTunnel-Protokoll eliminiert wird.

[0152] Fig. 24 stellt die Protokollstapel, welche während der Registrierungsphase (Endsystemregistrierung) verwendet werden, für eine Zellarchitektur mit lokalem Zugangspunkt dar. Der Stapel für eine Architektur mit abgesetztem Zugangspunkt ist sehr ähnlich.

[0153] Das oben dargestellte Szenarium ist für ein Gast-Endsystem. Für ein Endsystem zu Hause gibt es keinen fremden Registrierungsserver auf dem Registrierungsweg.

[0154] Man beachte den Mobilitätsagenten im Endsystem. Der Mobilitätsagent im Endsystem und der fremde Agent im drahtlosen Hub sind konzeptionell ähnlich dem Mobile IP RFC 2002. Der Mobilitätsagent wickelt Netzfehler unter Verwendung von Zeitüberschreitungen und Wiederholungsversuchen ab. Im Gegensatz zu bekannten Protokollstapeln für Trägerdaten wird kein RLP verwendet. Der fremde Agent und die Registrierungsserver verwenden Radius über UDP/IP zur Kommunikation miteinander, um das Endsystem zu registrieren.

[0155] Es sind mehrere Sicherheitsaspekte zu berücksichtigen. Der erste, das Authentifizieren der Identitäten des Endsystems und des Fremd/Heimatnetzes während der drahtlosen Registrierungsphase. Der zweite, das Authentifizieren der Identität des Endsystems mit seinem PPP-Server während der PPP-Authentifizierungsphase. Der dritte, die Authentifizierung zum Speichern von Abrechnungsdaten, zum Gebührenerfassen und zum Aktualisieren von Heimatdomäneninformationen. Der vierte, die Verschlüsselung von Trägerverkehr, der zum und vom Endsystem übertragen wird. Der fünfte, die Verschlüsselung zum Austauschen von Rechnungsinformationen über Diensteanbietergrenzen.

[0156] Es werden gemeinsam benutzte Geheimcodes verwendet, um die Identität von Endsystemen mit ihren Heimatnetzen und die Identität des Heimat- und des Fremdnetzes untereinander während der drahtlosen Registrierung zu authentifizieren.

[0157] Die Endsystemauthentifizierung verwendet einen gemeinsamen benutzten 128-Bit-Geheimcode, um eine Identitätsmarke für seine Registrierungsaufforderung zu erzeugen. Die Identitätsmarke wird unter Verwendung des bekannten MD5-Message-Digest-Algorithmus, wie im Mobile IP RFC 2002 beschrieben, erzeugt. Alternativerweise kann ein anderer Algorithmus verwendet werden. Der gemeinsam benutzte Geheim-

code wird nicht in der Registrierungsaufforderung durch das Endsystem gesendet. Es wird nur die Identitätsmarke gesendet. Bei Empfang der Registrierungsaufforderung vom Endsystem errechnet der Heimatregistrierungsserver die Identitätsmarke über die Registrierungsaufforderungsdaten unter Verwendung des gemeinsam benutzten Geheimcodes neu. Wenn der errechnete Identitätsmarkenwert mit dem Identitätsmarkenwert übereinstimmt, der durch das Endsystem gesendet wurde, erlaubt der Heimatregistrierungsserver, dass der Registrierungsprozess fortgesetzt wird. Wenn die Werte nicht übereinstimmen, protokolliert der Heimatregistrierungsserver das Ereignis, erzeugt einen Sicherheitsverletzungsalarm und eine „nak" (d.h. eine negative Bestätigung) für die Aufforderung.

[0158] In der Registrierungsantwort macht der Heimatregistrierungsserver dasselbe, das heißt er verwendet den gemeinsam benutzten Geheimcode, um eine Identitätsmarke für die Registrierungsantwort zu erzeugen, die er an das Endsystem sendet. Nach Empfang der Antwort errechnet das Endsystem die Identitätsmarke unter Verwendung des gemeinsam benutzten Geheimcodes neu. Wenn der errechnete Wert nicht mit dem Identitätsmarkenwert übereinstimmt, der durch den Heimatregistrierungsserver in der Antwort gesendet wurde, verwirft das Endsystem die Antwort und versucht es erneut.

[0159] Diese Netzsicherheitskonzepte sind den Konzepten ähnlich, die im Mobile IP RFC 2002 definiert sind. Gemäß RFC besteht eine Mobilitätssicherheitsvereinbarung zwischen jedem Endsystem und seinem Heimatnetz. Jede Mobilitätssicherheitsvereinbarung definiert eine Sammlung von Sicherheitskontexten. Jeder Sicherheitskontext definiert einen Authentifizierungsalgorithmus, einen Modus, einen Geheimcode (gemeinsam benutzt oder öffentlich-privat), ein Wiederholungsschutzformat und die zu verwendende Art von Verschlüsselung. Im Kontext des vorliegenden Netzes wird der User-Name des Endsystems (anstelle der Mobile-IP-Heimatadresse) verwendet, um die Mobilitätssicherheitsvereinbarung zwischen dem Endsystem und seinem Heimatnetz zu identifizieren. Ein anderer Parameter, genannt Sicherheitsparameterindex (SPI), wird verwendet, um einen Sicherheitskontext innerhalb der Mobilitätssicherheitsvereinbarung auszuwählen. In einer grundlegenden Ausführungsform der Erfindung werden nur der vorgegebene Mobile-IP-Authentifizierungsalgorithmus (MD5-verschlüsselt) und der vorgegebene Modus („Präfix + Suffix") mit gemeinsam benutzten 128-Bit-Geheimcodes unterstützt. Netzbenutzer dürfen mehrere gemeinsam benutzte Geheimcodes mit ihrem Heimatnetz definieren. Der Mechanismus zum Erzeugen von Sicherheitskontexten für Endbenutzer, wobei jedem Sicherheitskontext ein SPI zugeordnet wird, zum Einstellen der Inhalte des Sicherheitskontextes (welcher den gemeinsam benutzten Geheimcode beinhaltet) und zum Modifizieren ihrer Inhalte wird im Folgenden beschrieben. Während der Registrierung wird durch das Endsystem unter Verwendung des MD5-Algorithmus ein 128-Bit-Message-Digest in einem Präfix+Suffix-Modus errechnet. Der gemeinsam benutzte Geheimcode wird als das Präfix und das Suffix für die Daten verwendet, die in der Registrierungsaufforderung zu schützen sind. Die auf diese Weise errechnete Identitätsmarke wird zusammen mit dem SPI und dem User-Name in der Registrierungsaufforderung durch das Endsystem gesendet. Nach Empfang der Registrierungsaufforderung des Endsystems leitet der fremde Registrierungsserver die Aufforderung zusammen mit der Identitätsmarke und dem SPI unverändert an den Heimatregistrierungsserver weiter. Nach Empfang der Registrierungsaufforderung direkt vom Endsystem oder indirekt über einen fremden Registrierungsserver verwendet der Heimatregistrierungsserver den SPI und den User-Name zur Auswahl des Sicherheitskontextes. Der Heimatserver errechnet die Identitätsmarke unter Verwendung des gemeinsam benutzten Geheimcodes neu. Wenn der errechnete Identitätsmarkenwert mit dem Wert der Identitätsmarke übereinstimmt, die in der Aufforderung durch das Endsystem gesendet wurde, ist die Identität des Benutzers erfolgreich authentifiziert. Andernfalls bestätigt der Heimatregistrierungsserver die Registrierungsaufforderung, die durch das Endsystem gesendet wurde, negativ (nak).

[0160] Die Registrierungsantwort, die durch den Heimatregistrierungsserver an das Endsystem gesendet wird, wird ebenfalls unter Verwendung des zuvor beschriebenen Algorithmus authentifiziert. Der SPI und der errechnete Identitätsmarkenwert werden in der Registrierungsantwortnachricht durch den Heimatserver an das Endsystem übertragen. Nach Empfang der Antwort errechnet das Endsystem die Identitätsmarke neu und, wenn der errechnete Wert mit dem übertragenen Wert nicht übereinstimmt, verwirft es die Antwort und versucht es erneut.

[0161] Das Endsystem des Benutzers muss für alle Sicherheitskontexte, die der Benutzer mit seinen Registrierungsserver(n) gemeinsam benutzt, mit dem gemeinsam benutzten Geheimcode und den SPIs konfiguriert werden. Diese Konfigurationsinformationen werden für Windows 95-basierte Endsysteme vorzugsweise in einem Win 95-Register gespeichert. Während der Registrierung wird auf diese Informationen zugegriffen, und sie werden für Authentifizierungszwecke verwendet.

[0162] Im Netz werden durch den fremden Agenten FA Radius-Protokolle verwendet, um das Endsystem zu

registrieren und den XTunnel zwischen dem drahtlosen Hub und der Heimat- und der versorgenden IWF für das Endsystem zu konfigurieren. Bei Empfang einer Registrierungsaufforderung vom Endsystem erzeugt der FA ein Radius Access-Request-Paket (Radius-Zugangsanforderungspaket), speichert seine eigenen Attribute ins Paket, kopiert die Registrierungsaufforderungsattribute des Endsystems unverändert in dieses Paket und sendet die verknüpfte Aufforderung an den Registrierungsserver in der MSC.

[0163] Eine Radius-Authentifizierung erfordert, dass der Radius-Client (in diesem Fall der FA in der Basisstation) und der Radius-Server (in diesem Fall der Registrierungsserver in der MSC) einen Geheimcode für Authentifizierungszwecke gemeinsam benutzen. Dieser gemeinsam benutzte Geheimcode wird auch verwendet, um alle Privatinformationen zu verschlüsseln, die zwischen dem Radius-Client und dem Radius-Server übertragen werden. Der gemeinsam benutzte Geheimcode ist ein konfigurierbarer Parameter. Das Netz folgt den Empfehlungen im Radius RFC und verwendet den gemeinsam benutzten Geheimcode und den MD5-Algorithmus zur Authentifizierung und zur Verschlüsselung, wenn eine Verschlüsselung notwendig ist. Das Radius Access-Request-Paket, das durch den FA gesendet wurde, enthält ein Radius User-Name- oder Radius-Benutzernamen-Attribut (welches durch das Endsystem bereitgestellt wird) und ein Radius User-Password- oder Radius-Benutzerpasswort-Attribut. Der Wert des User-Password-Attributs ist ebenfalls ein konfigurierbarer Wert und wird in der durch das Radius-Protokoll empfohlenen Weise verschlüsselt. Andere netzspezifische Attribute, welche vom Gesichtspunkt des Radius RFC-Standards keine standardmäßigen Attribute sind, werden als herstellerspezifische Radius-Attribute codiert und im Access-Request-Paket gesendet.

[0164] Die folgenden Attribute werden durch den FA im Radius Access-Request-Paket an seinen Registrierungsserver gesendet.

1. User-Name-Attribut. Dies ist der Benutzername des Endsystems so, wie durch das Endsystem in seiner Registrierungsaufforderung geliefert.
2. User-Password-Attribut. Dieses Benutzerpasswort wird durch die Basisstation/den drahtlosen Hub für den Benutzer geliefert. Es wird so codiert, wie im Radius RFC beschrieben, wobei der Geheimcode verwendet wird, der zwischen der Basisstation und ihrem Registrierungsserver gemeinsam benutzt wird.
3. NAS-Port. Dies ist der Anschluss auf der Basisstation.
4. NAS-IP-Address. Dies st die IP-Adresse der Basisstation.
5. Service-Type. Dies ist ein gerahmter Dienst.
6. Framed Protocol. Dies ist ein PPP-Protokoll.
7. XTunnel Protocol Parameters. Diese Parameter werden durch die Basisstation gesendet, um die Parameter zu spezifizieren, die zum Aufbau des XTunnel-Protokolls für das Endsystem notwendig sind. Dies ist ein herstellerspezifisches Attribut.
8. AP-IP-Address. Dies ist die IP-Adresse des APs, durch welchen der Benutzer sich registrieren lässt. Dies ist ein herstellerspezifisches Attribut.
9. AP-MAC-Address. Dies ist die MAC-Adresse des APs, durch welchen der Benutzer sich registrieren lässt. Dies ist ein herstellerspezifisches Attribut.
10. End systems Registration Request. Die Registrierungsaufforderung vom Endsystem wird unverändert in dieses herstellerspezifische Attribut kopiert.

[0165] Die folgenden Attribute werden vom Registrierungsserver im Radius Access-Response- oder Radius-Zugangsantwort-Paket an den FA gesendet:

1. Service Type. Dies ist ein gerahmter Dienst.
2. Framed-Protocol. Dies ist ein PPP.
3. XTunnel Protocol Parameters. Diese Parameter werden durch den Registrierungsserver gesendet, um die Parameter zu spezifizieren, die zum Aufbau des XTunnel-Protokolls für das Endsystem notwendig sind. Dies ist ein herstellerspezifisches Attribut.
4. Home Registration Servers Registration Reply. Dieses Attribut wird vom Heimatregistrierungsserver an den FA gesendet. Der FA leitet dieses Attribut in einem Registrierungsantwortpaket unverändert an das Endsystem weiter. Wenn es einen fremden Registrierungsserver auf dem Weg gibt, wird dieses Attribut durch ihn unverändert an den FA weitergeleitet. Es wird als ein herstellerspezifisches Attribut codiert.

[0166] Um Gast-Endsysteme zu versorgen, werden das Fremdnetz und das Heimatnetz unter Verwendung des Radius-Protokolls zur Authentifizierung und Konfiguration untereinander für Abrechnungs- und Gebührenverrechnungszwecke authentifiziert. Diese Authentifizierung wird zum Zeitpunkt der Endsystemregistrierung durchgeführt. Wie bereits erwähnt, verwendet der Registrierungsserver im Fremdnetz, wenn er eine Registrierungsaufforderung von einem Endsystem empfängt (eingekapselt als ein herstellerspezifisches Attribut in einem Radius Access Request-Paket durch den FA), den User-Name des Endsystems, um die Identität des Heimatregistrierungsservers des Endsystems durch Konsultieren seines Heimatdomänenverzeichnisses HDD zu

bestimmen. Die folgenden Informationen sind im Heimatdomänenverzeichnis HDD gespeichert, und auf sie greift der fremde Registrierungsserver zu, um die Registrierungsaufforderung des Endsystems weiterzuleiten:

1. Home Registration Server IP Address. Dies ist die IP-Adresse des Heimatregistrierungsservers, um die Registrierungsaufforderung zu übermitteln.
2. Foreign Registration Server Machine Id. Dies ist Maschinen-ID des fremden Registrierungsservers im vereinfachten E-Mail-Übertragungsprotokoll- oder SMTP-Format (für engl. simplified mail transfer protocol) (z.B. machine@fgdn, wobei machine der Name der fremden Registrierungsservermaschine und fgdn der voll qualifizierte Domänenname der Domäne des fremden Registrierungsservers ist).
3. Tunneling Protocol Parameters. Dies sind Parameter zum Konfigurieren des Tunnels zwischen der versorgenden IWF und der Heimat-IWF für das Endsystem. Diese umfassen das Tunnelprotokoll, das zwischen ihnen zu verwendet ist, und die Parameter zum Konfigurieren des Tunnels.
4. Shared Secret. Dies ist der gemeinsam benutzte Geheimcode, der zur Authentifizierung zwischen dem fremden Registrierungsserver und dem Heimatregistrierungsserver zu verwenden ist. Dieser Geheimcode wird zum Errechnen des Radius User-Password-Attributs im Radius-Paket verwendet, das durch den fremden Registrierungsserver an den Heimatregistrierungsserver gesendet wird. Er wird zwischen den beiden Drahtlosdiensteanbietern definiert.
5. User-Password. Dies ist das Benutzerpasswort, das für das Gast-Endsystem zu verwenden ist. Dieses Benutzerpasswort wird zwischen den beiden Drahtlosdiensteanbietern definiert. Dieses Passwort wird unter Verwendung des gemeinsam benutzten Geheimcodes, wie im Radius RFC beschrieben, verschlüsselt.
6. Accounting Parameters. Dies sind Parameter zum Konfigurieren der Abrechnung für das Endsystem, das sich registrieren lässt. Diese Parameter werden durch den Registrierungsserver zum Konfigurieren der Abrechnung für das Endsystem an seine IWF gesendet.

[0167] Durch Verwenden dieser Informationen erzeugt der fremde Registrierungsserver eine Radius Access-Request, fügt seine eigenen Registrierungs- und Authentifizierungsinformationen in die Radius Access-Request hinzu, kopiert die Registrierungsinformationen, die durch das Endsystem gesendet wurden, unverändert in die Radius Access-Request und sendet die verknüpfte Anforderung an den Heimatregistrierungsserver.

[0168] Nach Empfang der Radius Access-Request vom fremden Registrierungsserver (für ein Gast-Endsystem) oder direkt vom FA (für ein Endsystem zu Hause) befragt der Heimatregistrierungsserver seinen eigenen Verzeichnisserver nach den gemeinsam benutzten Geheimcodes, um die Identität des Endsystems und die Identität des fremden Registrierungsservers in einem Roaming-Szenarium durch Neuerrechnen von Identitätsmarken zu überprüfen.

[0169] Nach einer erfolgreichen Verarbeitung der Anforderung erzeugt der Heimatregistrierungsserver ein Radius Access-Accept- oder Radius-Zugangsgenehmigungs-Antwortpaket und sendet es an den fremden Registrierungsserver, wenn das Endsystem wandert, oder direkt zum FA, von welchem er die Radius Access-Request empfing. Die Antwort enthält das Registrierungsantwortattribut, das der FA an das Endsystem weiterleitet.

[0170] Wenn die Anforderung nicht erfolgreich verarbeitet werden kann, erzeugt der Heimatregistrierungsserver ein Radius Access-Reject- oder Radius-Zugangsverweigerungs-Antwortpaket und sendet es an den fremden Registrierungsserver, wenn das Endsystem wandert, oder direkt an den FA, von welchem er die Radius Access-Request empfing. Die Antwort enthält das Registrierungsantwortattribut, das der FA an das Endsystem weiterleitet.

[0171] In einem Roaming-Szenarium wird die Antwort vom Heimatregistrierungsserver durch den fremden Registrierungsserver empfangen. Sie wird durch den fremden Registrierungsserver unter Verwendung des gemeinsam benutzten Geheimcodes authentifiziert. Nach der Authentifizierung verarbeitet der fremde Registrierungsserver die Antwort und erzeugt seinerseits ein Radius-Antwortpaket (Accept oder Reject) zum Versand an den FA. Der fremde Registrierungsserver kopiert das Registrierungsantwortattribut aus dem Radius-Zugangsantwortpaket des Heimatregistrierungsservers unverändert in sein Radius-Antwortpaket. Wenn der FA das Radius Access-Response- oder Radius Access-Reject-Antwortpaket empfängt, erzeugt er unter Verwendung der Registrierungsantwortattribute aus der Radius-Antwort ein Registrierungsantwortpaket und sendet die Antwort an das Endsystem, wodurch die Registrierungsumlauffolge abgeschlossen ist.

[0172] Die Mobile-IP-Standards spezifizieren, dass ein Wiederholungsschutz für Registrierungen implementiert wird, wobei Zeitstempel oder optional Nonces verwendet werden. Da jedoch ein Wiederholungsschutz, der Zeitstempel verwendet, angemessen synchronisierte Tageszeittakte zwischen den entsprechenden Knoten er-

fordert, implementiert die vorliegende Erfindung einen Wiederholungsschutz während der Registrierung unter Verwendung von Nonces, auch wenn ein Wiederholungsschutz, der Zeitstempel verwendet, in den Mobile-IP-Standards vorgeschrieben ist und die Verwendung von Nonces optional ist. Es ist jedoch ein Wiederholungsschutz, der Zeitstempel verwendet, als eine alternative Ausführungsform vorgesehen.

[0173] Das Wiederholungsschutzformat, das zwischen Knoten verwendet wird, wird zusätzlich zu Authentifizierungskontext, Modus, Geheimcode und Verschlüsselungsart im Sicherheitskontext gespeichert.

[0174] Das Netz unterstützt die Verwendung von PPP-PAP (Passwort-Authentifizierung) und -CHAP (abfrageauthentifiziertes Passwort) zwischen dem Endsystem und seinem PPP-Server. Dies erfolgt unabhängig von den zuvor beschriebenen Registrierungs- und Authentifizierungsmechanismen. Dies ermöglicht es einem privaten Intranet oder einem ISP, die Identität des Benutzers zu überprüfen.

[0175] Eine Authentifizierung für Abrechnungs- und Verzeichnisdienste wird im Folgenden in Bezug auf die Abrechnungssicherheit beschrieben. Der Zugang zu Verzeichnisservern von Netzbetriebsmitteln in derselben MSC braucht nicht authentifiziert zu werden.

[0176] Das Netz unterstützt die Verschlüsselung von Trägerdaten, die zwischen dem Endsystem und der Heimat-IWF gesendet werden. Die Endsysteme handeln durch Auswählen des geeigneten Sicherheitskontextes aus, ob eine Verschlüsselung ein oder aus sein soll. Nach Empfang der Registrierungsaufforderung bewilligt der Heimatregistrierungsserver des Endsystems Anforderung einer Verschlüsselung basierend auf dem Sicherheitskontext. Neben dem Speichern von Authentifizierungsalgorithmus, Modus, gemeinsam benutztem Code und Wiederholungsschutzformat wird der Sicherheitskontext auch verwendet, um das zu verwendende Format des Verschlüsselungsalgorithmus zu spezifizieren. Wenn die Verschlüsselung zwischen dem Endsystem und dem Heimatagenten ausgehandelt wird, dann wird der gesamte PPP-Rahmen vor der Kapselung im RLP so verschlüsselt.

[0177] Die IWF, der Abrechnungsserver und das Gebührenverrechnungssystem sind Teil derselben zuverlässigen Domäne in der MSC. Diese Entitäten sind entweder an dasselbe LAN angeschlossen oder Teil eines zuverlässigen Intranets, das dem Drahtlosdiensteanbieter gehört und von ihm betrieben wird. Die Übertragung von Abrechnungsstatistiken zwischen der IWF und dem Abrechnungsserver und zwischen dem Abrechnungsserver und dem Kundengebührenverrechnungssystem brauchen nicht unter Verwendung von Internet-IP-Sicherheitsprotokollen wie IP-Sec verschlüsselt zu werden.

[0178] Das Netz macht es schwieriger, den Aufenthaltsort des Endsystems zu überwachen, da es scheint, dass alle PPP-Rahmen, die vom und zum Endsystem gehen, ungeachtet des tatsächlichen Aufenthaltsorts des Endsystemgeräts durch die Heimat-IWF gehen.

[0179] Die Abrechnungsdaten werden durch die versorgende IWF und die Heimat-IWF im Netz gesammelt. Abrechnungsdaten, die durch die versorgende IWF gesammelt werden, werden an einen Abrechnungsserver in der MSC der versorgenden IWF gesendet. Abrechnungsdaten, die durch die Heimat-IWF gesammelt werden, an einen Abrechnungsserver in der MSC der Heimat-IWF gesendet. Die Abrechnungsdaten, die durch die versorgende IWF gesammelt werden, werden durch den fremden Drahtlosdiensteanbieter zur Rechnungsprüfung und zur Zahlung von Rechnungen über Drahtlosdienteanbietergrenzen verwendet (um Roaming und Mobilität zu unterstützen). Die Abrechnungsdaten, die durch die Heimat-IWF gesammelt werden, werden zur Vergebührung des Endbenutzers und auch zur Zahlung über Drahtlosdiensteanbietergrenzen verwendet, um Roaming und Mobilität abzuwickeln.

[0180] Da ungeachtet des Aufenthaltsorts des Endsystems und des Aufenthaltsorts des fremden Agenten der gesamte Datenverkehr durch die Heimat-IWF fließt, hat die Heimat-IWF alle Informationen zur Erstellung von Rechnungen für den Kunden und auch Zahlungsinformationen zur Verwendung von Fremdnetzen.

[0181] Die versorgende IWF und die Heimat-IWF verwenden vorzugsweise das Radius-Abrechnungsprotokoll zum Senden von Abrechnungssätzen für registrierte Endsysteme. Das Radius-Abrechnungsprotokoll ist so, wie in einem IETF RFC-Entwurf dokumentiert. Für die vorliegende Erfindung muss das Protokoll durch Hinzufügen von herstellerspezifischen Attributen für das Netz und durch Hinzufügen einer Kontrollpunktmarkierung zum Radius-Accounting-Protokoll erweitert werden. Kontrollpunktmarkierung in diesem Kontext bezieht sich auf das regelmäßige Aktualisieren von Abrechnungsdaten, um das Risiko eines Verlusts von Abrechnungssätzen zu minimieren.

[0182] Das Radius-Abrechnungsprotokoll läuft über UDP/IP und verwendet Wiederholungsversuche auf der Basis von Bestätigung und Zeitüberschreitungen. Die Radius-Abrechnungsclients (versorgende IWFs oder Heimat-IWFs) sendet UDP-Abrechnungsanforderungspakete an ihre Abrechnungsserver, welche Bestätigungen an die Abrechnungsclients zurücksenden.

[0183] Im Netz geben die Abrechnungsclients (die versorgende IWF und die Heimat-IWF) eine Abrechnungsstartanzeige am Beginn der Sitzung des Benutzers und eine Abrechnungsstoppanzeige am Ende der Sitzung des Benutzers aus. In der Mitte der Sitzung geben die Abrechnungsclients Abrechnungskontrollpunktanzeigen aus. Im Gegensatz dazu spezifiziert die Radius-Abrechnungs-RFC keine Abrechnungskontrollpunktanzeige. Die Software der vorliegenden Erfindung erzeugt ein herstellerspezifisches Abrechnungsattribut zu diesem Zweck. Dieses Abrechnungsattribut ist in allen Radius Accounting-Request- oder Radius-Abrechnungsanforderungs-Paketen vorhanden, welche einen Acct-Status-Type von Start (Abrechnungsstartanzeigen) aufweisen. Der Wert dieses Attributs wird verwendet, um an den Abrechnungsserver zu übertragen, ob der Abrechnungssatz ein Kontrollpunktsatz ist oder nicht. Kontrollpunktabrechnungssätze weisen ein Zeitattribut auf und enthalten kumulative Abrechnungsdaten vom Start der Sitzung. Die Häufigkeit des Übertragens von Kontrollpunktpaketen ist in der vorliegenden Erfindung konfigurierbar.

[0184] Die versorgende IWF und die Heimat-IWF werden durch ihre jeweiligen Registrierungsserver zur Verbindung mit ihren Abrechnungsservern während der Registrierungsphase konfiguriert. Die konfigurierbaren Abrechnungsparameter umfassen die IP-Adresse und den UDP-Port des Abrechnungsservers, die Häufigkeit der Kontrollpunktmarkierung, die Sitzungs-/Mehrfachsitzungs-ID und den gemeinsam benutzten Geheimcode, der zwischen dem Abrechnungsclient und dem Abrechnungsserver zu verwenden ist.

[0185] Das Netz zeichnet die folgenden Abrechnungsattribute für jedes registrierte Endsystem auf. Diese Abrechnungsattribute werden durch die Abrechnungsclients in Radius-Abrechnungspaketen am Beginn der Sitzung, am Ende der Sitzung und in der Mitte (Kontrollpunkt) ihren Abrechnungsservern gemeldet.

1. User-Name. Dieses Attribut ist wie das zuvor erörterte Radius User-Name-Attribut. Dieses Attribut wird verwendet, um den Benutzer zu identifizieren und ist in allen Abrechnungsberichten vorhanden. Das Format ist „user@domain", wobei domain der voll qualifizierte Domänenname der Heimat des Benutzers ist.
2. NAS-IP-Address. Dieses Attribut ist wie das zuvor erörterte Radius NAS-IP-Address-Attribut. Dieses Asttribut wird verwendet, um die IP-Adresse der Maschine zu identifizieren, welche die Heimat-IWF oder die versorgende IWF ausführt.
3. Radio Port. Dieses Attribut identifiziert den Funkanschluss auf dem Zugangspunkt, der den Benutzer versorgt. Dieses Attribut wird als ein herstellerspezifisches Attribut codiert.
4. Access Point IP Address. Dieses Attribut identifiziert die IP-Adresse des Zugangspunkts, der den Benutzer versorgt. Dieses Attribut wird als ein herstellerspezifisches Attribut codiert.
5. Service Type. Dieses Attribut ist wie das zuvor beschriebene Radius Service-Type-Attribut. Der Wert dieses Attributs ist Framed (gerahmt).
6. Framed Protocol. Dieses Attribut ist wie das zuvor beschriebene Radius Framed-Protocol-Attribut. Der Wert dieses Attributs ist so eingestellt, dass er PPP anzeigt.
7. Accounting Status Type. Dieses Attribut ist wie das zuvor beschriebene Radius Acct-Status-Type-Attribut. Der Wert dieses Attributs kann Start sein, um den Start einer Sitzung des Benutzers mit dem Radius-Client zu markieren, und es kann Stopp sein, um das Ende der Sitzung des Benutzers mit dem Radius-Client zu markieren. Für Abrechnungsclients wird das Acct-Status-Type/Start-Attribut erzeugt, wenn das Endsystem sich registrieren lässt. Das Acct-Status-Type/Stopp-Attribut wird erzeugt, wenn das Endsystem sich aus irgendeinem Grund aus dem Register löschen lässt. Für Kontrollpunkte ist der Wert dieses Attributs ebenfalls Start, und das Accounting Checkpoint- oder Abrechnungskontrollpunkt-Attribut ist ebenfalls vorhanden.
8. Accounting Session Id. Diese ist wie die zuvor beschriebene Radius Acct-Session-ID. In einem Roaming-Szenarium wird diese Sitzungs-ID durch den fremden Registrierungsserver zugeordnet, wenn das Endsystem eine Registrierungsaufforderung ausgibt. Sie wir während der Registrierungsfolge durch den fremden Registrierungsserver an Heimatregistrierungsserver übertragen. Das Heimatnetz und das Fremdnetz kennen beide das Acct-Session-ID-Attribut und sind imstande, dieses Attribut auszugeben, während sie Abrechnungssätze an ihre jeweiligen Abrechnungsserver senden. In einem „Endsystem-zu-Hause"-Szenarium wird dieses Attribut durch den Heimatregistrierungsserver erzeugt. Der Registrierungsserver kommuniziert den Wert dieses Attributs der IWF, welche ihn in allen Abrechnungssätzen ausgibt.
9. Accounting Multi-Session-Id. Diese ist wie die zuvor erörterte Radius Acct-Multi-Session-ID. Diese ID wird durch den Heimatregistrierungsserver zugeordnet, wenn eine Registrierungsaufforderung von einem FA direkt oder über einen fremden Registrierungsserver für ein Endsystem empfangen wird. Sie wird durch den Heimatregistrierungsserver in der Registrierungsantwortnachricht an den fremden Registrierungsser-

ver übertragen. Der oder die Registrierungsserver kommunizieren den Wert dieses Attributs der oder den IWF(s), welche ihn in allen Abrechnungssätzen ausgeben.

[0186] Bei einer zuverlässigen Mobilität, die der Architektur hinzugefügt wird, wird die ID verwendet, um die Abrechnungssätze von verschiedenen IWFs für dasselbe Endsystem miteinander in Beziehung zu bringen, wenn das Endsystem sich von einer IWF zu einer anderen bewegt. Für Weiterschaltungen über IWF-Grenzen ist die Acct-Session-ID oder Abrechnungssitzungs-ID verschieden für Abrechnungssätze, die von verschiedenen IWFs stammen. Das Acct-Multi-Session-ID- oder Mehrfach-Abrechnungssitzungs-ID-Attribut ist jedoch dasselbe für alle Abrechnungssätze, die von allen IWFs ausgegeben wurden, die den Benutzer versorgten. Da die Sitzungs-ID und die Mehrfachsitzungs-ID sowohl dem Fremdnetz als auch dem Heimatnetz bekannt sind, sind sie imstande, diese Attribute in Abrechnungsberichten an ihre jeweiligen Abrechnungsserver auszugeben. Mit der Sitzungs-ID und der Mehrfachsitzungs-ID sind Gebührenverrechnungssysteme imstande, Abrechnungssätze über IWF-Grenzen im selben Drahtlosdiensteanbieter und sogar über Drahtlosdiensteanbietergrenzen zu korrelieren.

1. Accounting Delay Time (Abrechnungsverzögerungszeit). Siehe Radius Acct-Delay-Time-Attribut.

2-. Accounting Input Octets. Siehe Radius Acct-Input-Octets. Dieses Attribut wird verwendet, um die Anzahl von Oktetten im Auge zu behalten, die durch das Endsystem gesendet werden (eingegeben ins Netz vom Endsystem). Diese Zählung wird verwendet, um nur die PPP-Rahmen zu verfolgen. Die Luftverbindungszusatzaufwand oder irgendein Zusatzaufwand, der durch RLP usw. eingeführt wird, wird nicht gezählt.

3. Accounting Output Octets. Siehe Radius Acct-Output-Octets. Dieses Attribut wird verwendet, um die Anzahl von Oktetten im Auge zu behalten, die an das Endsystem gesendet werden (ausgegeben vom Netz zum Endsystem). Diese Zählung wird verwendet, um nur die PPP-Rahmen zu verfolgen. Der Luftverbindungszusatzaufwand oder irgendein Zusatzaufwand, der durch RLP usw. eingeführt wird, wird nicht gezählt.

4. Accounting Authentic (Abrechnung authentisch). Siehe Radius Acct-Authentic-Attribut. Der Wert dieses Attributs ist in Abhängigkeit davon, ob die versorgende IWF oder die Heimat-IWF den Abrechnungssatz erzeugt, Local oder Remote (abgesetzt).

5. Accounting Session Time. Siehe Radius Acct-Session-Time-Attribut. Dieses Attribut zeigt die Dauer von Zeit an, die der Benutzer versorgt wurde. Wenn durch die versorgende IWF gesendet, verfolgt dieses Attribut die Zeitdauer, die der Benutzer von der versorgenden IWF versorgt wurde. Wenn durch die Heimat-IWF gesendet, verfolgt dieses Attribut die Zeitdauer, die der Benutzer von der Heimat-IWF versorgt wurde.

6. Accounting Input Packets. Siehe Radius Acct-Input-Packets-Attribut. Dieses Attribut zeigt die Anzahl von Paketen an, die vom Endsystem empfangen werden. Für eine versorgende IWF verfolgt dieses Attribut die Anzahl von PPP-Rahmen, die von einem Endsystem in die versorgende IWF eingegeben werden. Für eine Heimat-IWF verfolgt dieses Attribut die Anzahl von PPP-Rahen, die von einem Endsystem in die Heimat-IWF eingegeben werden.

7. Accounting Output Packets. Siehe Radius Acct-Output-Packets-Attribut. Dieses Attribut zeigt die Anzahl von Paketen an, die an das Endsystem gesendet werden. Für eine versorgende IWF verfolgt dieses Attribut die Anzahl von PPP-Rahmen, die von einer versorgenden IWF an ein Endsystem ausgegeben werden. Für eine Heimat-IWF verfolgt dieses Attribut die Anzahl von PPP-Rahen, die von einer Heimat-IWF an ein Endsystem ausgegeben werden.

8. Accounting Terminate Cause. Siehe Radius Acct-Terminate-Cause-Attribut. Dieses Attribut gibt die Ursache dafür an, warum eine Benutzersitzung beendet wurde. Außerdem ist ein spezifischer Ursachencode vorhanden, um zusätzliche Details bereitzustellen. Dieses Attribut ist nur in Abrechnungsberichten am Ende der Sitzung vorhanden.

9. Network Accounting Terminate Cause. Dieses Attribut gibt die Ursache für die Beendigung einer Sitzung detailliert an. Dieses spezifische Attribut wird als ein herstellerspezifisches Attribut codiert und wird nur in einem Radius Accounting-Attribut am Ende der Sitzung gemeldet. Das Radius-Standardattribut Acct-Terminat-Cause ist ebenfalls vorhanden. Dieses Attribut stellt spezifische Ursachencodes bereit, die durch das Acct-Terminate-Cause-Attribut nicht gedeckt werden.

10. Network Air Link Access Protocol. Dieses Attribut gibt das Luftverbindungszugangsprotokoll an, das vom Endsystem verwendet wird. Dieses Attribut wird als herstellerspezifisches Attribut codiert.

11. Network Backhaul Access Protocol. Dieses Attribut gibt das Backhaul-Zugangsprotokoll an, das vom Zugangspunkt verwendet wird, um Daten zum und vom Endsystem zu übertragen. Dieses Attribut wird im herstellerspezifischen Format codiert.

12. Network Agent Machine Name. Dieses Attribut ist der voll qualifizierte Domänenname der Maschine, welche die Heimat-IWF oder die versorgende IWF ausführt. Dieses spezifische Attribut wird im herstellerspezifischen Format codiert.

13. Network Accounting Check-point. Da die Radius-Abrechnungs-RFC kein Kontrollpunktpaket definiert, verwendet die vorliegende Erfindung ein Radius-Abrechnungsstartpaket mit diesem Attribut, um einen Kon-

trollpunkt zu markieren. Das Nichtvorhandensein dieses Attributs bedeutet ein herkömmliches Abrechnungsstartpaket. Das Vorhandensein dieses Attributs in einem Abrechnungsstartpaket bedeutet ein Abrechnungskontrollpunktpaket. Abrechnungsstopppakete weisen dieses Attribut nicht auf.

[0187] In einer bevorzugten Ausführungsform müssen jedes Abrechnungspaket und die entsprechende Antwort unter Verwendung des MD5 und eines gemeinsam benutzten Geheimcodes authentifiziert werden. Die IWFs sind mit einem gemeinsam benutzten Geheimcode konfiguriert, der von ihnen während der Kommunikation mit ihrem Radius-Abrechnungsserver zur Authentifizierung verwendet wird. Die gemeinsam benutzten Geheimcodes, die von den IWFs zum Kommunizieren mit ihren Abrechnungsservern verwendet werden, sind im Heimat/Fremddomänenverzeichnis gespeichert, das sich in der MSC befindet. Die gemeinsam benutzten Geheimcodes für Abrechnungssicherheit werden den IWFs durch ihre Registrierungsserver während der Endsystemregistrierungsfolge kommuniziert.

[0188] Die Abrechnungsserversoftware läuft in einem Computer, der sich in der MSC befindet. Die Funktion des Abrechnungsservers im System ist es, Rohabrechnungsdaten von den Netzelementen (den Heimat- und versorgenden IWFs) zu sammeln, die Daten zu verarbeiten und sie zur Übertragung an das Gebührenverrechnungssystem des Drahtlosdiensteanbieters zu speichern. Der Abrechnungsserver weist kein Gebührenverrechnungssystem auf. Stattdessen weist er eine Unterstützung für einen automatischen oder manuellen Abrechnungsdatenübertragungsmechanismus auf. Bei Verwenden des automatischen Abrechnungsdatenübertragungsmechanismus überträgt der Abrechnungsserver Abrechnungssätze in einem AMA-Rechnungsformat über eine TCP/IP-Übertragung an das Kundengebührenverrechnungssystem. Zu diesem Zweck definiert das System AMA-Rechnungsprotokollformate für Paketdaten. Bei Verwenden des manuellen Übertragungsmechanismus sind Kunden imstande, ein Band zu bilden, um Abrechnungssätze an ihr Gebührenverrechnungssystem zu übertragen. Um das Band zu ihren Spezifikationen zu bilden, werden die Kunden mit Informationen versehen, um auf Abrechnungssätze zuzugreifen, damit sie sie verarbeiten können, bevor sie sie aufs Band schreiben.

[0189] In Fig. 25 werden die Rohabrechnungsdaten, die durch den Abrechnungsserver von den Heimat- oder versorgenden IWFs empfangen werden, verarbeitet und durch den Abrechnungsserver gespeichert. Die Verarbeitung, die durch den Abrechnungsserver erfolgt, umfasst Filterung, Kompression und Korrelation der Rohabrechnungsdaten, die von der IWF empfangen werden. Ein hochverfügbarer Dateiserver, der Aktiv/In-Bereitschaft-Doppelprozessoren und austauschbare RAID-Platten verwendet, wird zum Puffern der Abrechnungsdaten verwendet, während sie den Abrechnungsserver durchqueren.

[0190] Der Abrechnungsserver verzögert die Verarbeitung der Rohabrechnungsdaten, bis ein Endsystem seine Sitzung beendet hat. Wenn ein Endsystem seine Sitzung beendet, verarbeitet der Abrechnungsserver die Rohabrechnungsdaten, die er für die Sitzung gesammelt hat und speichert einen Abrechnungsauszugssatz in einer SQL-Datenbank. Der Abrechnungsauszugssatz, der in der SQL-Datenbank gespeichert ist, zeigt auf eine ASN.1-codierte Datei. Diese Datei enthält detaillierte Abrechnungsinformationen über die Sitzung des Endsystems. Die Daten, die im Abrechnungsserver gespeichert sind, werden dann durch den Rechnungsdatenübertragungsagenten an das Kundengebührenverrechnungssystem übertragen. Alternativerweise kann der Drahtlosdiensteanbieter die Abrechnungsdaten von der SQL-Datenbank und/oder der ASN.1-codierten Datei über ein Band an das Gebührenverrechnungssystem übertragen. Das Datenbankschema und das Format der ASN.1-codierten Datei werden dokumentiert und den Kunden für diesen Zweck zugänglich gemacht. Wenn das Volumen von verarbeiteten Abrechnungsdaten, die im Abrechnungssystem gespeichert sind, eine Hochwassermarke überschreitet, erzeugt der Abrechnungsserver einen NMS-Alarm. Dieser Alarm wird aufgehoben, wenn das Volumen von Daten, die im Abrechnungsserver gespeichert sind, unter eine Niedrigwassermarke fällt. Die Hoch- und die Niedrigwassermarke zum Erzeugen und Aufheben des Alarm sind konfigurierbar. Der Abrechnungsserver erzeugt einen NMS-Alarm auch, wenn das Alter der gespeicherten Abrechnungsdaten eine konfigurierbare Schwelle überschreitet. Umgekehrt wird der Alarm aufgehoben, wenn das Alter der Abrechnungsdaten unter die Schwelle fällt.

[0191] Das Teilnehmerverzeichnis wird verwendet, um Informationen über Teilnehmer zu speichern und befindet sich im Heimatnetz. Der Heimatregistrierungsserver konsultiert dieses Verzeichnis während der Registrierungsphase, um ein Endsystem zu authentifizieren und zu registrieren. Für jeden Teilnehmer speichert das Teilnehmerverzeichnis die folgenden Informationen:

1. User-Name (Benutzer-Name). Dieses Feld im Teilnehmerdatensatz ist im SMTP-Format (z.B. user@fgdn), wobei das user-Teilfeld den Teilnehmer in seiner drahtlosen Heimatdomäne und das fgdn-Teilfeld die drahtlose Heimatdomäne des Teilnehmers identifiziert. Dieses Feld wird durch das Endsystem in der Registrierungsaufforderung während der Registrierungsphase gesendet. Dieses Feld wird durch den

Drahtlosdiensteanbieter dem Teilnehmer zum Zeitpunkt der Antragstellung für den Netzdienst zugeordnet. Dieses Feld unterscheidet sich von dem Benutzernamenfeld, das im PPP verwendet wird.

2. Mobility Security Association. Dieses Feld im Teilnehmerdatensatz enthält die Mobilitätssicherheitsvereinbarung zwischen dem Teilnehmer und seinem Heimatnetz. Wie bereits erwähnt, besteht eine Mobilitätssicherheitsvereinbarung zwischen jedem Teilnehmer und seinem Heimatregistrierungsserver. Die Mobilitätssicherheitsvereinbarung definiert eine Sammlung von Sicherheitskontexten. Jeder Sicherheitskontext definiert einen Authentifizierungsalgorithmus, einen Authentifizierungsmodus, einen gemeinsam benutzten Geheimcode, ein Wiederholungsschutzformat und eine Verschlüsselungsart (einschließlich ohne Verschlüsselung) zur Verwendung zwischen dem Endsystem und seinem Heimatserver. Während der Registrierung ruft der Heimatregistrierungsserver unter Verwendung des User-Name und des Sicherheitsparameterindexes (SPI), die durch den Endsystem in seiner Registrierungsaufforderung geliefert werden, Informationen über den Sicherheitskontext des Teilnehmers aus dem Teilnehmerverzeichnis ab. Die Informationen im Sicherheitskontext werden zum Erzwingen von Authentifizierung, Verschlüsselung und Wiederholungsschutz während der Sitzung verwendet. Die Mobilitätssicherheitsvereinbarung wird durch den Drahtlosdiensteanbieter zum Zeitpunkt der Antragstellung erzeugt. Es liegt am Drahtlosdiensteanbieter, ob er es dem Teilnehmer entweder durch einen Anruf bei einem Kundendienstrepräsentanten oder, indem er die Teilnehmer auf eine sichere Web-Site zugreifen lässt, gestattet, diese Vereinbarung zu modifizieren. Die Web-Site-Software exportiert Webseiten, welche der Drahtlosdiensteanbieter von einem sicheren Webserver für die Teilnehmer zugänglich macht. Auf diese Weise sind Teilnehmer imstande, neben anderen Teilnehmerinformationen, die der Diensteanbeiter möglicherweise zugänglich macht, auch die Inhalte der Mobilitätssicherheitsvereinbarung einzusehen/zu modifizieren.

3. Modem MAC Address. Dieses Feld enthält die MAC-Adresse des Modems, das dem Teilnehmer gehört. Zusätzlich zum gemeinsam benutzten Geheimcode wird dieses Feld während der Registrierung verwendet, um den Benutzer zu identifizieren. Es ist möglich, eine MAC-Adressen-basierte Authentifizierung auf einer Pro-Benutzer-Basis auszuschalten. Die MAC-Adresse wird dem Heimatregistrierungsserver während der Registrierung kommuniziert.

4. Enable MAC Address Authentication (MAC-Adressen-Authentifizierung Freigeben). Dieses Feld wird verwendet, um festzustellen, ob die MAC-Adressen-basierte Authentifizierung enabled (freigegeben) oder disabled (gesperrt) ist. Wenn enabled, dann überprüft der Heimatregistrierungsserver die MAC-Adresse des zu registrierenden Endsystems mit diesem Feld, um die Identität des Endsystems zu bestätigen. Wenn disabled, dann erfolgt keine Überprüfung.

5. Roaming Enabled Flag (Roaming-Freigegeben-Flagge). Wenn dieses Feld auf enabled gesetzt ist, dann darf das Endsystem zu Fremdnetzen wandern. Wenn dieses Feld disabled ist, dann darf das System nicht zu Fremdnetzen wandern.

6. Roaming Domain List (Roaming-Domänenliste). Dieses Feld ist nur von Bedeutung, wenn das Roaming Enabled Flag auf enabled gesetzt ist. Dieses Feld enthält eine Liste von fremden Domänen, in die das Endsystem wandern darf. Wenn der Inhalt dieser Liste null ist und die Roaming Enabled Flag auf enabled gesetzt ist, darf das Endsystem frei wandern.

7. Service Enable/Disable Flag (Dienst-Freigeben/Sperren-Flagge). Dieses Feld kann durch den Systemadministrator auf disable gesetzt werden, um einen Dienst für einen Teilnehmer zu sperren. Wenn dieses Feld gesperrt ist, dann darf der Teilnehmer sich für den Dienst registrieren lassen. Wenn der Teilnehmer registriert ist und der Wert dieses Feldes auf gesperrt gesetzt ist, dann wird das Endsystem des Teilnehmers durch das Netz unverzüglich getrennt.

8. Internet Service Provider Association (Internetdiensteanbietervereinbarung). Dieses Feld enthält Informationen über den Internetdiensteanbieter des Teilnehmers. Diese Informationen werden durch die IWF während der PPP-Registrierungsphase verwendet, um eine Authentifizierung mit dem Internetdiensteanbieter für das Endsystem durchzuführen, und auch, um einen L2TP-Tunnel zwischen der IWF und dem PPP-Server des Internetdiensteanbieters zu erzeugen. Das Feld enthält die Identität des ISPs des Teilnehmers. Die IWF verwendet diese Informationen, um zum Durchführen der Authentifizierung und des Aufbaus des L2TP-Tiunnels für das Endsystem auf das ISP-Verzeichnis zuzugreifen.

9. Subscriber's Name & Address Information. Dieses Feld enthält Name, Adresse, Telefonnummer, Faxnummer, E-Mail-Adresse usw. des Teilnehmers.

[0192] Das Heimatdomänenverzeichnis (HDD) wird durch den Registrierungsserver verwendet, um Parameter über das Endsystem abzurufen, um die Registrierung für das Endsystem abzuschließen. Durch Verwenden dieser Informationen bestimmt der Registrierungsserver, ob das Endsystem sich zu Hause registrieren lässt oder ob das Endsystem ein Gast-Endsystem ist. Im ersteren Fall übernimmt der Registrierungsserver die Funktion eines Heimatregistrierungsservers und verfährt mit der Endsystemregistrierung. Im letzteren Fall übernimmt der Registrierungsserver die Funktion eines fremden Registrierungsservers und leitet als Radius-Proxy agierend die Aufforderung zum echten Heimatregistrierungsserver, dessen Identität er aus diesem

Verzeichnis erhält. Für ein Gast-Endsystem umfassen die Parameter, die im HDD gespeichert sind, die IP-Adresse des Heimatregistrierungsservers, den heimat-fremdseitig gemeinsam benutzten Geheimcode, die Konfiguration des Tunnels zwischen Heimat- und versorgender IWF usw. Das HDD befindet sich in der MSC.

[0193] Die folgenden Informationen sind im HDD gespeichert:

1. Home Domain Name (Heimatdomänenname). Dieses Feld wird als Schlüssel beim Absuchen des HDDs nach einem Eintrag verwendet, der mit dem voll qualifizierten Heimatdomänennamen übereinstimmt, der durch das Endsystem in seiner Registrierungsaufforderung geliefert wird.
2. Proxy Registration Request (Proxy-Registrierungsaufforderung). Dieses Feld wird durch den Registrierungsserver verwendet, um festzustellen, ob er als ein fremder Registrierungsserver agieren und die Registrierungsaufforderung des Endsystems zum echten Heimatregistrierungsserver durchreichen soll.
3. Home Registration Server DNS Name (DNS-Name des Heimatregistrierungsservers). Wenn die Proxy-Registrierungsaufforderungs-Flagge auf TRUE (wahr) ist, dann wird dieses Feld verwendet, um auf den DNS-Namen des Heimatregistrierungsservers zuzugreifen. Andernfalls wird dieses Feld ignoriert. Der DNS-Name wird durch den fremden Registrierungsserver in eine IP-Adresse übersetzt. Der fremde Registrierungsserver verwendet die IP-Adresse, um die Registrierungsaufforderung des Endsystems weiterzuleiten.
4. Foreign Domain Name (Fremder Domänenname). Wenn die Proxy-Registrierungsaufforderungs-Flagge auf TRUE (wahr) ist, dann wird dieses Feld verwendet, um den fremden Domänennamen für den Heimatregistrierungsserver des Endsystems zu identifizieren. Andernfalls wird dieses Feld ignoriert. Der fremde Registrierungsserver verwendet diese Informationen, um die Maschinen-ID des fremden Servers im SMTP-Format, zum Beispiel machine@fgdn, zu erzeugen. Diese Maschinen-ID wird durch den fremden Registrierungsserver in der Radius Access-Request oder Radius-Zugangsanforderung an den Heimatregistrierungsserver gesendet.
5. Shared Secret (Gemeinsam benutzter Geheimcode). Wenn die Proxy-Registrierungsaufforderungs-Flagge auf TRUE (wahr) ist, wird der gemeinsam benutzte Geheimcode zwischen dem fremden und dem Heimatregistrierungsserver verwendet, um ihre Identitäten untereinander zu identifizieren. Andernfalls wird das Feld ignoriert.
6. Tunneling Protocol Parameters. Dieses Feld wird zum Speichern von Parametern verwendet, um die Tunnel zur Versorgung des Endsystems zu konfigurieren. Für ein Endsystem zu Hause umfasst es Informationen über Tunnelparameter zwischen der Basisstation und der Heimat-IWF und von der Heimat-IWF zum PPP-Server. Für ein Gast-Endsystem umfasst es Tunnelparameter von der Basisstation zur versorgenden IWF und von der versorgenden IWF zur Heimat-IWF. Für jeden Tunnel enthält dieses Feld wenigstens die Art des zu verwendenden Tunnelprotokolls und irgendwelche tunnelprotokollspezifischen Parameter. Zum Beispiel kann dieses Feld die Kennung für das Tunnelprotokoll L2TP und irgendwelche zusätzlichen Parameter enthalten, die erforderlich sind, um den L2TP-Tunnel zwischen der IWFD und ihrem Partner zu konfigurieren.
7. Accounting Server Association (Abrechnungsserververeinbarung). Dieses Feld wird verwendet, um Informationen zu speichern, die durch die IWF zum Erzeugen von Abrechnungsdaten für das Endsystem benötigt werden. Es enthält den Namen des Abrechnungsprotokolls (z.B. RADIUS), den DNS-Namen des Abrechnungsservers und zusätzliche Parameter, die für das Abrechnungsprotokoll spezifisch sind, wie die UDP-Port-Nummer, den gemeinsam benutzten Geheimcode, den die IWF im Radius Accounting- oder Radius-Abrechnungsprotokoll verwenden muss, die Häufigkeit der Kontrollpunktmarkierung, den Anfangswert zum Erzeugen der Sitzungs-/Mehrfachsitzungs-ID usw. Der DNS-Name des Abrechnungsservers wird in die IP-Adresse des Abrechnungsservers übersetzt, welche an die IWF gesendet wird.

[0194] Für Drahtlosdiensteanbeiter, die Roaming-Vereinbarungen miteinander haben, wird das HDD zur Authentifizierung und zum Abschluss des Registrierungsprozesses verwendet. Wenn ein Endsystem von seinem Heimatnetz in ein Fremdnetz wandert, konsultiert der fremde Registrierungsserver in diesem Netz das HDD in seiner MSC, um Informationen über die Heimatregistrierung des Besucher-Endsystems zu erhalten und das Heimatnetz zu authentifizieren, bevor er das Besucher-Endsystem versorgt.

[0195] Die Software für die Heimatdomänenverzeichnisverwaltung stellt vorzugsweise eine HDD-Verwaltungsschnittstelle für Systemadministratoren bereit, die auf einer graphischen Benutzeroberfläche (GUI für engl. graphical user interface) basiert. Durch Verwenden dieser GUI sind Systemadministratoren imstande, die Einträge im HDD einzusehen und zu aktualisieren. Diese GUI ist nicht zur Verwendung durch fremde Drahtlosnetzdiensteanbieter gedacht, um auf der Basis von Roaming-Vereinbarungen Fernaktualisierungen durchzuführen. Sie ist nur zur Verwendung durch zuverlässiges Personal des Heimat-Drahtlosdiensteanbieters bestimmt und arbeitet hinter Firewalls.

[0196] Das Fremddomänenverzeichnis (FDD) stellt eine Funktionalität bereit, welche die Umkehr des Heimatdomänenverzeichnisses ist. Das FDD wird durch den Heimatregistrierungsserver verwendet, um Parameter über den fremden Registrierungsserver und das Fremdnetz abzurufen, um das fremde Netz zu authentifizieren und einen Tunnel zwischen einer versorgenden IWF und eine Heimat-IWF zu erzeugen. Diese Parameter umfassen den heimat-fremdseitig gemeinsam benutzten Geheimcode, die Konfiguration des Tunnels zwischen Heimat-IWF und versorgender IWF usw. Das FDD befindet sich vorzugsweise in der MSC des Heimatregistrierungsservers. Das FDD wird durch den Heimatregistrierungsserver zum Registrieren von Gast-Endsystemen verwendet.

[0197] Die folgenden Informationen sind im FDD gespeichert:

1. Foreign Domain Name. Dieses Feld wird als Schlüssel beim Absuchen des FDDs nach einem Eintrag verwendet, der mit dem voll qualifizierten Domänennamen des fremden Registrierungsservers, der die Registrierungsaufforderung weiterleitet, übereinstimmt.
2. Shared Secret. Dies ist der gemeinsam benutzte Geheimcode, der zwischen dem fremden und dem Heimatregistrierungsserver verwendet wird, um sich gegenseitig ihre Identität zu authentifizieren.
3. Home IWF-Serving UWF Tunneling Protocol Parameters. Dieses Feld wird zum Speichern von Parametern verwendet, um den Tunnel zwischen der Heimat-IWF und der versorgenden IWF zu konfigurieren. Dieses Feld enthält wenigstens die Art des zu verwendenden Tunnelprotokolls und irgendwelche tunnelprotokollspezifischen Parameter. Zum Beispiel kann dieses Feld die Kennung für das Tunnelprotokoll L2TP und irgendwelche zusätzlichen Parameter enthalten, die erforderlich sind, um den L2TP-Tunnel zwischen der versorgenden IWF und der Heimat-IWF zu konfigurieren.
4. Accounting Server Association (Abrechnungsserververeinbarung). Dieses Feld wird verwendet, um Informationen zu speichern, die durch die Heimat-IWF zum Erzeugen von Abrechnungsdaten für das Endsystem benötigt werden. Es enthält den Namen des Abrechnungsprotokolls (z.B. RADIUS), den DNS-Namen des Abrechnungsservers und zusätzliche Parameter, die für das Abrechnungsprotokoll spezifisch sind, wie die UDP-Port-Nummer, den gemeinsam benutzten Geheimcode, den die IWF im Radius Accounting-Protokoll verwenden muss, die Häufigkeit der Kontrollpunktmarkierung, den Anfangswert zum Erzeugen der Sitzungs-/Mehrfachsitzungs-ID usw. Der DNS-Name des Abrechnungsservers wird in die IP-Adresse des Abrechnungsservers übersetzt, welche an den fremden Agenten gesendet wird.

[0198] Für Drahtlosdiensteanbieter, die Roaming-Vereinbarungen miteinander haben, wird das FDD zur Authentifizierung und zum Abschluss des Registrierungsprozesses verwendet. Wenn ein Endsystem von seinem Heimatnetz in ein Fremdnetz wandert, konsultiert der Registrierungsserver im Heimatnetz das FDD in seiner MSC, um Informationen zu erhalten und das Fremdnetz zu authentifizieren, welches das Endsystem versorgt.

[0199] Die Software für die Fremddomänenverzeichnisverwaltung stellt vorzugsweise eine FDD-Verwaltungsschnittstelle für Systemadministrator bereit, die auf einer graphischen Benutzeroberfläche (GUI) basiert. Durch Verwenden dieser GUI sind Systemadministratoren imstande, die Einträge im FDD einzusehen und zu aktualisieren. Diese GUI ist nicht zur Verwendung durch fremde Drahtlosnetzdiensteanbieter gedacht, um auf der Basis von Roaming-Vereinbarungen Fernaktualisierungen durchzuführen. Sie ist nur zur Verwendung durch zuverlässiges Personal des Heimat-Drahtlosdiensteanbieters bestimmt und arbeitet hinter Firewalls.

[0200] Das Internetdiensteanbieterverzeichnis (ISPD) wird durch die Heimat-IWF verwendet, um die Verbindungsfähigkeit mit ISPs zu verwalten, die Dienstvereinbarungen mit dem Drahtlosdiensteanbieter haben, damit Teilnehmer unter der Verwendung des Netzes auf ihre ISPs zugreifen können. Für jeden Teilnehmer weist das Teilnehmerverzeichnis einen Eintrag für den ISP des Teilnehmers auf. Dieses Feld zeigt auf einen Eintrag im ISPD. Die Heimat-IWF verwendet diese Informationen, um die Verbindung mit dem ISP für den Teilnehmer aufzubauen.

[0201] Die Netzarchitektur unterstützt Roaming. Damit ein Roaming zwischen Drahtlosdiensteanbietern funktioniert, muss die Architektur das Aufstellen von Roaming-Vereinbarungen zwischen Drahtlosdiensteanbietern unterstützen. Dies bringt zweierlei mit sich: (1) Aktualisierung von Systemverzeichnissen über Drahtlosdiensteanbieter und (2) Zahlung von Rechnungen zwischen Diensteanbietern.

[0202] Um Teilnehmern den Zugriff auf Internetdiensteanbieter zu erlauben, unterstützt die Architektur Roaming-Vereinbarungen mit Internetdiensteanbietern. Dies bringt mit sich, dass die Architektur imstande sein muss, Daten an ISP-PPP-Server zu senden und Daten von ISP-PPP-Servern zu empfangen (d.h. die Industriestandardprotokolle wie PPP, L2TP und Radius unterstützen). Es bringt auch mit sich, dass die Architektur Verzeichnisaktualisierungen für den ISP-Zugang bearbeitet und die Zahlung von Rechnungen mit ISPs abwickelt.

[0203] Wenn Roaming-Vereinbarungen zwischen zwei Drahtlosdiensteanbietern getroffen werden, müssen beide Anbieter ihre Heimat- und Fremddomänenverzeichnisse aktualisieren, um Authentifizierungs- und Registrierungsfunktionen für Endsysteme, die ihre Netze vom anderen Netz besuchen, zu unterstützen. Die Architektur der vorliegenden Ausführungsform unterstützt wenigstens manuelle Verzeichnisaktualisierungen. Wenn eine Roaming-Vereinbarung zwischen zwei Drahtlosdiensteanbietern getroffen wird, dann tauschen die beiden Vereinbarungspartner Informationen zum Bestücken ihrer Heimat- und Fremddomänenverzeichnisse aus. Die tatsächlichen Aktualisierungen der Verzeichnisse erfolgt manuell durch Personal der jeweiligen Diensteanbieter. Wenn später die Informationen in den Heimat- und Fremddomänenverzeichnissen aktualisiert werden müssen, tauschen die beiden Vereinbarungspartner die aktualisierten Informationen aus und wenden dann ihre Aktualisierungen manuell auf die Verzeichnisse an.

[0204] In einer alternativen Ausführungsform umfasst die Verzeichnisverwaltungssoftware Entwicklungsstandards in der IETF, um ein Roaming zwischen Internetdiensteanbietern zu ermöglichen und ISPs zu befähigen, Roaming-Verhältnisse automatisch zu verwalten und zu ermitteln. Dies macht eine manuelle Verzeichnisverwaltung nicht mehr nötig. Das Netzsystem verbreitet Roaming-Verhältnisse automatisch und ermittelt sie, um Besucher-Endsysteme zu authentifizieren und zu registrieren.

[0205] Die Netzarchitektur verarbeitet und speichert wenigstens die Abrechnungsdaten und stellt die Daten dem Gebührenverrechnungssystem des Drahtlosdiensteanbieters zur Verfügung. Es liegt am Gebührenverrechnungssystem, die Zahlung von Rechnungen für das Roaming abzuwickeln.

[0206] In einer alternativen Ausführungsform werden Entwicklungsstandards in der IETF zum Abwickeln der Verteilung von Abrechnungssätzen zwischen Internetdiensteanbietern in die Netzarchitektur aufgenommen, um ISPs zu befähigen, die Zahlung von Rechnungen für Gast-Endsysteme durchzuführen.

[0207] Die Systemsoftware unterstützt den Zugang zu IPS und privaten Intranets durch Unterstützen des L2TPs zwischen der Heimat-IWF und dem ISP- oder Intranet-PPP-Server der. Das Internetdiensteanbieterverzeichnis enthält Informationen, die für die IWF zum Erzeugen dieser Tunnel nützlich sind. Wenn Zugangsvereinbarungen zwischen dem Drahtlosdiensteanbieter und den Internetdiensteanbietern etabliert sind, wird dieses Verzeichnis durch das Personal des Drahtlosdiensteanbieters manuell aktualisiert. Automatische Aktualisierungen und eine automatische Ermittlung von Zugangsverhältnissen zwischen dem Drahtlosdiensteanbieter und Internetdiensteanbietern sind ins Auge gefasst und werden implementiert, sobald die Internetstandards weiter entwickelt sind. Während der Teilnehmer auf einen Internetdiensteanbieter zugreift, empfängt er zwei Rechnungen – eine vom Drahtlosdiensteanbieter für die Verwendung des drahtlosen Netzes, und die zweite vom Internetdiensteanbieter. Obwohl durch die Software der Mindestausführungsform keine gemeinsame Vergebührung, welche die beiden Arten von Gebühren vereinigt, abgewickelt wird, ist vorgesehen, dass die Software die Internetstandards für Rechnungszahlung, sobald sie weiter entwickelt sind, nutzen wird, damit Teilnehmer eine gemeinsame Rechnung basierend auf Roaming-Vereinbarungen zwischen dem ISP und Drahtlosdiensteanbietern empfangen können.

[0208] Das System weist ein Elementverwaltungssystem zum Verwalten der Netzelemente auf. Vom Elementverwalter führen Systemadministratoren Konfigurations-, Erfüllungs- und Fehler/Alarmverwaltungsfunktionen aus. Die Elementverwaltungsanwendungen laufen über einem Webbrowser. Bei Verwenden eines Webbrowsers verwalten Systemadministratoren das Netz von überall, von wo sie einen TCP/IP-Zugang haben. Der Elementverwalter führt auch eine Agentenfunktion für einen übergeordneten Verwalter aus. In dieser Funktion exportiert er eine SNMP MIB zur Alarm- und Fehlerüberwachung.

[0209] Ein übergeordneter SNMP-Verwalter wird über SNMP-Unterbrechungen von Alarmbedingungen unterrichtet. Der übergeordnete SNMP-Verwalter fragt die MIB des Elementverwalters regelmäßig hinsichtlich der Gesundheit und des Status des Netzes ab. Das Systemverwaltungspersonal beim übergeordneten Verwalter ist imstande, eine Bildschirmsymboldarstellung des Netzes und seines aktuellen Alarmzustands einzusehen. Durch Zeigen und Klicken auf das Netzelementsymbol kann das Systemverwaltungspersonal unter Verwendung eines Webbrowsers Elementverwaltungsanwendungen ausführen und genauere Verwaltungsfunktionen durchführen.

[0210] Innerhalb des Netzes erfolgt die Verwaltung der physikalischen und logischen Netzelemente unter Verwendung einer Kombination des SNMP-Protokolls und internen Verwaltungsanwendungsprogrammierschnittstellen. Anwendungen im Elementverwalter verwenden SNMP- oder andere Verwaltungs-APIs zur Ausführung von Netzverwaltungsfunktionen.

[0211] Architektonisch weist ein Elementverwaltungssystem zwei verschiedene Sätze von Funktionselementen auf. Der erste Satz von Funktionselementen, welcher die Konfigurationsdatenserver-, Leistungsdatenüberwachungs-, Gesundheits/Statusüberwachungs- und Netzelementwiederherstellungs-Software umfasst, läuft auf einem HA-Server, der mit RAID-Platten ausgestattet ist. Der zweite Satz von Funktionselementen, welcher die Verwaltungsanwendungen umfasst, läuft auf einem dedizierten Nicht-HA-Verwaltungssystem. Selbst wenn das Elementverwaltungssystem betriebsunfähig wird, sind die Netzelemente weiter imstande, zu laufen und Alarme zu melden, und sie sind sogar imstande, sich von Störbedingungen zu regenerieren. Da jedoch alle Verwaltungsanwendungen im Nicht-HA-Elementverwalter ablaufen, sind dann, wenn der Elementverwalter ausfällt, Wiederherstellungsmaßnahmen, die der Intervention von Menschen bedürfen, nicht möglich, bis der Elementverwalter wieder betriebsfähig wird.

[0212] Die drahtlosen Hubs (WHs) in den Basisstationen gehören normalerweise einem Drahtlosdiensteanbeiter (WSP) und sind über Punkt-zu-Punkt-Verbindungen, Intranets oder das Internet mit dem Registrierungsserver (RS) des WSPs verbunden. Der WSP-Registrierungsserver ist normalerweise ein Softwaremodul, das auf einem Prozessor läuft, um bestimmte Registrierungsfunktionen auszuführen. Netzübergangsfunktionseinheiten (IWF-Einheiten) sind normalerweise Softwaremodule, die auf einem Prozessor laufen, um bestimmte Anbindungsfunktionen auszuführen. Die IWF-Einheiten sind normalerweise über Intranets/WAN mit den Registrierungsservern verbunden, und die IWF-Einheiten gehören normalerweise dem WSP. Die IWF-Einheiten brauchen jedoch nicht innerhalb desselben LANs wie die Registrierungsserver angeordnet zu sein. Normalerweise sind Abrechnungs- und Verzeichnisserver (ebenfalls Softwaremodule, die auf einem Prozessor laufen) über ein LAN im Datenzentrum des Diensteanbieters (z.B. einem Zentrum, das einen oder mehr Prozessoren aufweist und verschiedenen Servern und anderen Softwaremodulen als Host dient) mit den Registrierungsservern verbunden. Der Verkehr vom Endsystem wird dann über einen Router (verbunden mit dem LAN) zum öffentlichen Internet oder zu einem ISP-Intranet geleitet. Der Registrierungsserver, der sich in einem WSP-Fremdnetz befindet, wird als der fremde Registrierungsserver (FRS) bezeichnet, und der Registrierungsserver, der im Heimatnetz des Endsystems (wo die Mobileinheit ihren Dienst erwirbt) angeordnet ist, wird als der Heimatregistrierungsserver (HRS) bezeichnet. Die Netzübergangsfunktionseinheit im Heimatnetz wird als die Heimat-IWF bezeichnet, während die Netzübergangsfunktion im Fremdnetz (d.h. im Netz, das vom Endsystem besucht wird) als die versorgende IWF bezeichnet wird.

[0213] Für feste drahtlose Dienste (d.h. ein sich nicht bewegendes Endsystem) kann ein Endsystem sich für einen Dienst auf dem Heimatnetz vom Heimatnetz (z.B. Zu-Hause-Dienst) oder von einem Fremdnetz (z.B. einem Roaming-Dienst) registrieren lassen. Das Endsystem empfängt eine Ankündigung, die durch einen Agenten (z.B. einer Agentenfunktion, die in Software implementiert ist) im drahtlosen Hub über den Zugangspunkt gesendet wird. Es ist sowohl eine MAC-Schicht-Registrierung als auch eine Netzschichtregistrierung zu bewerkstelligen. Diese können zur besseren Wirksamkeit miteinander verknüpft werden.

[0214] Für Endsystem zu Hause (Fig. 26) wird die Netzschichtregistrierung (wie eine lokale Registrierung) über den drahtlosen Hub, an welchen das Endsystem gerade angeschlossen ist, an den Heimatregistrierungsserver gesendet. Eine IWF im Heimatnetz des Endsystems wird zur Anker- oder Heimat-IWF. Auf diese Weise pflanzen sich PPP-Rahmen von und zum Endsystem über den drahtlosen Hub zur Heimat-IWF im Heimatnetz fort. Wenn das Endsystem zu Hause ist, wird die Heimat-IWF über ein XTunnel-Protokoll mit dem drahtlosen Hub verbunden.

[0215] For einen drahtlosen Roaming-Dienst (Fig. 27) stellt der fremde Registrierungsserver während der Registrierungsphase die Identität des Heimatnetzes für das Gast-Endsystem fest. Unter Verwendung dieser Informationen kommuniziert der fremde Registrierungsserver mit dem Heimatregistrierungsserver, um das Endsystem zu authentifizieren und zu registrieren. Der fremde Registrierungsserver ordnet dann eine versorgende IWF zu, und es wird eine I-XTunnel-Protokoll-Verbindung zwischen der Heimat-IWF und der versorgenden IWF für das Gast-Endsystem hergestellt. Die versorgende IWF leitet Rahmen zwischen dem drahtlosen Hub und der Heimat-IWF weiter. Von der Heimat-IWF werden Daten an einen PPP-Server (d.h. Punkt-zu-Punkt-Protokollserver) gesendet, welcher in derselben IWF sitzt. Wenn jedoch die Daten zu einem firmeneigenen Intranet oder einem ISP-Intranet, das seinen eigenen PPP-Server hat, gehen sollen, werden die Daten über das L2TP-Protokoll an den getrennten PPP-Server gesendet. Der getrennte Server gehört normalerweise einem Internetdiensteanbieter, der vom Drahtlosdiensteanbieter verschieden ist, und wird von diesem betrieben. Für die Dauer der Sitzung bleiben die Aufenthaltsorte der Heimat-IWF und des PPP-Servers fest. Die MAC-Schicht-Registrierung kann mit der Netzschichtregistrierung verknüpft werden, um Zusatzaufwand von getrennten Kommunikationen für die MAC-Schicht- und die Netzschichtregistrierung einzusparen; es kann jedoch vorteilhaft sein, diese Registrierungsprozesse nicht zu verknüpfen, damit die WSP-Betriebsmittel mit anderen drahtlosen Netzen, welche nur das IETF Mobile IP unterstützen, zusammenwirken können.

[0216] Eine Registrierung erstellt drei Tabellen. Eine Tabelle 1 wird jedem Zugangspunkt zugeordnet, und Tabelle 1 identifiziert jede Verbindung (d.h. jedes Endsystem) durch eine Verbindungs-ID (CID für engl. connection ID) und ordnet der Verbindungs-ID eine bestimmte Drahtlosmodem- oder WM-Adresse (WM für engl. wireless modem) (d.h. die Adresse des Endsystems oder das Endsystem) zu. Eine Tabelle 2 wird jedem drahtlosen Hub (WH) zugeordnet, und Tabelle 2 ordnet jeder Verbindung-ID eine entsprechende Drahtlosmodemadresse, einen Zugangspunkt und eine XTunnel-ID (XID) zu. Eine Tabelle 3 wird jeder Netzübergangsfunktion (IWF) zugeordnet, und Tabelle 3 ordnet jeder Verbindungs-ID eine entsprechende Drahtlosmodemadresse, Drahtloshubadresse, XTunnel-ID und einen entsprechenden IP-Port (IP/Port) zu. Die für diese Tabellen beschriebenen Einträge sind so dargestellt, dass sie nur relevante Einträge enthalten, die zur Erörterung der Mobilitätsverwaltung beitragen. In Wirklichkeit gibt es andere wichtige Felder, die ebenfalls aufgenommen werden müssen.

Tabelle 1: Verbindungstabelle am AP

CID	WM
C1	WM1

C2	WM1
C1	WM2

Tabelle 2: Verbindungstabelle am WH

CID	WM	AP	XID
C1	WM1	AP1	5
C2	WM1	AP1	5
C1	WM2	AP1	6
C1	WM3	AP2	7

Tabelle 3: Verbindungstabelle an der IWF

CID	WM	WH	XID	IP/Port
C1	WM1	WH1	5	IP1/P1
C2	WM1	WH1	5	IP1/P2
C1	WM2	WH1	6	IP2/P3
C1	WM3	WH1	7	IP3/P1
C5	WM5	WH2	8	IP4/P1

[0217] Die Protokollstapel für Wähl-Benutzer zu Hause in einem Netz, sowie für Gast-Benutzer sind in Fig. 28 bis Fig. 31 dargestellt. Fig. 28 veranschaulicht Protokollstapel, die für direkten Internetzugang durch ein festes (d.h. sich nicht bewegendes) Endsystem zu Hause verwendet werden, wobei eine PPP-Protokoll-Nachricht in der Heimat-IWF (normalerweise ortsgleich mit dem drahtlosen Hub untergebracht) endet, welche die Nachricht zu und von einem IP-Router und von da zum öffentlichen Internet weiterleitet. Fig. 29 veranschaulicht Protokollstapel, die für einen Internetfernzugang (d.h. entweder private Firmennetze oder einen ISP) durch ein festes (d.h. sich nicht bewegendes) Endsystem zu Hause verwendet werden, wobei eine PPP-Protokoll-Nachricht durch die Heimat-IWF (normalerweise ortsgleich mit de drahtlosen Hub untergebracht) zu einem PPP-Server des privaten Firmenintranets oder ISPs weiterleitet. Fig. 30 veranschaulicht Protokollstapel, die für direkten Internetzugang durch ein wanderndes, aber festes (d.h. sich nicht bewegendes) oder ein sich bewegendes Endsystem verwendet werden, wobei das PPP-Protokoll in der Heimat-IWF (normalerweise in einer Mobilvermittlungseinrichtung des Heimatnetzes angeordnet) endet, welche die Nachricht zu und von einem IP-Router weiterleitet. Man beachte in Fig. 30, wie der Nachrichtenverkehr neben der Heimat-IWF auch eine versorgende IWF (normalerweise ortsgleich mit dem drahtlosen Hub untergebracht) passiert. Fig. 31 veranschaulicht Protokollstapel, die für einen Internetfernzugang (d.h. entweder private Firmennetze oder einen ISP) durch ein

wanderndes, aber festes (d.h. sich nicht bewegendes) oder ein sich bewegendes Endsystem verwendet werden, wobei eine PPP-Protokoll-Nachricht durch die Heimat-IWF (normalerweise in einer Mobilvermittlungseinrichtung des Heimatnetzes angeordnet) zu einem PPP-Server des privaten Firmenintranets oder ISPs weitergeleitet wird. Man beachte in Fig. 31, wie der Nachrichtenverkehr neben der Heimat-IWF auch eine versorgende IWF (normalerweise ortsgleich mit dem drahtlosen Hub untergebracht) passiert. Wenn die versorgende IWF und der drahtlose Hub ortsgleich im selben Computersatz untergebracht oder sogar in denselben Computer programmiert sind, ist es nicht notwendig, einen Tunnel unter Verwendung des XTunnel-Protokolls zwischen der versorgenden IWF und dem drahtlosen Hub aufzubauen.

[0218] Gleichwertige Varianten dieser Protokollstapel (z.B. kann das RLP für Mobileinheiten zu Hause am drahtlosen Hub statt an der versorgenden IWF oder der Heimat-IWF beendet werden) sind ebenfalls vorgesehen. Wenn die IWF entfernt vom drahtlosen Hub angeordnet ist, und die Pakete potenziell über ein verlustbehaftetes IP-Netz zwischen der IWF und dem drahtlosen Hub übertragen werden können, ist es vorzuziehen, dass das RLP-Protokoll am drahtlosen Hub endet. Eine andere Variante ist, dass der XTunnel zwischen dem drahtlosen Hub und der IWF nicht über dem UDP/IP aufgebaut zu werden braucht. XTunnel können unter Verwendung der Rahmenweiterleitungs/ATM-Verbindungsschicht aufgebaut werden. Die Verwendung von UDP/IP macht es jedoch leichter, die Drahtloshub- und IWF-Software von einem Netz zum anderen zu bewegen.

[0219] Es können vier Weiterschaltungsszenarien stattfinden, und sie werden folgendermaßen bezeichnet: (i) lokale Mobilität, (ii) Mikromobilität, (iii) Makromobilität und (iv) globale Mobilität. In keinem der vier Szenarien (in einer Ausführungsform der Erfindung) wird eine Leitwegoptimierungsoption berücksichtigt, so dass die Aufenthaltsorte des Heimatregistrierungsservers und des ISP-PPP-Servers sich nicht ändern. In einer anderen Ausführungsform der Erfindung mit Leitwegoptimierung können die ISP-PPP-Server wechseln. Dieser Aspekt wird jedoch im Folgenden erörtert. Außerdem ändern sich die Aufenthaltsorte des fremden Registrierungsservers und IWF in den ersten drei Szenarien nicht.

[0220] Der vorgeschlagene Mobile-IP-Standard von IETF erfordert, dass ein Endsystem, wann immer es das IP-Teilnetz wechselt, an welches es angeschlossen ist, eine Registrierungsaufforderungsnachricht an dem Heimatagenten in seinem Heimatteilnetz sendet. Diese Nachricht führt eine Gastadresse mit, unter der das Endsystem im neuen Teilnetz erreicht werden kann. Wenn Verkehr zum Beispiel von einem ISP an ein Endsystem gesendet wird, fängt der Heimatagent den Verkehr, der für das Endsystem bestimmt ist, auf und übermittelt den Verkehr dann an die Gastadresse. Die Gastadresse identifiziert einen bestimmten fremden Agenten im fremden Teilnetz. Der fremde Agent eines Endsystems kann im Endsystem selbst oder in einem getrennten Knoten sitzen, der den Verkehr seinerseits an das Endsystem übermittelt (d.h. ein Proxy-Registrierungsagent). Mobile-IP-Weiterschaltungen beziehen den Austausch von Steuernachrichten zwischen dem Agenten eines Endsystems, dem Heimatagenten eines Endsystems und möglicherweise seinen entsprechenden Hosts (CHs für engl. corresponding hosts) ein (bei Leitwegoptimierungsoption).

[0221] Für den vorgeschlagenen Mobile-IP-Standard von IETF wäre es schwierig, die Latenzzeit- und Skalierbarkeitsziele für alle Bewegungen in einem großen Verbindungsnetz zu erreichen. Die vorliegende hierarchische Mobilitätsverwaltung erreicht jedoch solche Ziele. Für kleine Bewegungen (z.B. einen Wechsel von Zugangspunkten) werden nur MAC-Schicht-Neuregistrierungen benötigt. Für größere Bewegungen werden Netzschicht-Neuregistrierungen durchgeführt. Die vorliegende hierarchische Mobilitätsverwaltung unterscheidet sich von der Flachstruktur, die in dem von der IETF vorgeschlagenen Mobile-IP-Standard verwendet wird, sowie dem Model von versorgender/Anker-Netzübergangsfunktion, das in zellularen Systemen wie CDPD (basierend auf einem Standard, der durch das Forum digitaler Zellen-Paketdaten gefördert wird) verwendet wird.

[0222] Wie in Fig. 32 dargestellt, wickelt die lokale Mobilitätsweiterschaltung Endsystembewegungen (als MN für mobile node, mobiler Knoten, bezeichnet) zwischen APs ab, die zu demselben drahtlosen Hub gehören. Demnach ist nur eine MAC-Schicht-Neuregistrierung erforderlich. Das Endsystem empfängt eine Drahtloshubankündigung von einem neuen AP und antwortet mit einer Registrierungsaufforderung, die an den neuen AP adressiert ist.

[0223] Der neue AP (d.h. der AP, der die Registrierungsaufforderung vom Endsystem empfängt) erzeugt neue Einträge in seiner Verbindungstabelle und leitet die Registrierungsnachricht an seinen drahtlosen Hub weiter. Bei lokalen Mobilitätsweiterschaltungen ändert sich der drahtlose Hub nicht. Der drahtlose Hub erkennt die Registrierungsaufforderung des Endsystems als eine MAC-Ebene-Registrierungsaufforderung und aktualisiert sie in seiner Verbindungstabelle, um die Verbindung zum neuen AP zu reflektieren. Dann löscht der alte AP den Verbindungseintrag aus seiner Verbindungstabelle. Es gibt wenigstens drei Möglichkeiten, wie der alte AP

die alten Einträge löschen kann, nämlich (i) bei Zeitüberschreitung, (ii) bei Empfang einer Kopie der weitergeleiteten MAC-Schicht-Vereinbarungsnachricht vom neuen AP an den drahtlosen Hub (wenn diese Weiterleitungsnachricht eine Rundesendenachricht ist), und (iii) bei Benachrichtigung durch den drahtlosen Hub über die Notwendigkeit, den Eintrag zu löschen.

[0224] Wie in Fig. 33 dargestellt, wickelt die Mikromobilitätsweiterschaltung Endsystembewegungen (als MN für mobile node, mobiler Knoten, bezeichnet) zwischen drahtlosen Hubs ab, die zu demselben Registrierungsserver gehören und wo das Endsystem noch durch die bestehende versorgende IWF versorgt werden kann. Wenn eine Ankündigung von einem neuen drahtlosen Hub (durch einen neuen AP) empfangen wird, sendet das Endsystem eine Nachricht, um den Registrierungsserver zu einer Registrierung aufzufordern. Die Registrierungsaufforderung wird vom neuen AP zum neuen drahtlosen Hub an den Registrierungsserver weitergeleitet.

[0225] Wenn der Registrierungsserver bestimmt, dass die bestehende IWF noch verwendet werden kann, sendet der Registrierungsserver eine build XTunnel Request- oder XTunnel-Aufbau-Aufforderungsnachricht, um die bestehende IWF aufzufordern, einen XTunnel zum neuen drahtlosen Hub aufzubauen. Später sendet der Registrierungsserver eine tear down XTunnel Request- oder XTunnel-Abbau-Aufforderungsnachricht, um die bestehende IWF aufzufordern, den bestehenden XTunnel mit dem alten drahtlosen Hub abzubauen. Die XTunnel-Aufbau- und die XTunnel-Abbau-Aufforderungsnachrichten können in eine Nachricht verknüpft werden. Ein fremder Registrierungsserver übermittelt die Registrierungsnachricht nicht an den Heimatregistrierungsserver, da es keinen Wechsel von IWF gibt, weder der versorgenden noch der Heimat-IWF, gibt.

[0226] Nach Empfang einer positiven XTunnel-Aufbau-Antwort und einer positiven XTunnel-Abbau-Antwort von der IWF sendet der Registrierungsserver eine Registrierungsantwort an das Endsystem. Wenn die Registrierungsantwort den neuen drahtlosen Hub erreicht, wird die Verbindungstabelle am neuen drahtlosen Hub aktualisiert, um die Verbindung zum neuen AP zu reflektieren. Der neue AP aktualisiert seine MAC-Filter-Adressentabelle und seine Verbindungstabelle nach Empfang einer Nachricht vom neuen drahtlosen Hub, und die Registrierungsantwort wird an das Endsystem übermittelt.

[0227] Der Registrierungsserver sendet eine Freigabenachricht an den alten drahtlosen Hub. wenn der alte drahtlose Hub die Freigabenachricht empfängt, aktualisiert er seine Verbindungstabelle und die MAC-Filter-Adressentabelle und die Verbindungstabelle des alten APs.

[0228] Wie in Fig. 34 dargestellt, wickelt die Makromobilitätsweiterschaltung Bewegungen zwischen drahtlosen Hubs ab, die zwar einen Wechsel der versorgenden IWF im Fremdnetz mit sich bringen, aber keinen Wechsel des Registrierungsservers mit sich bringen. Wenn eine Ankündigung von einem neuen drahtlosen Hub (durch einen neuen AP) empfangen wird, sendet das Endsystem eine Nachricht, um den Registrierungsserver zur Netzschichtregistrierung aufzufordern. Die Registrierungsaufforderung wird vom neuen AP zum neuen drahtlosen Hub an den Registrierungsserver weitergeleitet.

[0229] Der Registrierungsserver erkennt, dass er ein fremder Registrierungsserver ist, wenn das Endsystem nicht zum Netz des gegenwärtigen Registrierungsservers gehört. Dieser fremde Registrierungsserver bestimmt die Identität des Heimatregistrierungsservers durch Verwenden einer Anforderung, vorzugsweise einer Radius Access- oder Radius-Zugangsanforderung (RA-Anforderung) an den Fremdverzeichnisserver (wie ein großer Gelbe Seiten), und er ordnet dann eine geeignete IWF zu, um die versorgende IWF zu sein, und übermittelt eine Registrierungsaufforderung an den Heimatregistrierungsserver, vorzugsweise durch eine Radius Access-Anforderung (RA-Anforderung), um den Heimatregistrierungsserver über die neu ausgewählte IWF zu informieren.

[0230] Der Heimatregistrierungsserver authentifiziert die Registrierungsaufforderung durch Verwenden einer Anforderung, vorzugsweise einer Radius Access- oder Radius-Zugangsanforderung (RA-Anforderung), an den Heimatverzeichnisserver. Nach dem Authentifizieren der Aufforderung und Bestimmen, dass die bestehende Heimat-IWF noch verwendet werden kann, weist der Heimatregistrierungsserver die Heimat-IWF an, einen neuen I-XTunnel zur neu zugeordneten versorgenden IWF aufzubauen und den bestehende I-XTunnel zur alten versorgenden IWF abzubauen. Nach Empfang einer positiven I-XTunnel-Aufbau-Antwort und einer positiven I-XTunnel-Abbau-Antwort von der Heimat-IWF sendet der Heimatregistrierungsserver eine Registrierungsantwort an den fremden Registrierungsserver.

[0231] Der fremde Registrierungsserver weist dann die neu zugeordnete IWF an, einen XTunnel zum neuen drahtlosen Hub aufzubauen. Nach Empfang einer positiven XTunnel-Aufbau-Antwort weist der fremde Regis-

trierungsserver die alte IWF an, den XTunnel zum alten drahtlosen Hub abzubauen. Nach Empfang einer positiven XTunnel-Aufbau-Antwort und einer positiven XTunnel-Abbau-Antwort sendet der fremde Registrierungsserver eine Registrierungsantwort an das Endsystem.

[0232] Wenn die Registrierungsantwort den neuen drahtlosen Hub erreicht, wird die Verbindungstabelle am neuen drahtlosen Hub aktualisiert, um die Verbindung zum neuen AP zu reflektieren. Der neue AP aktualisiert seine MAC-Filter-Adressentabelle und seine Verbindungstabelle nach Empfang einer Nachricht vom neuen drahtlosen Hub, und die Registrierungsantwort wird an das Endsystem weitergeleitet.

[0233] Der Registrierungsserver sendet eine Freigabenachricht an den alten drahtlosen Hub. Wenn der alte drahtlose Hub die Freigabenachricht empfängt, aktualisiert er seine Verbindungstabelle und die MAC-Filter-Adressentabelle, und der alte AP aktualisiert seine MAC-Filter-Adressentabelle und seine Verbindungstabelle nach Empfang einer Nachricht vom alten drahtlosen Hub.

[0234] Die globale Mobilitätsweiterschaltung wickelt Bewegungen zwischen drahtlosen Hubs ab, die einen Wechsel des Registrierungsserver mit sich bringen. **Fig. 35** veranschaulicht eine globale Mobilitätsumschaltung, bei welcher die Heimat-IWF nicht wechselt, und **Fig. 36** veranschaulicht eine globale Mobilitätsweiterschaltung, bei welcher die Heimat-IWF wechselt. Wenn eine Ankündigung von einem neuen drahtlosen Hub (durch einen neuen AP) in einem Fremdnetz empfangen wird, sendet das Endsystem eine Nachricht, um den fremden Registrierungsserver zu einer Netzuschichtregistrierung aufzufordern. Die Registrierungsaufforderung wird vom neuen AP zum neuen drahtlosen Hub an den neuen fremden Registrierungsserver weitergeleitet.

[0235] Der Registrierungsserver erkennt, dass er ein fremder Registrierungsserver ist, wenn das Endsystem nicht zum Netz des gegenwärtigen Registrierungsservers gehört. Dieser fremde Registrierungsserver bestimmt die Identität des Heimatregistrierungsservers durch Verwenden einer Anforderung, vorzugsweise einer Radius Access- oder Radius-Zugangsanforderung (RA-Anforderung), an den Fremdverzeichnisserver (wie ein großer Gelbe Seiten), und er ordnet dann eine geeignete IWF zu, um die versorgende IWF zu sein, und übermittelt eine Registrierungsaufforderung an den Heimatregistrierungsserver, vorzugsweise durch eine Radius Access-Anforderung (RA-Anforderung), um den Heimatregistrierungsserver über die neu ausgewählte IWF zu informieren.

[0236] Der Heimatregistrierungsserver authentifiziert die Registrierungsaufforderung durch Verwenden einer Anforderung, vorzugsweise einer Radius Access- oder Radius-Zugangsanforderung (RA-Anforderung), an den Heimatverzeichnisserver. Nach dem Authentifizieren der Aufforderung und Bestimmen, dass die bestehende Heimat-IWF noch verwendet werden kann (**Fig. 35**), weist der Heimatregistrierungsserver die Heimat-IWF an, einen neuen I-XTunnel zur versorgenden IWF, die durch den neuen fremden Registrierungsserver neu zugeordnet wurde, aufzubauen. Der Heimatregistrierungsserver sendet auch eine Nachricht zur Löschung aus dem Register an den alten fremden Registrierungsserver und weist die Heimat-IWF an, den bestehenden I-T-Tunnel zur bestehenden versorgenden IWF des alten Fremdnetzes abzubauen. Nach Empfang einer positiven I-XTunnel-Aufbau-Antwort und einer positiven I-XTunnel-Abbau-Antwort von der Heimat-IWF sendet der Heimatregistrierungsserver eine Registrierungsantwort an den neuen fremden Registrierungsserver.

[0237] Der neue fremde Registrierungsserver weist dann die neu zugeordnete IWF an, einen XTunnel zum neuen drahtlosen Hub aufzubauen. Nach Empfang einer positiven XTunnel-Aufbau-Antwort sendet der fremde Registrierungsserver eine Registrierungsantwort an das Endsystem. Wenn die Registrierungsantwort den neuen drahtlosen Hub erreicht, wird die Verbindungstabelle am neuen drahtlosen Hub aktualisiert, um die Verbindung zum neuen AP zu reflektieren. Der neue AP aktualisiert seine MAC-Filter-Adressentabelle und seine Verbindungstabelle nach Empfang einer Nachricht vom neuen drahtlosen Hub, und die Registrierungsantwort wird an das Endsystem weitergeleitet.

[0238] Der alte fremde Registrierungsserver weist die alte IWF an, den XTunnel zum alten drahtlosen Hub abzubauen. Nach Empfang einer positiven XTunnel-Abbau-Antwort oder gleichzeitig mit der XTunnel-Abbau-Aufforderung sendet der alte fremde Registrierungsserver eine Freigabenachricht an den alten drahtlosen Hub. Wenn der alte drahtlose Hub, die Freigabenachricht empfängt, aktualisiert er seine Verbindungstabelle und die MAC-Filter-Adressentabelle, und der alte AP aktualisiert seine MAC-Filter-Adressentabelle und seine Verbindungstabelle nach Empfang einer Nachricht vom alten drahtlosen Hub.

[0239] Alternativerweise wählt der Heimatregistrierungsserver, sobald der Heimatregistrierungsserver die Registrierungsaufforderung vom neuen fremden Registrierungsserver authentifiziert und bestimmt hat, dass

die bestehende Heimat-IWF nicht mehr verwendet werden kann (Fig. 36), eine neue Heimat-IWF und weist die neue Heimat-IWF an, einen neuen Ebene-2-Tunnelprotokoll-Tunnel (L2TP)-Tunnel) zum gegenwärtigen PPP-Server (z.B. dem PPP-Server in einem verbunden ISP-Intranet) aufzubauen. Dann weist der Heimatregistrierungsserver die alte Heimat-IWF an, ihren L2TP-Tunnelverkehr an die neue Heimat-IWF zu übertragen.

[0240] Dann weist der Heimatregistrierungsserver die neue Heimat-IWF an, einen neuen I-XTunnel zur versorgenden IWF, die durch den neuen fremden Registrierungsserver neu zugeordnet wurde, aufzubauen. Der Heimatregistrierungsserver sendet auch eine Nachricht zur Löschung aus dem Register an den alten fremden Registrierungsservers und weist die Heimat-IWF an, den bestehenden I-XTunnel zur bestehenden versorgenden IWF des alten Fremdnetzes abzubauen. Nach Empfang einer positiven I-XTunnel-Aufbau-Antwort und einer positiven I-XTunnel-Abbau-Antwort sendet der Heimatregistrierungsserver eine Registrierungsantwort an den neuen fremden Registrierungsserver.

[0241] Der neue fremde Registrierungsserver weist dann die neu zugeordnete IWF an, einen XTunnel zum neuen drahtlosen Hub aufzubauen. Nach Empfang einer positiven XTunnel-Aufbau-Antwort sendet der fremde Registrierungsserver eine Registrierungsantwort an das Endsystem. Wenn die Registrierungsantwort den neuen drahtlosen Hub erreicht, wird die Verbindungstabelle am neuen drahtlosen Hub aktualisiert, um die Verbindung zum neuen AP zu reflektieren. Der neue AP aktualisiert seine MAC-Filter-Adressentabelle und seine Verbindungstabelle nach Empfang einer Nachricht vom neuen drahtlosen Hub, und die Registrierungsantwort wird an das Endsystem weitergeleitet.

[0242] Der alte fremde Registrierungsserver weist die alte IWF an, den XTunnel zum alten drahtlosen Hub abzubauen. Nach Empfang einer positiven XTunnel-Abbau-Antwort oder gleichzeitig mit der XTunnel-Abbau-Aufforderung sendet der alte fremde Registrierungsserver eine Freigabenachricht an den alten drahtlosen Hub. Wenn der alte drahtlose Hub die Freigabenachricht empfängt, aktualisiert er seine Verbindungstabelle und die MAC-Filter-Adressentabelle, und der alte AP aktualisiert seine MAC-Filter-Adressentabelle und seine Verbindungstabelle nach Empfang einer Nachricht vom alten drahtlosen Hub.

[0243] Endsysteme, die gemäß der vorliegenden Erfindung aufgebaut sind, wirken mit Netzen zusammen, die gemäß den vorgeschlagenen Mobile-IP-Standards von IETF aufgebaut sind, und Endsysteme, die gemäß den vorgeschlagenen Mobile-IP-Standards von IETF aufgebaut sind, wirken mit Netzen zusammen, die gemäß der vorliegenden Erfindung aufgebaut sind.

[0244] Die Hauptunterschiede zwischen der vorliegenden Erfindung und dem IETF Mobile IP (RFC2002, ein Normendokument) sind:

(i) Die vorliegende Erfindung verwendet ein hierarchisches Konzept zur Mobilitätsverwaltung statt einer Flachstruktur wie im vorgeschlagenen IETF Mobile-IP-Standard. Eine kleine Mobilität in einem kleinen Bereich führt zu keiner Netzebenenregistrierung. Eine Mikromobilität bringt den Aufbau eines neuen XTunnels und den Abbau eines bestehenden XTunnels mit sich. Eine globale Mobilität bringt wenigstens den Aufbau eines neuen I-XTunnels und den Abbau eines bestehenden I-XTunnels abgesehen vom Aufbau/Abbau des XTunnels mit sich. Die globale Mobilität bringt manchmal auch den Aufbau eines neuen L2TP-Tunnels und die Übertragung des L2TP-Zustands vom bestehenden L2TP-Tunnel auf den neuen L2TP-Tunnel mit sich.

(ii) In der vorliegenden Erfindung wird ein Benutzername plus einen Bereich zur Identifizierung eines entfernten Wähl-Benutzers statt einer festen Heimatadresse wie im Falle des vorgeschlagenen IETF Mobil-IP-Standards verwendet.

(iii) In der vorliegenden Erfindung werden Registrierungs- und Leitweglenkungsfunktionen durch getrennten Entitäten ausgeführt. Die beiden Funktionen werden im vorgeschlagenen IETF Mobile-IP-Standard durch den Heimatagenten ausgeführt, und beide Funktionen werden im vorgeschlagenen IETF Mobile-IP-Standard durch den fremden Agenten ausgeführt. Im Gegensatz dazu wird in einer Ausführungsform der vorliegenden Erfindung die Registrierung im Registrierungsserver durchgeführt, und Leitweglenkungsfunktionen werden sowohl durch die Heimat- und versorgende IWF als auch den drahtlosen Hub (auch als Zugangshub bezeichnet) ausgeführt.

(iv) Die vorliegende Erfindung verwendet drei Tunnel je PPP-Sitzung. Der XTunnel ist mehr wie ein Verbindungsschichttunnel zwischen dem drahtlosen Hub und der versorgenden IWF. Der I-XTunnel zwischen der versorgenden IWF und der Heimat-IWF ist mehr wie der Tunnel zwischen Heimat- und fremden Agenten im vorgeschlagenen IETF Mobile-IP-Standard. Aber er weist auch zusätzliche Fähigkeiten auf, die über jene der durch den Mobile-IP-Standard vorgeschlagenen Tunnel hinausgehen. Der L2TP-Tunnel wird nur verwendet, wenn die Heimat-IWF kein PPP-Server ist. Die Anzahl dieser Tunnel kann durch Verknüpfen einiger Funktionen im selben Knoten, wie zuvor beschrieben, verringert werden.

(v) In der vorliegenden Erfindung findet eine drahtlose Registrierung statt, bevor eine PPP-Sitzung beginnt,

während im vorgeschlagenen IETF Mobile-IP-Standard eine Mobile-IP-Registrierung stattfindet, nachdem eine PPP-Sitzung in den offenen Zustand eintritt.

(vi) In der vorliegenden Erfindung ist die Netzentität, welche die Agentenankündigung (d.h. der drahtlose Hub) ankündigt, nicht auf einer direkten Verbindung zu den Endsystemen, wohingegen für den vorgeschlagenen IETF Mobile-IP-Standard die Agentenankündigung eine TTL von 1 haben muss, was bedeutet, dass die Endsysteme eine direkte Verbindung mit dem fremden Agenten haben. Außerdem ist die Agentenankündigung in der vorliegenden Erfindung keine Erweiterung zu den ICMP-Routerankündigungen wie im vorgeschlagenen IETF Mobile-IP-Standard.

[0245] Endsysteme in der vorliegenden Erfindung sollten einen Agentenabruf unterstützen. Wenn ein Endsystem in der vorliegenden Erfindung ein Netz besucht, welches den vorgeschlagenen IETF Mobile-IP-Standard unterstützt, wartet es, bis es eine Agentenankündigung hört. Wenn es innerhalb eines annehmbaren Zeitrahmens keine Agentenankündigung empfängt, sendet es einen Agentenabruf rund.

[0246] In der vorliegenden Erfindung können Netzbetreiber mit anderen Netzen, die den vorgeschlagenen IETF Mobile-IP-Standard unterstützen, derart verhandeln, dass den Endsystemen der vorliegenden Erfindung, die andere Netze zu verwenden wünschen, Heimatadressen zugeordnet werden können. Wenn das Endsystem der vorliegenden Erfindung die Agentenankündigung empfängt, kann es feststellen, dass das Netz, das es besucht, kein Netz gemäß der vorliegenden Erfindung ist, und verwendet infolgedessen die zugeordnete Heimatadresse, um sich registrieren zu lassen.

[0247] Für Netze, die den vorgeschlagenen IETF Mobile-IP-Standard unterstützen, beginnt die PPP-Sitzung vor der Mobile-IP-Registrierung, und es ist anzunehmen, dass der PPP-Server in solchen Netzen ortsgleich mit dem fremden Agenten untergebracht ist. In einer Ausführungsform wird ein SNAP-Kopf verwendet, um PPP-Rahmen in den MAC-Rahmen der vorliegenden Erfindung einzukapseln (in einer dem Ethernet-Format ähnlichen weise), und der fremde Agent interpretiert dieses Format als ein proprietäres PPP-Format über Ethernet-Kapselung. Demnach können das Endsystem der vorliegenden Erfindung und sein PPP-Partner in einen offenen Zustand eintreten, bevor der fremde Agent eine Agentenankündigung zu übertragen beginnt, und das Endsystem der vorliegenden Erfindung kann sich registrieren lassen.

[0248] Um Endsystemen, die den vorgeschlagenen IETF Mobile-IP-Standard unterstützen, zu ermöglichen, in Netzen von der Art der vorliegenden Erfindung zu arbeiten, sind solche Mobileinheiten wenigstens imstande, ähnliche MAC-Schicht-Registrierungen durchzuführen. Durch Ausführen des Agentenankündigungsnachrichtformats ähnlich dem Agentenankündigungsnachrichtenformat nach dem vorgeschlagenen IETF Mobile-IP-Standard kann ein Besucher-Endsystem die Agentenankündigung interpretieren und sich mit einem drahtlosen Hub registrieren lassen. In der vorliegenden Erfindung sind Registrierungsaufforderungs- und Registrierungsantwortnachrichten ähnlich den Registrierungsaufforderungs- und Registrierungsantwortnachrichten nach dem vorgeschlagenen IETF Mobile-IP-Standard (ohne irgendwelche unnötige Erweiterungen), derart dass der Rest der Mobilitätsverwaltungsmerkmale der vorliegenden Erfindung für die Besucher-Endsysteme transparent ist.

[0249] Da Endsysteme, die den vorgeschlagenen IETF Mobile-IP-Standard unterstützen, erwarten, dass eine PPP-Sitzung vor der Mobile-IP-Registrierung beginnt, beginnt ein optionales Merkmal in drahtlosen Hubs der vorliegenden Erfindung PPP-, LCP- und NCP-Pakete nach der MAC-Schicht-Registrierung zu interpretieren.

[0250] Um zu vermeiden, dass bei Weiterschaltungen Verkehr verloren geht, verwendet die Mobilitätsverwaltung der vorliegenden Erfindung das Schließer-vor-Öffner-Konzept. Für lokale Mobilität wird eine Schließer-vor-Öffner-Verbindung durch Umwandeln der MAC-Schicht-Registrierungsnachricht, die durch den neuen AP zum drahtlosen Hub weitergeleitet wird, in eine Rundesendenachricht erreicht. Auf diese Weise kann der alte AP von der neuen Registrierung hören und Pakete übermitteln, die für das Endsystem bestimmt sind und nicht an den neuen AP übertragen wurden.

[0251] Für Mikromobilität werden Informationen über den neuen drahtlosen Hub in die XTunnel-Abbau-Nachricht aufgenommen, die zwischen der versorgenden IWF und dem alten WH ausgetauscht wird. Auf diese Weise kann der alte drahtlose Hub bei Hören einer XTunnel-Abbau-Nachricht von der versorgenden IWF gepufferte Pakete übermitteln. Alternativerweise kennt die RLP-Schicht an der IWF die Folgenummer, die durch den alten drahtlosen Hub bis jetzt bestätigt wurde.

[0252] Gleichzeitig kennt die IWF die aktuelle Sendefolgenummer des letzten Pakets, das an den alten drahtlosen Hub gesendet wurde. Daher kann die IWF jene Pakete, die zwischen diesen beiden Nummern angeord-

net sind, an den neuen drahtlosen Hub übermitteln, bevor neuere Pakete an den neuen drahtlosen Hub gesendet werden. Es wird angenommen, dass die RLP-Schicht imstande ist, doppelte Pakete zu filtern. Die zweite Lösung ist der ersten Lösung wahrscheinlich vorzuziehen, da der alte drahtlose Hub möglicherweise nicht imstande ist, direkt mit einem anderen zu kommunizieren.

[0253] Für Makromobilität kann die alte versorgende IWF zusätzlich zu der Paketübermittlung, die vom alten drahtlosen Hub an den neuen drahtlosen Hub erfolgt, Pakete an die neue versorgende IWF übermitteln. Alles, was zu tun ist, ist die Identität der neuen versorgenden IWF in der I-XTunnel-Abbau-Nachricht an die neue versorgende IWF zu übermitteln. Eine andere Möglichkeit, dasselbe Ergebnis zu erreichen, ist, die Heimat-IWF die fehlenden Pakete an die neue versorgende IWF übermitteln zu lassen, statt die alte versorgende IWF zu ersuchen, dies zu tun, da die Heimat-IWF die I-XTunnel-Folgenummer, die als Letzte durch die alte versorgende IWF bestätigt wurde, und die aktuelle I-XTunnel-Folgenummer, die durch die Heimat-IWF gesendet wurde, kennt.

[0254] Das Verfahren des Schätzens, wie viel Puffer pro Mobileinheit pro AP pro drahtlosen Hub pro IWF zugewiesen werden sollte, derart dass ein Verkehrsverlust zwischen Weiterschaltungen minimiert werden kann, besteht darin, das Endsystem für den AP für den drahtlosen Hub für die IWF die Paketankunftsrate und die Weiterschaltzeit schätzen zu lassen. Diese Informationen werden an den alten AP des drahtlosen Hubs der IWF weitergegeben, um zu bestimmen, wie viel Verkehr bei Weiterschaltungen jeweils an den neuen AP übertragen werden sollte.

[0255] Um in der vorliegenden Erfindung eine Leitwegoptimierung zu erreichen, wählt das Endsystem den PPP-Server, der am nächsten zur versorgenden IWF ist. Ohne Leitwegoptimierung können übermäßige Transportverzögerungen und eine übermäßige Benutzung der physikalischen Leitung vorkommen.

[0256] Zum Beispiel kann ein Endsystem, das ein Abonnement bei einem Heimatnetz in New York City hat, nach Hongkong wandern. Um eine Verbindung zwischen einem ISP in Hongkong herzustellen, müsste das Endsystem eine versorgende IWF, die in einem drahtlosen Hub in Hongkong eingerichtet ist, und eine Heimat-IWF, die im Heimatnetz in New York City eingerichtet ist, aufweisen. Eine Nachricht würde dann vom Endsystem (nach Hongkong gewandert) durch die versorgende IWF (in Hongkong) und durch die Heimat-IWF (in New York City) und zurück zum ISP in Hongkong geleitet werden.

[0257] Eine bevorzugte Lösung ist, von der versorgenden IWF (in Hongkong) direkt zum ISP in Hongkong durchzuschalten. Die versorgende IWF agiert wie die Heimat-IWF. In dieser Ausführungsform bestehen Roaming-Vereinbarungen zwischen den fremden und de Heimat-Drahtlosanbietern. Außerdem kommunizieren die verschiedenen Abrechnungs/Gebührenverrechnungssysteme automatisch miteinander, derart dass die Rechnungsinformationen gemeinsam benutzt werden. Der Abrechnungs- und Rechnungsinformationsaustausch kann unter Verwendung von solchen Standards wie dem Standard erfolgen, der durch die ROAMOPS-Arbeitsgruppe der IETF vorgeschlagen wird.

[0258] Die versorgende IWF muss jedoch noch den nächstgelegenen PPP-Server (zum Beispiel den Hongkong-ISP) ermitteln. In der vorliegenden Ausführungsform erfährt der fremde Registrierungsserver von dem Wunsch des Endsystems zur Verbindung mit einem PPP-Server (z.B. einem Hongkong-ISP), wenn er eine Registrierungsaufforderung vom Endsystem empfängt. Wenn der fremde Registrierungsserver bestimmt, dass die versorgende IWF näher zum gewünschten PPP-Server (z.B. dem Hongkong-ISP) ist als die Heimat-IWF, weist der fremde Registrierungsserver die versorgende IWF an, einen L2TP-Tunnel zu ihrem nächstgelegenen PPP-Server herzustellen (im Gegensatz zum PPP-Server, welcher am nächsten zum Heimatregistrierungsserver und zur Heimat-IWF ist). Dann informiert der fremde Registrierungsserver den Heimatregistrierungsserver, dass das Endsystem durch die versorgende IWF und den fremden PPP versorgt wird.

[0259] In einer alternativen Ausführungsform bestimmt der fremde Registrierungsserver, dass die versorgende IWF näher zum gewünschten PPP-Server (z.B. dem Hongkong-ISP) ist als die Heimat-IWF, wenn er eine Registrierungsaufforderung vom Endsystem empfängt. Der fremde Registrierungsserver leitet die Registrierungsaufforderungsnachricht mit einer angehängten Nachricht, welche Informationen über die versorgende IWF angibt, und einer Mitteilung, dass eine Leitwegoptimierung bevorzugt wird, an den Heimatregistrierungsserver weiter. Gleichzeitig weist der fremde Registrierungsserver die versorgende IWF an, einen L2TP-Tunnel zum PPP-Server herzustellen. Nach Genehmigen der Registrierungsaufforderung weist der Heimatregistrierungsservers die Heimat-IWF an, den L2TP-Zustand an die fremde IWF zu übertragen.

[0260] Nachdem nun bevorzugte (zur Veranschaulichung dienende und nicht einschränkende) Ausführungs-

formen einer neuartigen Netzarchitektur mit drahtlosen Endbenutzern, die zu wandern imstande sind, beschrieben wurde, ist zu erwähnen, dass angesichts der zuvor dargelegten Lehren Modifikationen und Variationen durch Fachleute vorgenommen werden können. Zum Beispiel können die Verbindungsstrecken, die hierin beschrieben wurden, auf bekannte Verbindungsprotokolle (z.B. IP, TCP/IP, L2TP, IEEE 802.3 usw.) Bezug nehmen; die Erfindung sieht jedoch andere Verbindungsprotokolle in den Verbindungsstrecken vor, welche dieselben oder ähnliche Datenzustellungsfähigkeiten bereitstellen. Die handelnden Agenten in den zuvor beschriebenen Ausführungsformen können in Form von softwaregesteuerten Prozessoren sein, oder sie können eine andere Form von Steuerungen (z.B. programmierbare Logikanordnungen) sein. Die handelnden Agenten können so gruppiert sein, wie zuvor beschrieben, oder anderweitig gruppiert sein, solange sie sich an die hierin beschriebenen Verbindungslehren halten und den Sicherheits- und Authentifizierungslehren, wie hierin beschrieben, unterwerfen. Außerdem kann ein einziger Zugangspunkt (d.h. drahtloser Hub) oder eine einzige Netzübergangsfunktionseinheit (IWF-Einheit) eine Mehrkanalfähigkeit bereitstellen. Auf diese Weise kann ein einziger Zugangspunkt oder Zugangshub oder eine einzige IWF-Einheit auf den Verkehr von mehreren Endsystemen einwirken und, was hierin als getrennte Zugangspunkte, Zugangshubs oder IWF-Einheiten beschrieben wird, sieht eine Entsprechung mit einem einzigen Mehrkanal-Zugangspunkt, -Zugangshub oder -IWF-Einheit vor.

Patentansprüche

1. Gekoppeltes Datennetz, aufweisend Computer (**2**) und Modem (**4**), die mit dem Internet (**20**) und privaten Intranets (**18**) über ein öffentliches Telefonwählnetz (**6**) verbunden sind, das einen Übergabepunkt (**8**) für einen Internetdiensteanbieter (**8**) und einen Server (**16**) für die privaten Intranets (**18**) versorgt, aufweisend:
ein Fremdnetz (**62**), das eine Basisstation (**64**) und ein fremde Mobilfunkvermittlungsstelle mit einem versorgenden Registrierungsserver aufweist, wobei die Basisstation einen Zugangshub (**84**) mit einer versorgenden Netzübergangsfunktion (**66**) aufweist;
ein Heimatnetz (**70**), das eine Heimatmobilfunkvermittlungsstelle mit einem Heimatregistrierungsserver und einer Heimatnetzübergangsfunktion (**72**) aufweist; und
ein Endsystem (**32**), das am Heimatnetz angeschlossen und im Fremdnetz tätig ist, wobei das Endsystem einen Endregistrierungsagenten aufweist, um eine Registrierungsaufforderung zu erzeugen, die Registrierungsaufforderung eine Angabe eines gewünschten Kommunikationsnetzes und eines gewünschten PPP-Kommunikationsservers, mit dem das Endsystem eine PPP-Sitzung herstellt, enthält, das Endsystem die Registrierungsaufforderung an den versorgenden Registrierungsserver sendet, der versorgende Registrierungsserver ein erstes Mittel aufweist, das so ausgelegt ist, dass es die Registrierungsaufforderung verarbeitet und einen bestmöglichen Leitweg zwischen dem gewünschten PPP-Kommunikationsserver und der Heimatnetzübergangsfunktion oder der versorgenden Netzübergangsfunktion bestimmt, und der versorgende Registrierungsserver ferner ein zweites Mittel aufweist, das so ausgelegt ist, dass es die versorgende Netzübergangsfunktion mit dem gewünschten PPP-Kommunikationsserver verbindet, wenn das erste Modul bestimmt, dass der bestmögliche Leitweg zwischen der versorgenden Netzübergangsfunktion und dem gewünschten PPP-Kommunikationsserver ist.

2. Datennetz nach Anspruch 1, wobei der versorgende Registrierungsserver ferner ein drittes Mittel aufweist, das so ausgelegt ist, dass es die Registrierungsaufforderung mit einer angehängten Angabe, dass der versorgende Registrierungsserver die versorgende Netzübergangsfunktion und den gewünschten PPP-Kommunikationsserver verbunden hat, an den Heimatregistrierungsserver sendet.

3. Gekoppeltes Datennetz nach Anspruch 1, wobei das Endsystem am Heimatnetz angeschlossen und im Fremdnetz tätig ist, das Endsystem einen Endregistrierungsagenten aufweist, um eine Registrierungsaufforderung zu erzeugen, die Registrierungsaufforderung eine Angabe eines gewünschten Kommunikationsnetzes und eines gewünschten PPP-Kommunikationsservers enthält, das Endsystem die Registrierungsaufforderung an den versorgenden Registrierungsserver sendet, der versorgende Registrierungsserver ein erstes Mittel aufweist, das so ausgelegt ist, dass es die Registrierungsaufforderung verarbeitet und einen bestmöglichen Leitweg zwischen dem gewünschten PPP-Kommunikationsserver und der Heimatnetzübergangsfunktion oder der versorgenden Netzübergangsfunktion bestimmt, und der versorgende Registrierungsserver ferner ein zweites Mittel aufweist, das so ausgelegt ist, dass es die Registrierungsaufforderung mit einer ersten angehängten Angabe, dass der versorgende Registrierungsserver bestimmt hat, dass der bestmögliche Leitweg zwischen der versorgenden Netzübergangsfunktion und dem gewünschten PPP-Kommunikationsserver ist, und einer zweiten angehängten Angabe, dass eine Leitwegoptimierung bevorzugt wird, an den Heimatregistrierungsserver sendet.

4. Datennetz nach Anspruch 3, wobei der versorgende Registrierungsserver ein drittes Mittel aufweist, das

so ausgelegt ist, dass es nach dem Senden der Registrierungsaufforderung und der ersten und zweiten angehängten Angaben an den Heimatregistrierungsserver eine Verbindung zwischen der versorgenden Netzübergangsfunktion und dem gewünschten PPP-Kommunikationsserver herstellt.

5. Datennetz nach Anspruch 4, wobei:
der Heimatregistrierungsserver ein viertes Mittel aufweist, das so ausgelegt ist, dass es eine Registrierungsantwort an den versorgenden Registrierungsserver sendet und die Registrierungsantwort eine Angabe dessen enthält, dass die Verbindung zwischen der versorgenden Netzübergangsfunktion und dem gewünschten PPP-Kommunikationsserver zugelassen wird; und
der Heimatregistrierungsserver ferner ein fünftes Mittel aufweist, das so ausgelegt ist, dass es die Heimatnetzübergangsfunktion anweist, einen Verbindungszustand an die versorgende Netzübergangsfunktion zu übertragen.

6. Verfahren zum Optimieren der Leitweglenkung für ein gekoppeltes Datennetz, aufweisend Computer (**2**) und Modem (**4**), die mit dem Internet (**20**) und mit privaten Intranets (**18**) über ein öffentliches Telefonwählnetz (**6**) verbunden sind, das einen Übergabepunkt (**8**) für einen Internetdiensteanbieter (**8**) und einen Server (**16**) für die privaten Intranets (**18**) versorgt, wobei das gekoppelte Datennetz ferner aufweist
ein Fremdnetz, das eine Basisstation und eine fremde Mobilfunkvermittlungsstelle mit einem versorgenden Registrierungsserver aufweist, wobei die Basisstation einen Zugangshub mit einer versorgenden Netzübergangsfunktion aufweist,
ein Heimatnetz, das eine Heimatmobilfunkvermittlungsstelle mit einem Heimatregistrierungsserver und einer Heimatnetzübergangsfunktion aufweist, und
ein Endsystem, das am Heimatnetz angeschlossen ist, gekennzeichnet durch die folgenden Schritte: Tätig sein im Fremdnetz, wobei das Endsystem einen Endregistrierungsagenten aufweist, um eine Registrierungsaufforderung zu erzeugen, aufweisend die folgenden Schritte:
Erzeugen einer Registrierungsaufforderung am Endsystem, wobei die Registrierungsaufforderung eine Angabe eines gewünschten Kommunikationsnetzes und eines gewünschten PPP-Kommunikationsservers enthält;
Senden der Registrierungsaufforderung vom Endsystem an den versorgenden Registrierungsserver;
Verarbeiten der Registrierungsaufforderung in einem ersten Modul im versorgenden Registrierungsserver, um einen bestmöglichen Leitweg zwischen dem gewünschten PPP-Kommunikationsserver und der Heimatnetzübergangsfunktion oder der versorgenden Netzübergangsfunktion zu bestimmen;
Verbinden der versorgenden Netzübergangsfunktion mit dem gewünschten PPP-Kommunikationsserver, wenn das erste Modul bestimmt, dass der bestmögliche Leitweg zwischen der versorgenden Netzübergangsfunktion und dem gewünschten PPP-Kommunikationsserver ist.

7. Verfahren nach Anspruch 6, welches ferner den folgenden Schritt aufweist:
Senden der Registrierungsaufforderung mit einer angehängten Angabe, dass der versorgende Registrierungsserver die versorgende Netzübergangsfunktion und den gewünschten PPP-Kommunikationsserver verbunden hat, an den Heimatregistrierungsserver.

8. Verfahren nach Anspruch 6 oder Netz nach Anspruch 1 oder 3, wobei:
der gewünschte PPP-Kommunikationsserver ein Kommunikationsserver von mehreren Kommunikationsservern im gewünschten Kommunikationsnetz ist; und
das erste Modul ein Hilfsmittel aufweist, das so ausgelegt ist, dass es den ausgewählten, den gewünschten PPP-Kommunikationsserver unter den mehreren Kommunikationsservern bestimmt.

9. Verfahren nach Anspruch 6 oder Netz nach Anspruch 1 oder 3, wobei das Heimatnetz und das Fremdnetz Rechnungsinformationen für das Endsystem gemeinsam benutzen, wenn das Endsystem im Fremdnetz tätig ist.

10. Verfahren nach Anspruch 6, welches ferner die folgenden Schritte aufweist:
Feststellen, ob die versorgende Netzübergangsfunktion oder die Heimatnetzübergangsfunktion näher zum gewünschten PPP-Kommunikationsserver ist;
Anweisen der versorgenden Netzübergangsfunktion, eine Verbindung mit dem gewünschten PPP-Kommunikationsserver herzustellen, wenn die versorgende Netzübergangsfunktion näher zum gewünschten PPP-Kommunikationsserver als die Heimatnetzübergangsfunktion ist; und
Informieren des Heimatregistrierungsservers, dass das Endsystem durch die versorgende Netzübergangsfunktion und den gewünschten PPP-Kommunikationsserver versorgt wird.

Es folgen 32 Blatt Zeichnungen

Anhängende Zeichnungen

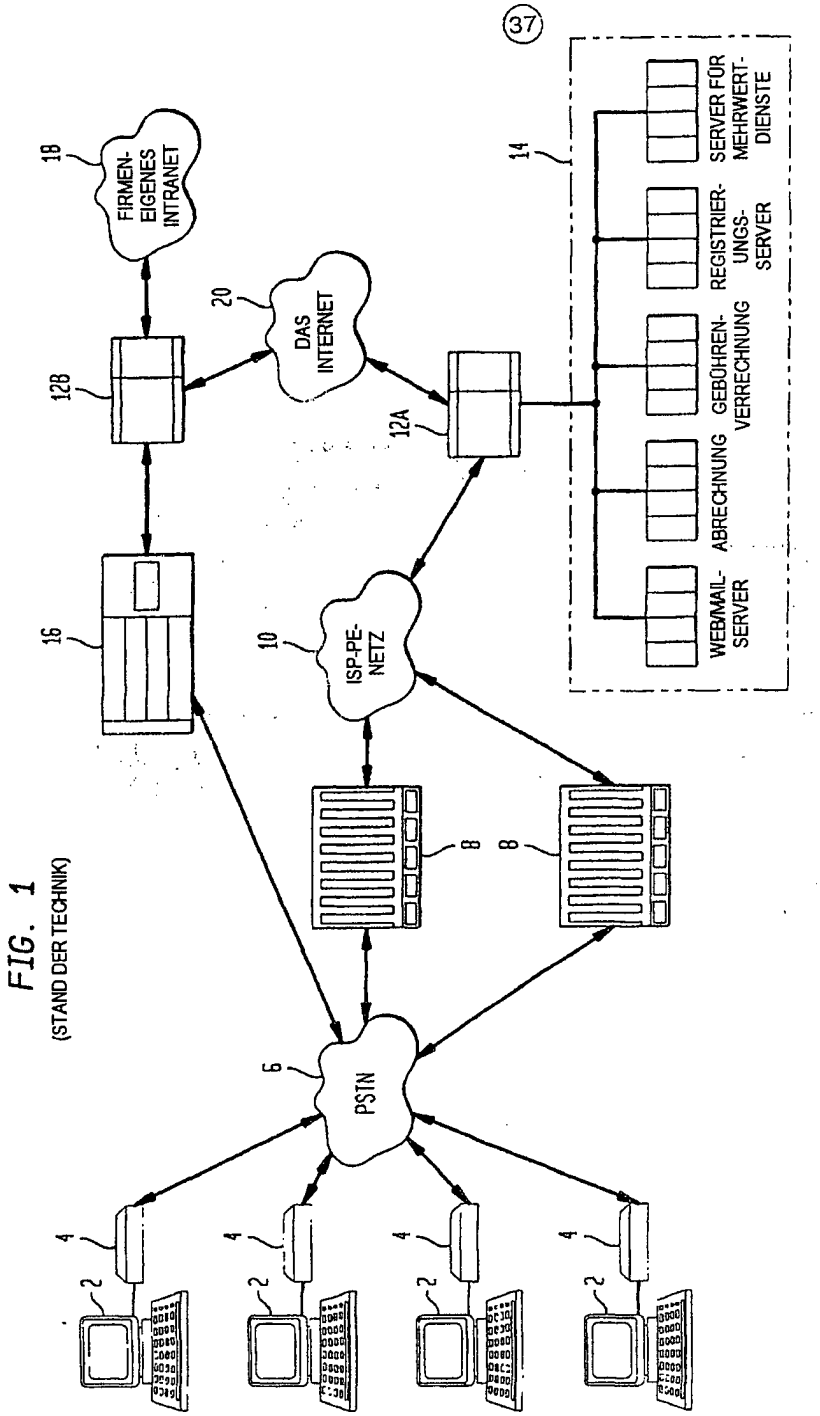


FIG. 1
(STAND DER TECHNIK)

FIG. 2

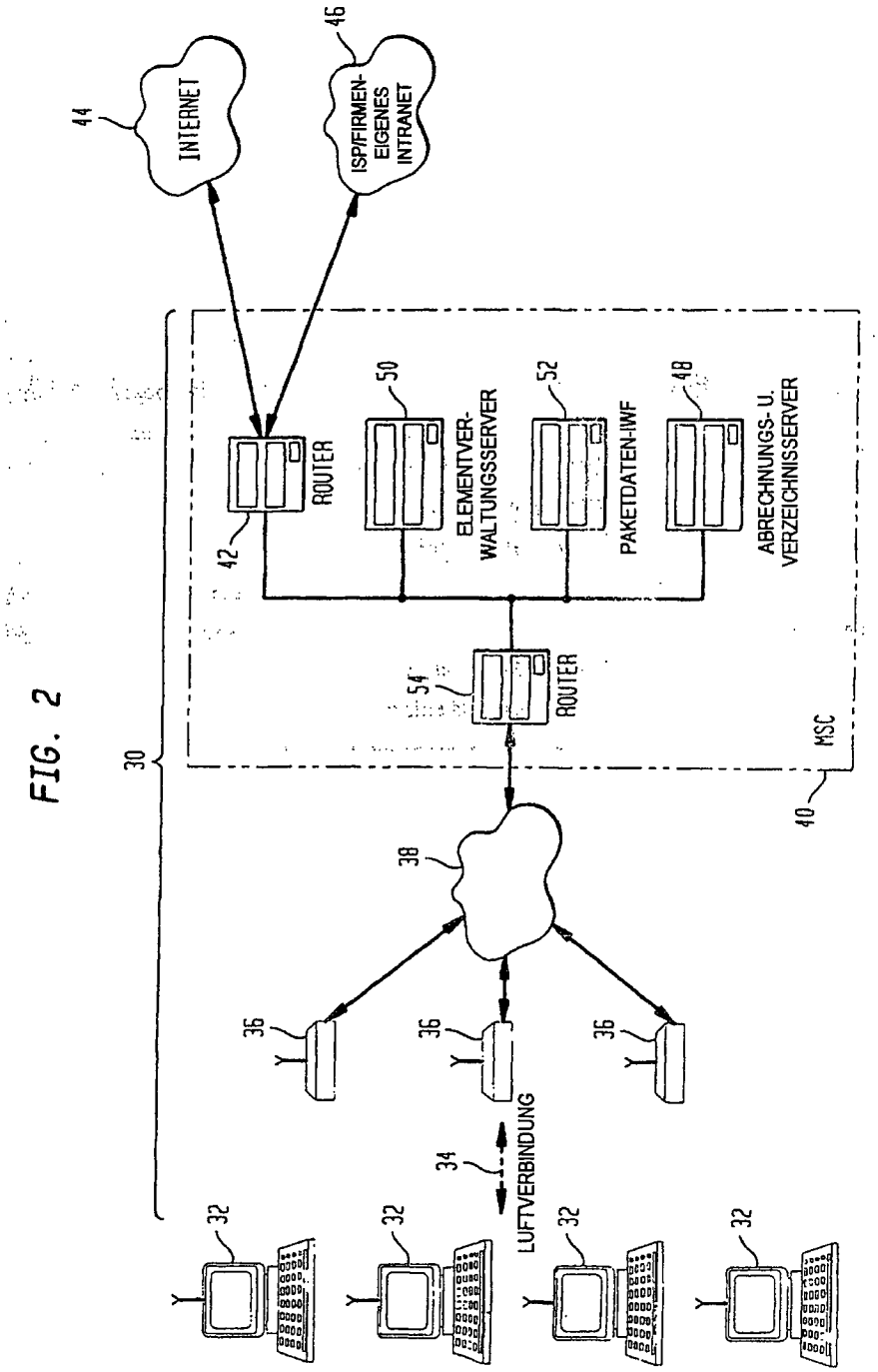

INTERNET
ISP/FIRMEN-EIGENES INTRANET
ROUTER
ELEMENTVERWALTUNGSSERVER
PAKETDATEN-IWF
ABRECHNUNGS- U. VERZEICHNISSERVER
ROUTER
MSC
LUFTVERBINDUNG
30
34
36
38
40
42
44
46
48
50
52
54

FIG. 3

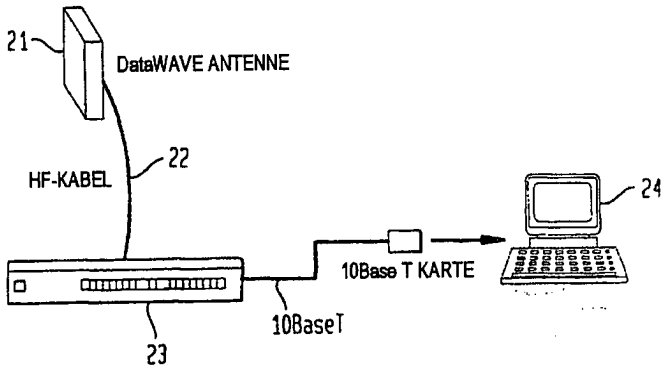


FIG. 4

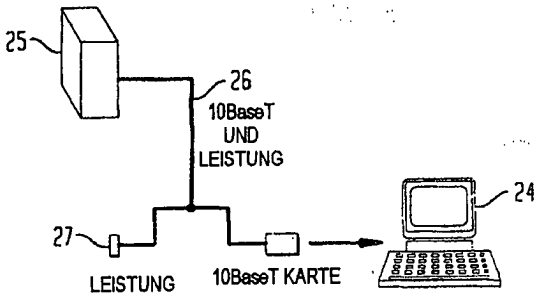


FIG. 5

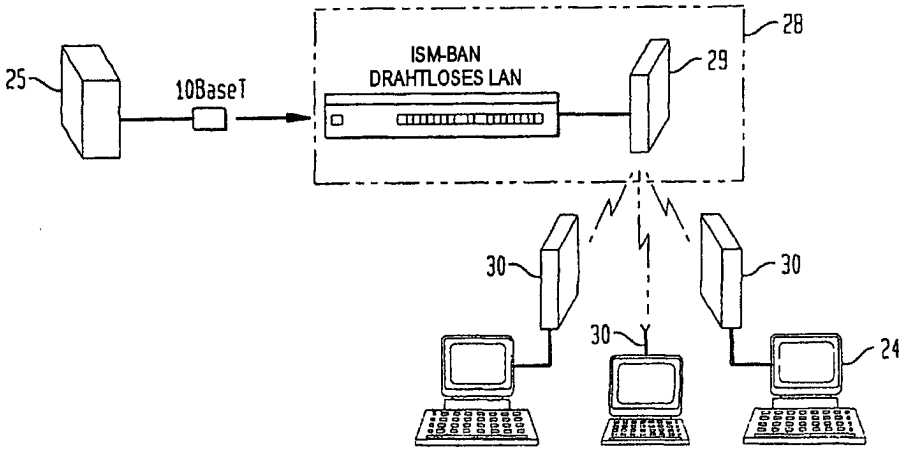


FIG. 6

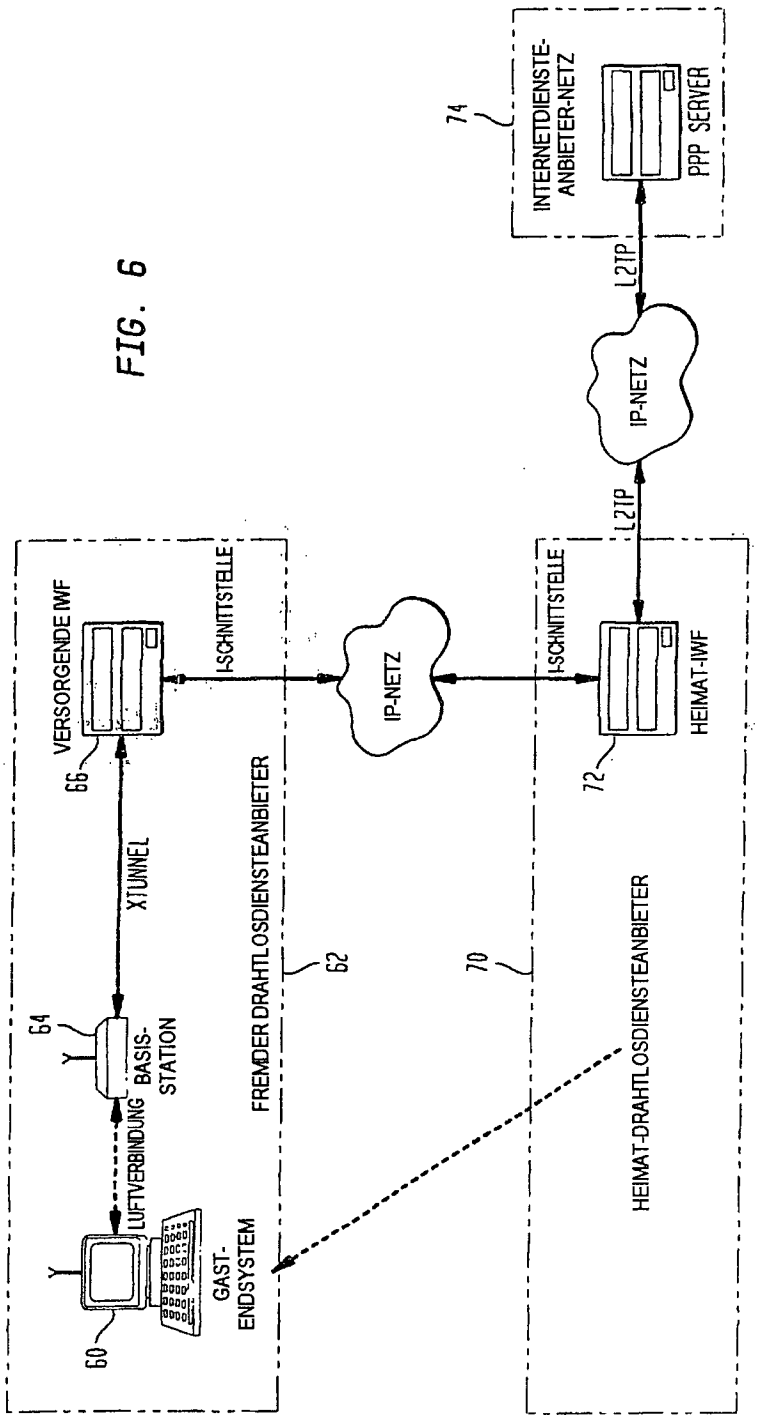

INTERNETDIENSTE-ANBIETER-NETZ
PPP SERVER
74
L2TP
IP-NETZ
L2TP
I-SCHNITTSTELLE
VERSORGENDE IWF
66
I-SCHNITTSTELLE
IP-NETZ
HEIMAT-IWF
72
XTUNNEL
64
BASIS-STATION
LUFTVERBINDUNG
FREMDER DRAHTLOSDIENSTEANBIETER
62
70
HEIMAT-DRAHTLOSDIENSTEANBIETER
GAST-ENDSYSTEM
60

FIG. 7

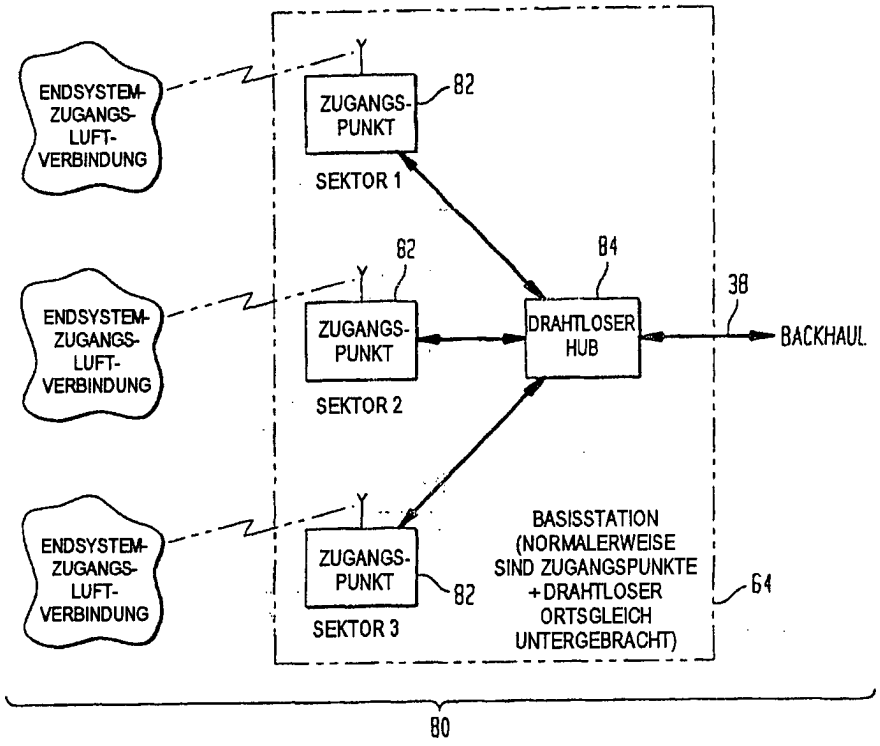

ENDSYSTEM-ZUGANGS-LUFT-VERBINDUNG
ENDSYSTEM-ZUGANGS-LUFT-VERBINDUNG
ENDSYSTEM-ZUGANGS-LUFT-VERBINDUNG
ZUGANGS-PUNKT
82
SEKTOR 1
ZUGANGS-PUNKT
82
SEKTOR 2
ZUGANGS-PUNKT
82
SEKTOR 3
84
DRAHTLOSER HUB
38
BACKHAUL
BASISSTATION (NORMALERWEISE SIND ZUGANGSPUNKTE + DRAHTLOSER ORTSGLEICH UNTERGEBRACHT)
64
80

FIG. 8

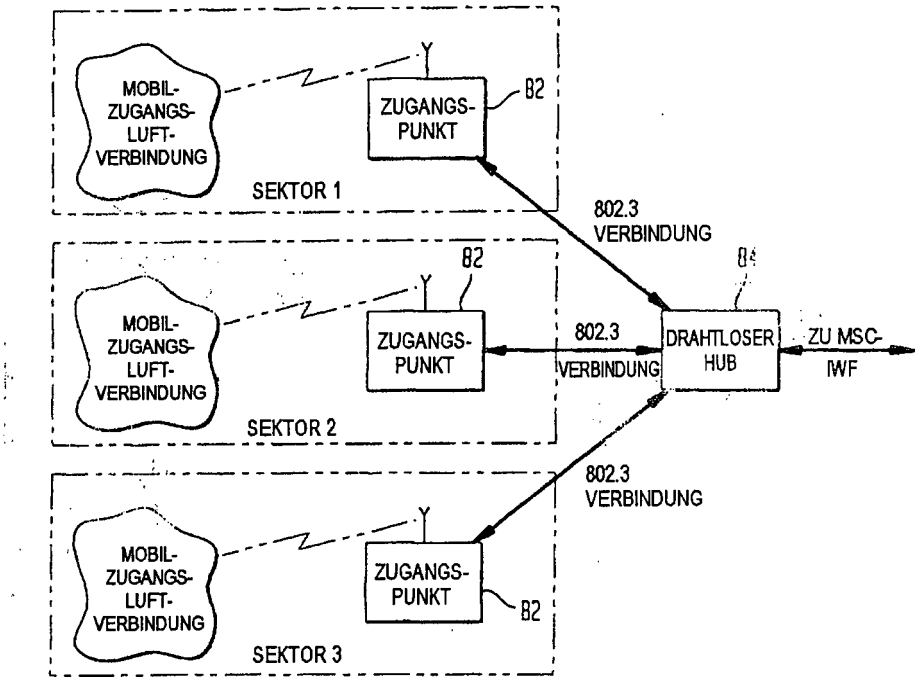

MOBIL-
ZUGANGS-
LUFT-
VERBINDUNG
SEKTOR 1
ZUGANGS-
PUNKT
82
802.3
VERBINDUNG
MOBIL-
ZUGANGS-
LUFT-
VERBINDUNG
SEKTOR 2
82
ZUGANGS-
PUNKT
802.3
VERBINDUNG
DRAHTLOSER
HUB
ZU MSC-
IWF
802.3
VERBINDUNG
MOBIL-
ZUGANGS-
LUFT-
VERBINDUNG
SEKTOR 3
ZUGANGS-
PUNKT
82

FIG. 9

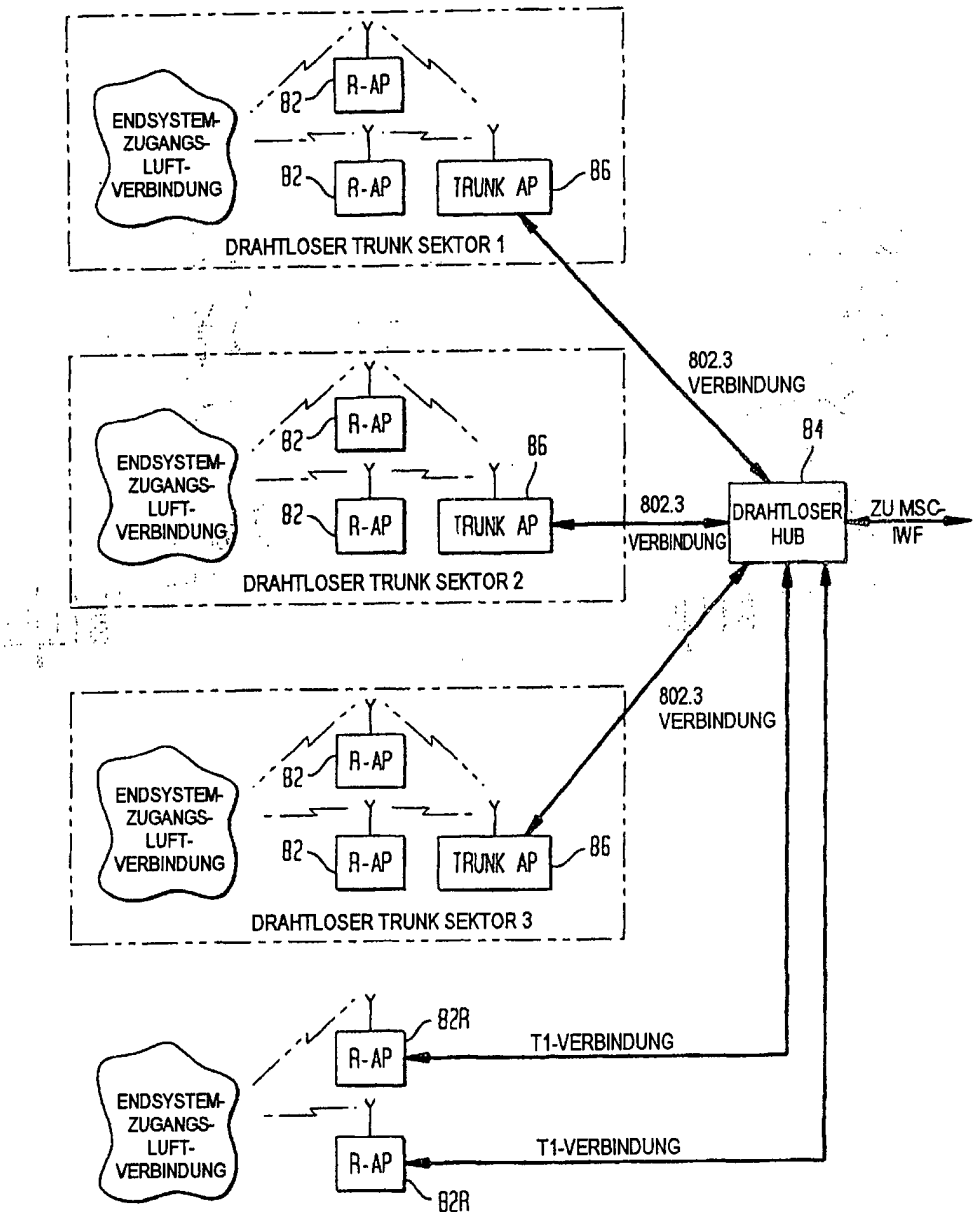

ENDSYSTEM-ZUGANGS-LUFT-VERBINDUNG
R-AP
82
TRUNK AP
86
DRAHTLOSER TRUNK SEKTOR 1
802.3 VERBINDUNG
84
DRAHTLOSER HUB
ZU MSC-IWF
DRAHTLOSER TRUNK SEKTOR 2
DRAHTLOSER TRUNK SEKTOR 3
82R
T1-VERBINDUNG

FIG. 10

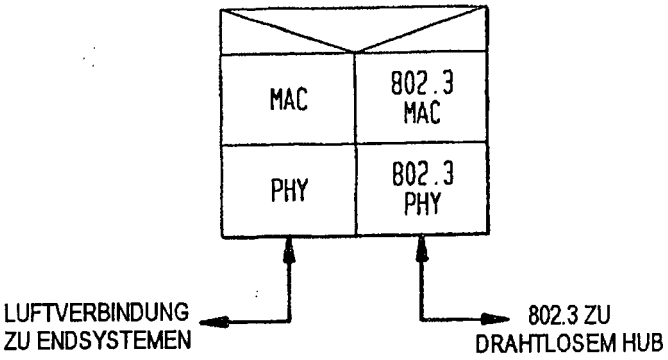


FIG. 11

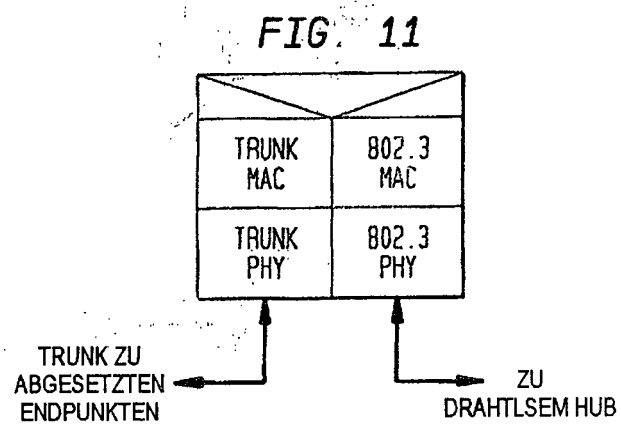


FIG. 12

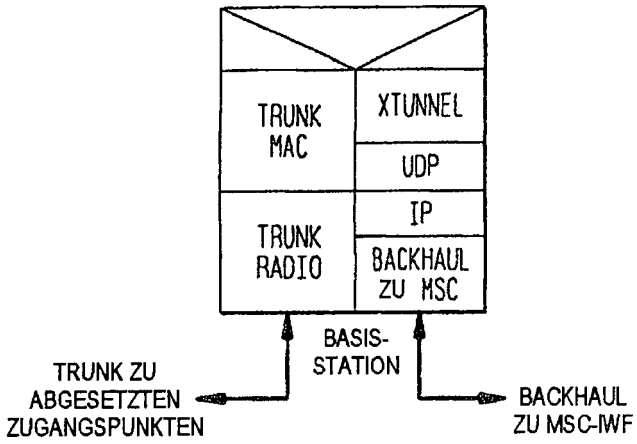


FIG. 13

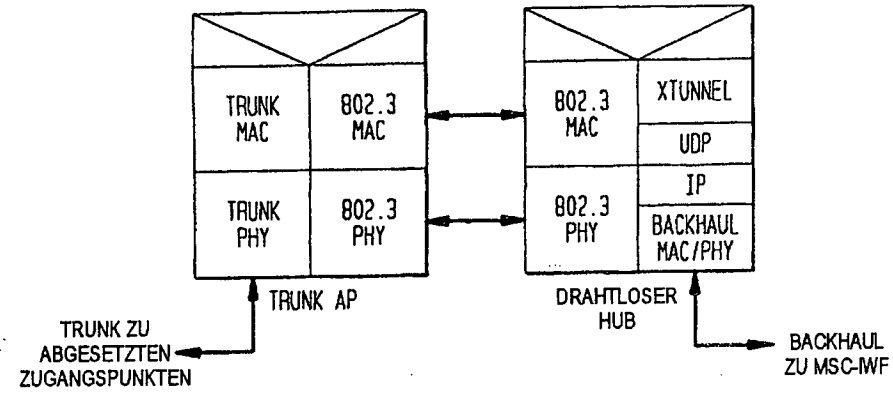

TRUNK MAC
802.3 MAC
TRUNK PHY
802.3 PHY
TRUNK AP
TRUNK ZU ABGESETZTEN ZUGANGSPUNKTEN
802.3 MAC
XTUNNEL
UDP
IP
802.3 PHY
BACKHAUL MAC/PHY
DRAHTLOSER HUB
BACKHAUL ZU MSC-IWF

FIG. 14

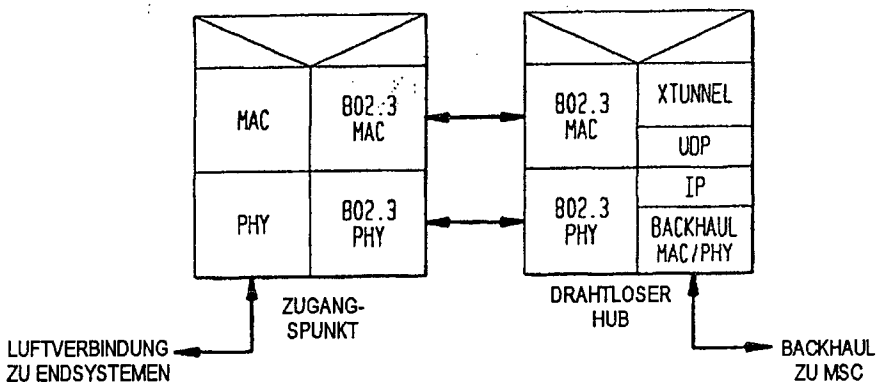

MAC
802.3 MAC
PHY
802.3 PHY
ZUGANG-SPUNKT
LUFTVERBINDUNG ZU ENDSYSTEMEN
802.3 MAC
XTUNNEL
UDP
IP
802.3 PHY
BACKHAUL MAC/PHY
DRAHTLOSER HUB
BACKHAUL ZU MSC

FIG. 15

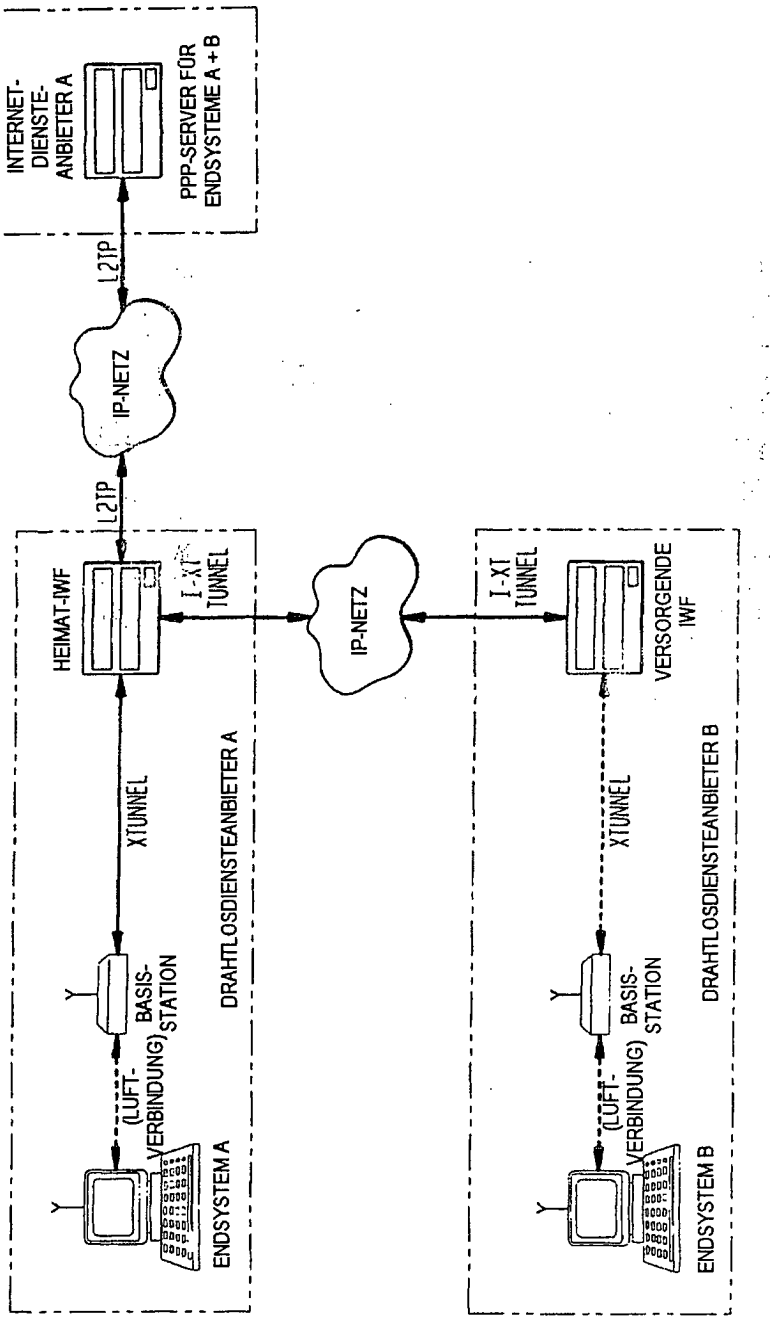

INTERNET-DIENSTE-ANBIETER A
PPP-SERVER FÜR ENDSYSTEME A + B
L2TP
IP-NETZ
L2TP
HEIMAT-IWF
I-XT TUNNEL
IP-NETZ
I-XT TUNNEL
VERSORGENDE IWF
XTUNNEL
XTUNNEL
BASIS-STATION
(LUFT-VERBINDUNG)
BASIS-STATION
(LUFT-VERBINDUNG)
DRAHTLOSDIENSTEANBIETER A
DRAHTLOSDIENSTEANBIETER B
ENDSYSTEM A
ENDSYSTEM B

FIG. 16

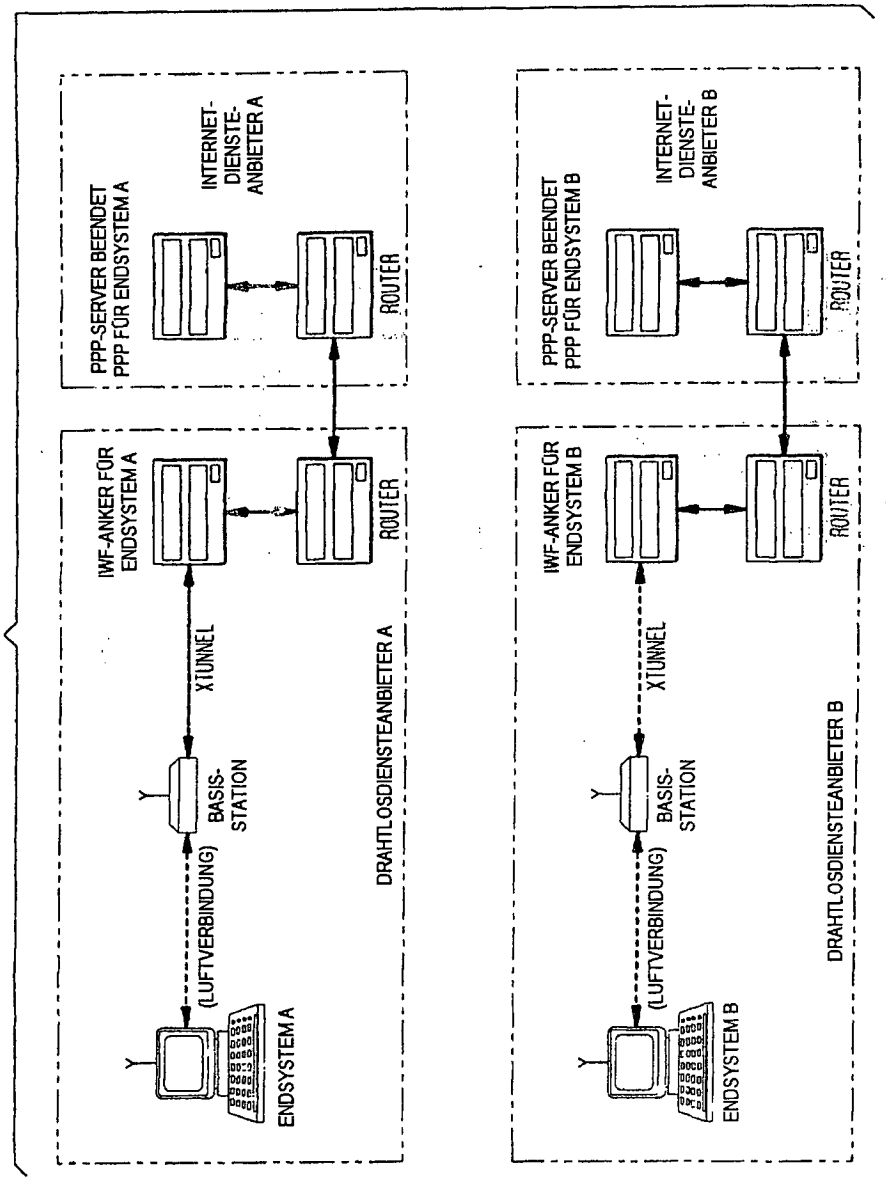

PPP-SERVER BEENDET PPP FÜR ENDSYSTEM A
INTERNET-DIENSTE-ANBIETER A
ROUTER
IWF-ANKER FÜR ENDSYSTEM A
ROUTER
XTUNNEL
BASIS-STATION
(LUFTVERBINDUNG)
ENDSYSTEM A
DRAHTLOSDIENSTEANBIETER A
PPP-SERVER BEENDET PPP FÜR ENDSYSTEM B
INTERNET-DIENSTE-ANBIETER B
ROUTER
IWF-ANKER FÜR ENDSYSTEM B
ROUTER
XTUNNEL
BASIS-STATION
(LUFTVERBINDUNG)
ENDSYSTEM B
DRAHTLOSDIENSTEANBIETER B

FIG. 17

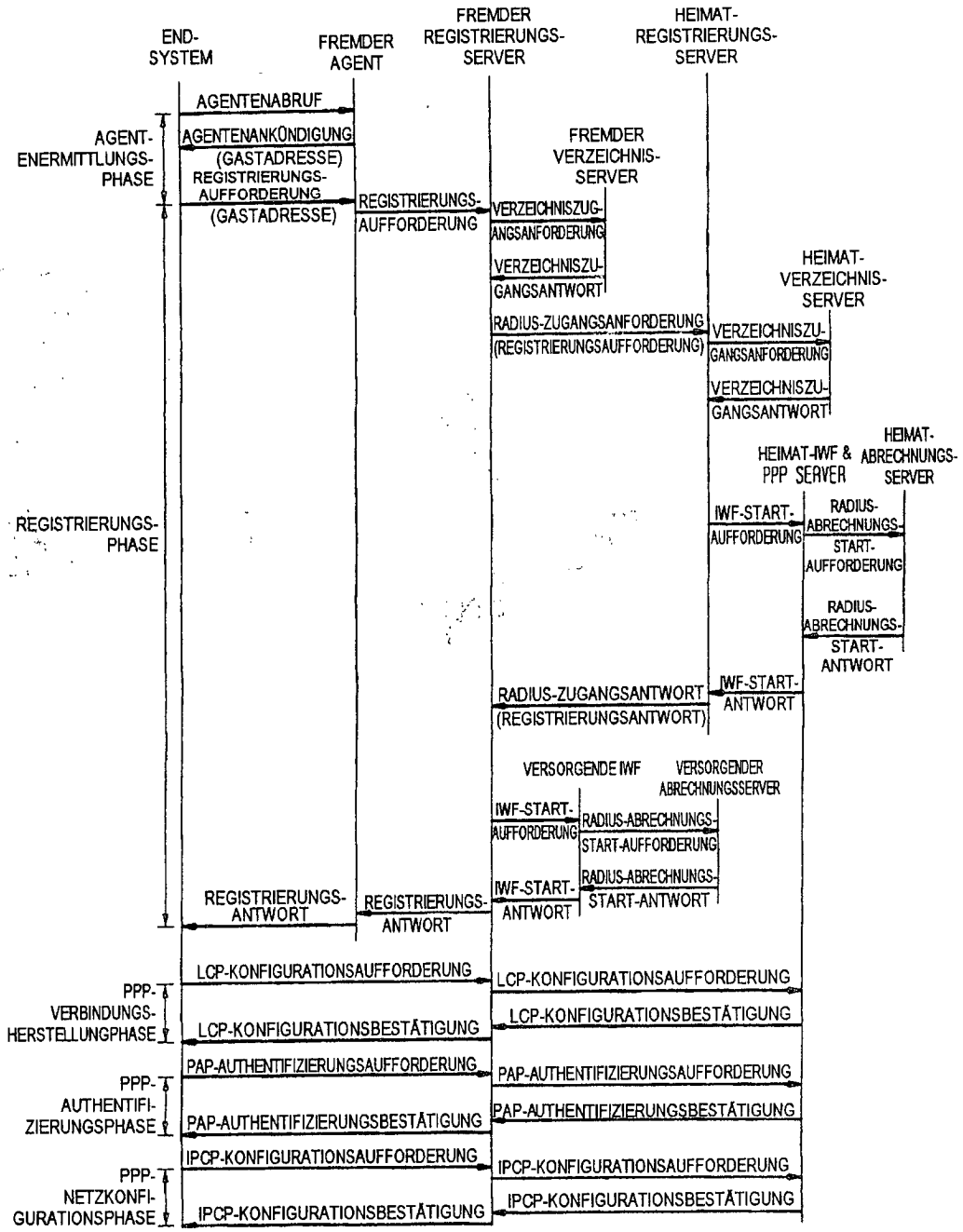

END-SYSTEM
FREMDER AGENT
FREMDER REGISTRIERUNGS-SERVER
HEIMAT-REGISTRIERUNGS-SERVER
FREMDER VERZEICHNIS-SERVER
HEIMAT-VERZEICHNIS-SERVER
HEIMAT-IWF & PPP SERVER
HEIMAT-ABRECHNUNGS-SERVER
VERSORGENDE IWF
VERSORGENDER ABRECHNUNGSSERVER
AGENTENABRUF
AGENTENANKÜNDIGUNG
(GASTADRESSE)
REGISTRIERUNGS-AUFFORDERUNG
(GASTADRESSE)
REGISTRIERUNGS-AUFFORDERUNG
VERZEICHNISZUGANGSANFORDERUNG
VERZEICHNISZUGANGSANTWORT
RADIUS-ZUGANGSANFORDERUNG
(REGISTRIERUNGSAUFFORDERUNG)
VERZEICHNISZUGANGSANFORDERUNG
VERZEICHNISZUGANGSANTWORT
IWF-START-AUFFORDERUNG
RADIUS-ABRECHNUNGS-START-AUFFORDERUNG
RADIUS-ABRECHNUNGS-START-ANTWORT
IWF-START-ANTWORT
RADIUS-ZUGANGSANTWORT
(REGISTRIERUNGSANTWORT)
IWF-START-AUFFORDERUNG
RADIUS-ABRECHNUNGS-START-AUFFORDERUNG
IWF-START-ANTWORT
RADIUS-ABRECHNUNGS-START-ANTWORT
REGISTRIERUNGS-ANTWORT
REGISTRIERUNGS-ANTWORT
LCP-KONFIGURATIONSAUFFORDERUNG
LCP-KONFIGURATIONSAUFFORDERUNG
LCP-KONFIGURATIONSBESTÄTIGUNG
LCP-KONFIGURATIONSBESTÄTIGUNG
PAP-AUTHENTIFIZIERUNGSAUFFORDERUNG
PAP-AUTHENTIFIZIERUNGSAUFFORDERUNG
PAP-AUTHENTIFIZIERUNGSBESTÄTIGUNG
PAP-AUTHENTIFIZIERUNGSBESTÄTIGUNG
IPCP-KONFIGURATIONSAUFFORDERUNG
IPCP-KONFIGURATIONSAUFFORDERUNG
IPCP-KONFIGURATIONSBESTÄTIGUNG
IPCP-KONFIGURATIONSBESTÄTIGUNG
AGENT-ENERMITTLUNGS-PHASE
REGISTRIERUNGS-PHASE
PPP-VERBINDUNGS-HERSTELLUNGPHASE
PPP-AUTHENTIFI-ZIERUNGSPHASE
PPP-NETZKONFI-GURATIONSPHASE

FIG. 18

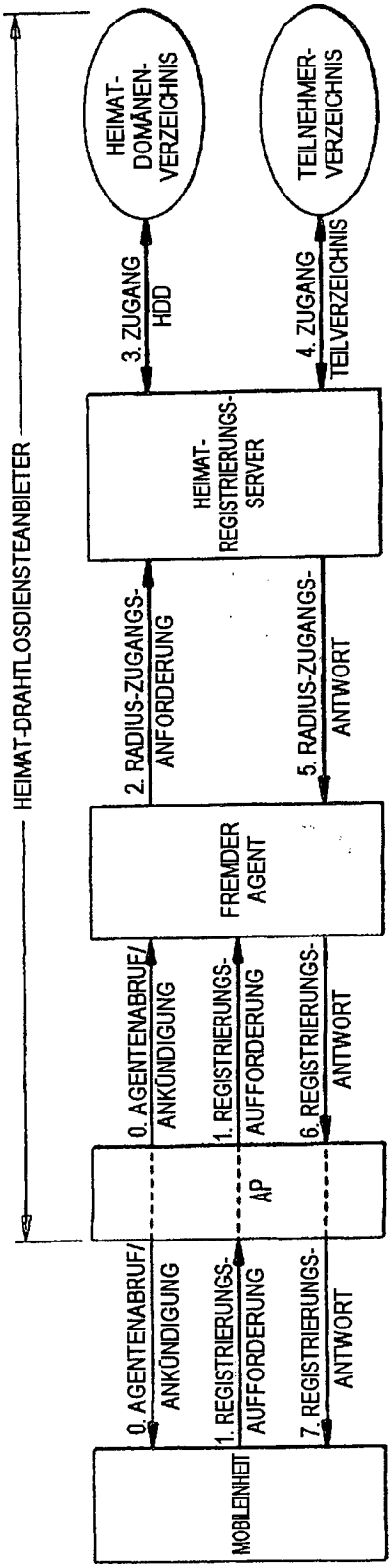
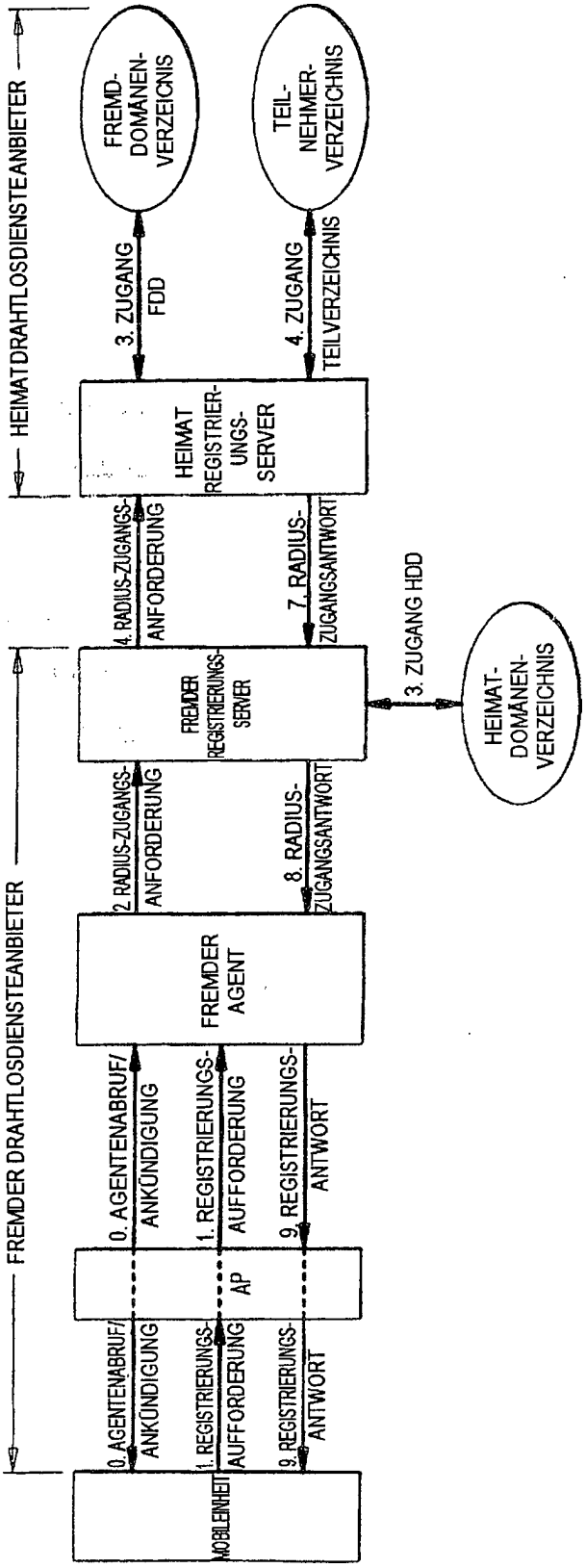

HEIMAT-DRAHTLOSDIENSTEANBIETER
HEIMAT-DOMÄNEN-VERZEICHNIS
TEILNEHMER-VERZEICHNIS
3. ZUGANG HDD
4. ZUGANG TEILVERZEICHNIS
HEIMAT-REGISTRIERUNGS-SERVER
2. RADIUS-ZUGANGS-ANFORDERUNG
5. RADIUS-ZUGANGS-ANTWORT
FREMDER AGENT
0. AGENTENABRUF/ ANKÜNDIGUNG
1. REGISTRIERUNGS-AUFFORDERUNG
6. REGISTRIERUNGS-ANTWORT
AP
0. AGENTENABRUF/ ANKÜNDIGUNG
1. REGISTRIERUNGS-AUFFORDERUNG
7. REGISTRIERUNGS-ANTWORT
MOBILEINHEIT

FIG. 19


HEIMATDRAHTLOSDIENSTEANBIETER
FREMDER DRAHTLOSDIENSTEANBIETER
FREMD-DOMÄNEN-VERZEICHNIS
TEIL-NEHMER-VERZEICHNIS
HEIMAT-DOMÄNEN-VERZEICHNIS
HEIMAT REGISTRIER-UNGS-SERVER
FREMDER REGISTRIERUNGS-SERVER
FREMDER AGENT
AP
MOBILEINHEIT
3. ZUGANG FDD
4. ZUGANG TEILVERZEICHNIS
3. ZUGANG HDD
4. RADIUS-ZUGANGS-ANFORDERUNG
7. RADIUS-ZUGANGSANTWORT
2. RADIUS-ZUGANGS-ANFORDERUNG
8. RADIUS-ZUGANGSANTWORT
0. AGENTENABRUF/ ANKÜNDIGUNG
1. REGISTRIERUNGS-AUFFORDERUNG
9. REGISTRIERUNGS-ANTWORT
0. AGENTENABRUF/ ANKÜNDIGUNG
1. REGISTRIERUNGS-AUFFORDERUNG
9. REGISTRIERUNGS-ANTWORT

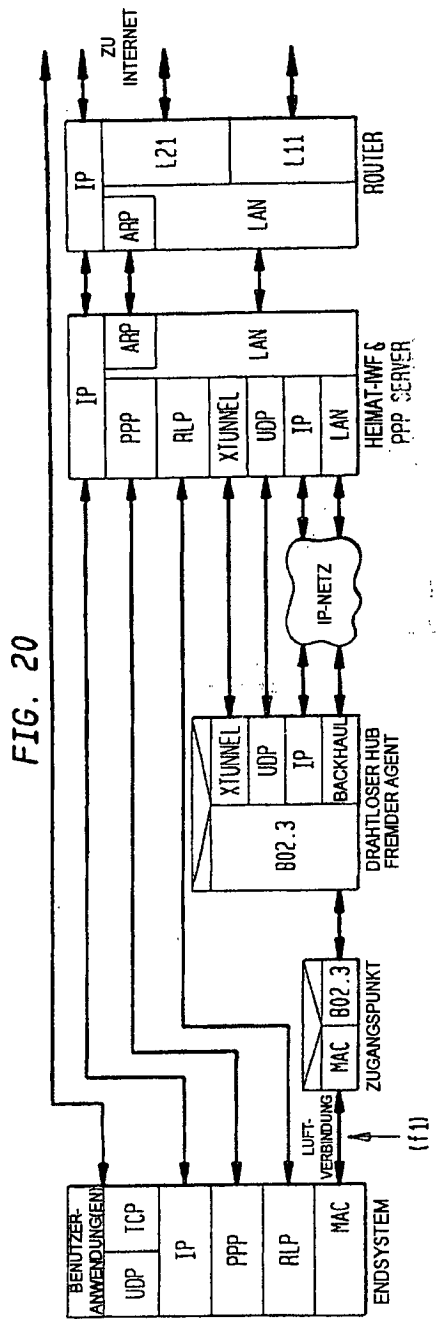

ZU INTERNET
IP
ARP
L21
L11
LAN
ROUTER
IP
ARP
PPP
RLP
XTUNNEL
UDP
IP
LAN
HEIMAT-IWF & PPP SERVER
IP-NETZ
XTUNNEL
UDP
IP
BACKHAUL
802.3
DRAHTLOSER HUB FREMDER AGENT
802.3
MAC
ZUGANGSPUNKT
LUFT-VERBINDUNG
(f1)
BENUTZER-ANWENDUNGEN
UDP
TCP
IP
PPP
RLP
MAC
ENDSYSTEM

FIG. 20

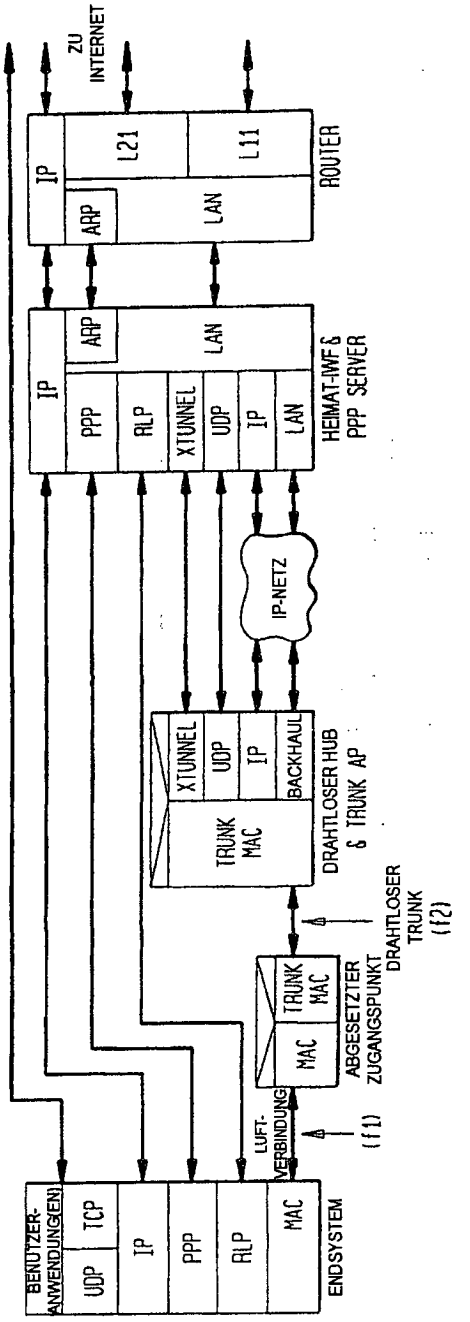

ZU INTERNET
IP
ARP
L21
L11
LAN
ROUTER
IP
ARP
PPP
RLP
XTUNNEL
UDP
IP
LAN
HEIMAT-IWF & PPP SERVER
IP-NETZ
XTUNNEL
UDP
IP
BACKHAUL
TRUNK MAC
DRAHTLOSER HUB & TRUNK AP
TRUNK MAC
MAC
ABGESETZTER ZUGANGSPUNKT
DRAHTLOSER TRUNK
(f2)
LUFT-VERBINDUNG
(f1)
BENUTZER-ANWENDUNGEN
UDP
TCP
IP
PPP
RLP
MAC
ENDSYSTEM

FIG. 21

FIG. 22

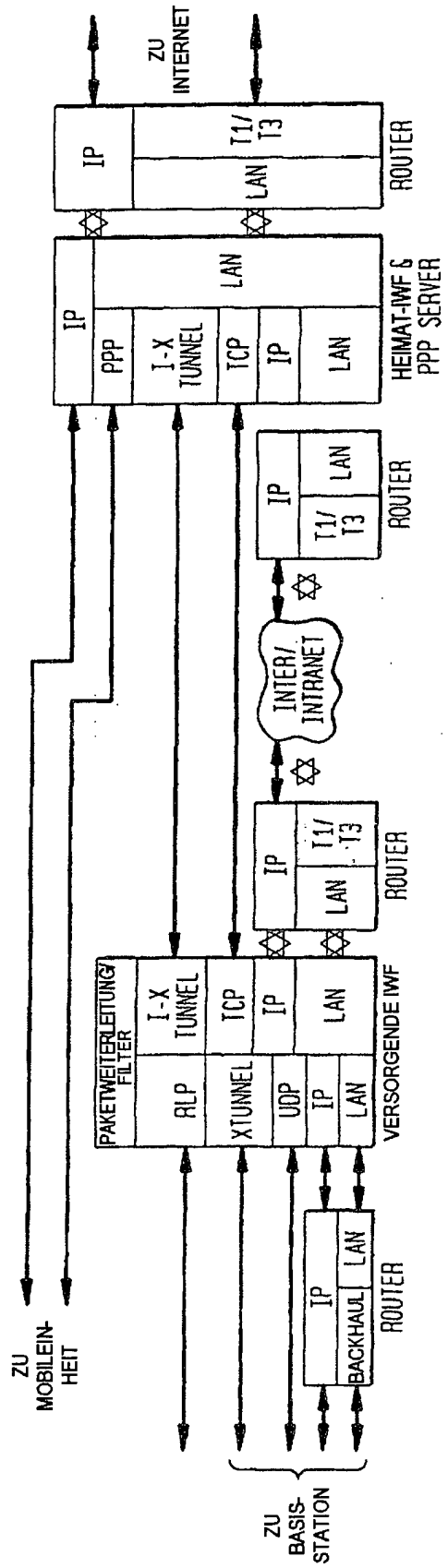

ZU INTERNET
IP
T1/ T3
LAN
ROUTER
IP
LAN
PPP
I-X TUNNEL
TCP
IP
LAN
HEIMAT-IWF & PPP SERVER
IP
LAN
T1/ T3
ROUTER
INTER/ INTRANET
IP
T1/ T3
LAN
ROUTER
PAKETWEITERLEITUNG/ FILTER
I-X TUNNEL
TCP
IP
LAN
ALP
XTUNNEL
UDP
IP
LAN
VERSORGENDE IWF
IP
LAN
BACKHAUL
ROUTER
ZU MOBILEIN-HEIT
ZU BASIS-STATION

FIG. 23

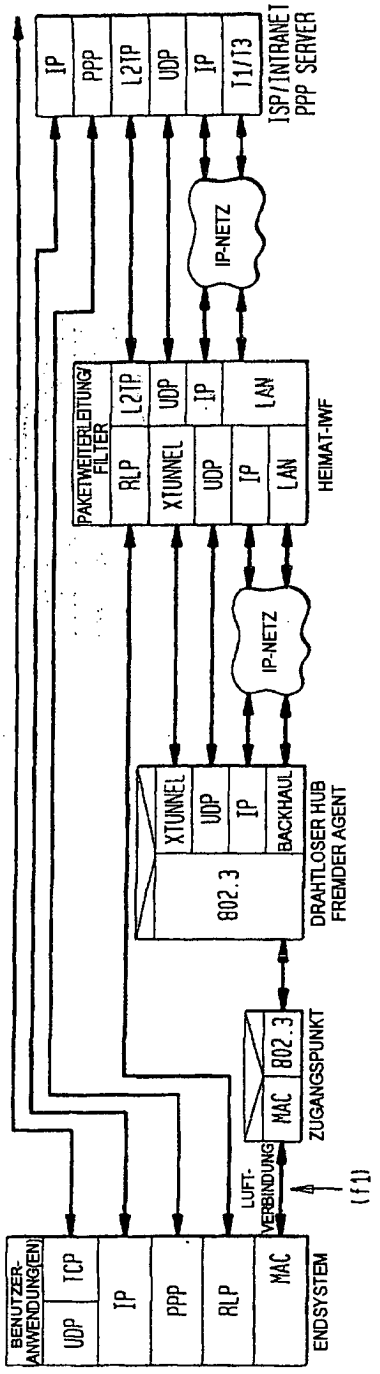
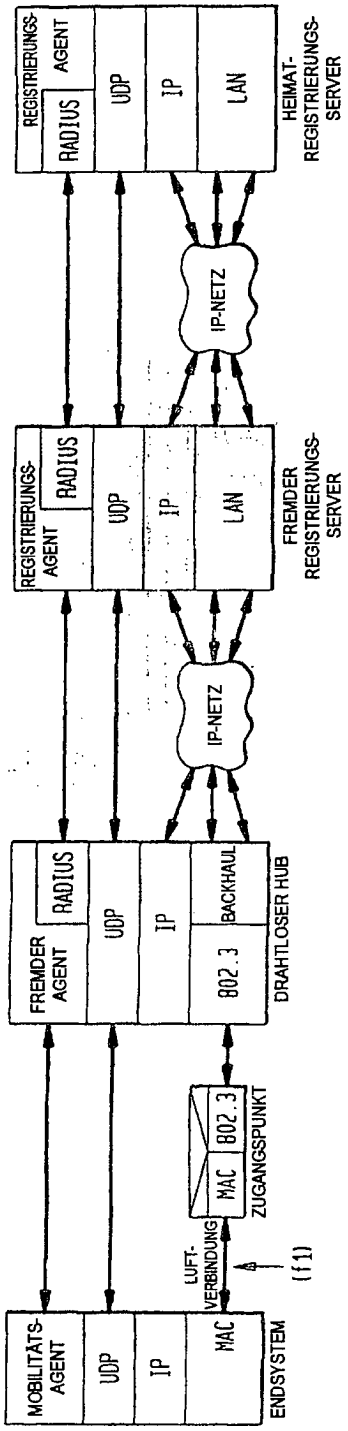

BENUTZER-ANWENDUNG(EN)
UDP
TCP
IP
PPP
RLP
MAC
ENDSYSTEM
LUFT-VERBINDUNG
(f1)
802.3
MAC
ZUGANGSPUNKT
XTUNNEL
UDP
IP
BACKHAUL
802.3
DRAHTLOSER HUB
FREMDER AGENT
IP-NETZ
PAKETWEITERLEITUNG/ FILTER
RLP
L2TP
XTUNNEL
UDP
IP
LAN
HEIMAT-IWF
IP-NETZ
IP
PPP
L2TP
UDP
IP
T1/I3
ISP/INTRANET PPP SERVER

FIG. 24


MOBILITÄTS-AGENT
UDP
IP
MAC
ENDSYSTEM
LUFT-VERBINDUNG
(f1)
802.3
MAC
ZUGANGSPUNKT
FREMDER AGENT
RADIUS
UDP
IP
BACKHAUL
802.3
DRAHTLOSER HUB
IP-NETZ
REGISTRIERUNGS-AGENT
RADIUS
UDP
IP
LAN
FREMDER REGISTRIERUNGS-SERVER
IP-NETZ
REGISTRIERUNGS-AGENT
RADIUS
UDP
IP
LAN
HEIMAT-REGISTRIERUNGS-SERVER

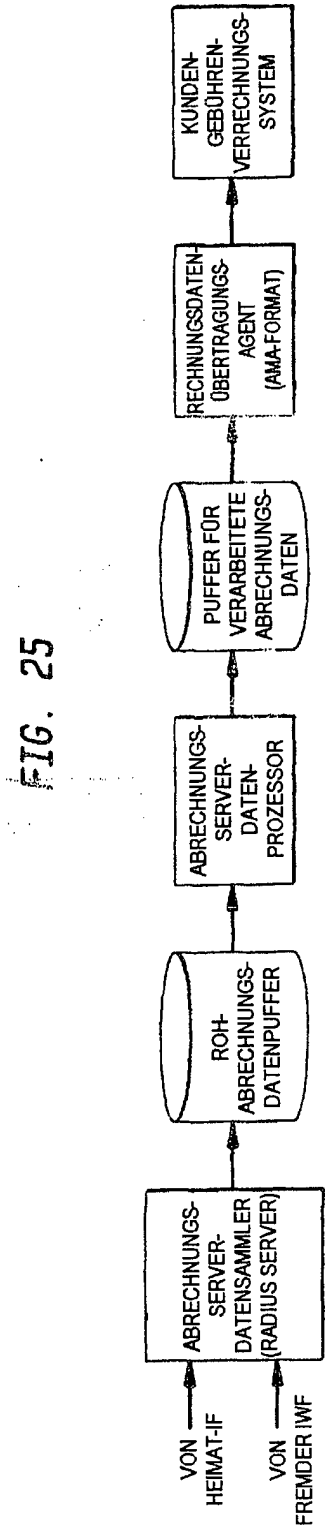
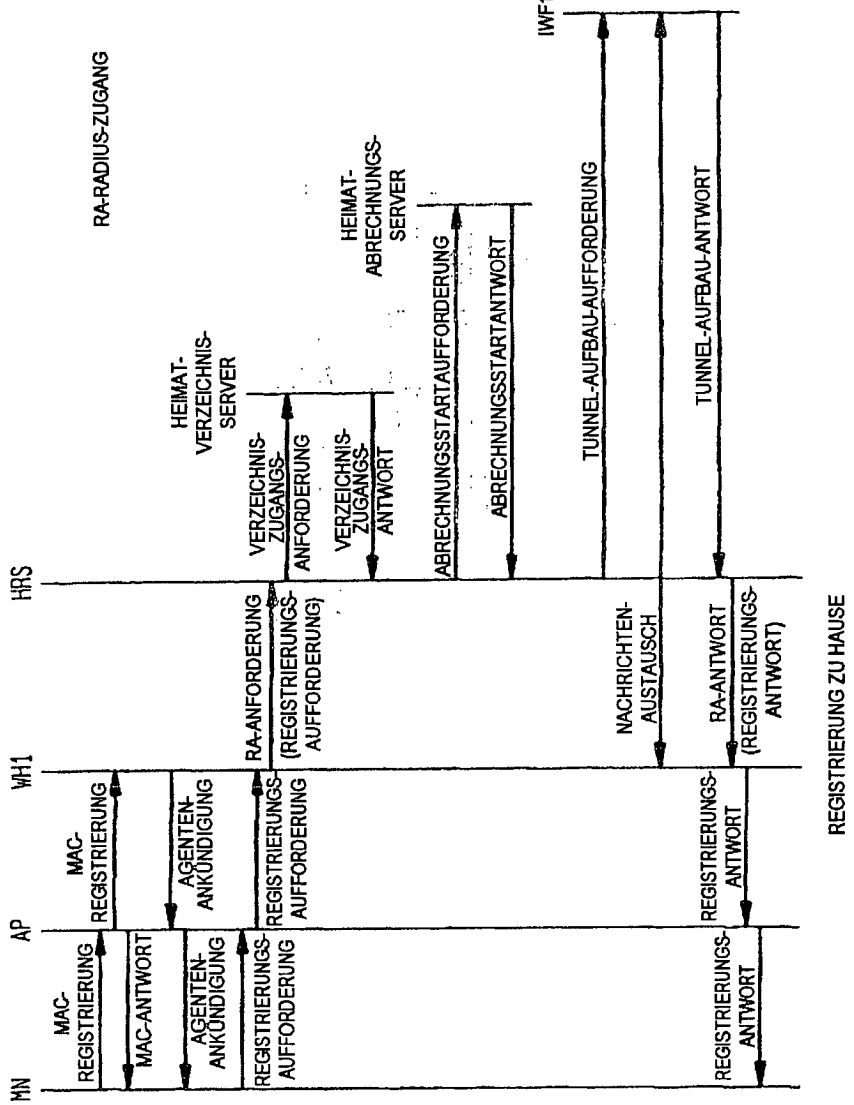

VON HEIMAT-IF
VON FREMDER IWF
ABRECHNUNGS-SERVER-DATENSAMMLER (RADIUS SERVER)
ROH-ABRECHNUNGS-DATENPUFFER
ABRECHNUNGS-SERVER-DATEN-PROZESSOR
PUFFER FÜR VERARBEITETE ABRECHNUNGS-DATEN
RECHNUNGSDATEN-ÜBERTRAGUNGS-AGENT (AMA-FORMAT)
KUNDEN-GEBÜHREN-VERRECHNUNGS-SYSTEM

FIG. 25

FIG. 26


MN
AP
WH1
HRS
IWF1
RA-RADIUS-ZUGANG
HEIMAT-VERZEICHNIS-SERVER
HEIMAT-ABRECHNUNGS-SERVER
MAC-REGISTRIERUNG
MAC-ANTWORT
AGENTEN-ANKÜNDIGUNG
REGISTRIERUNGS-AUFFORDERUNG
RA-ANFORDERUNG (REGISTRIERUNGS-AUFFORDERUNG)
VERZEICHNIS-ZUGANGS-ANFORDERUNG
VERZEICHNIS-ZUGANGS-ANTWORT
ABRECHNUNGSSTARTAUFFORDERUNG
ABRECHNUNGSSTARTANTWORT
TUNNEL-AUFBAU-AUFFORDERUNG
TUNNEL-AUFBAU-ANTWORT
NACHRICHTEN-AUSTAUSCH
RA-ANTWORT (REGISTRIERUNGS-ANTWORT)
REGISTRIERUNGS-ANTWORT
REGISTRIERUNG ZU HAUSE

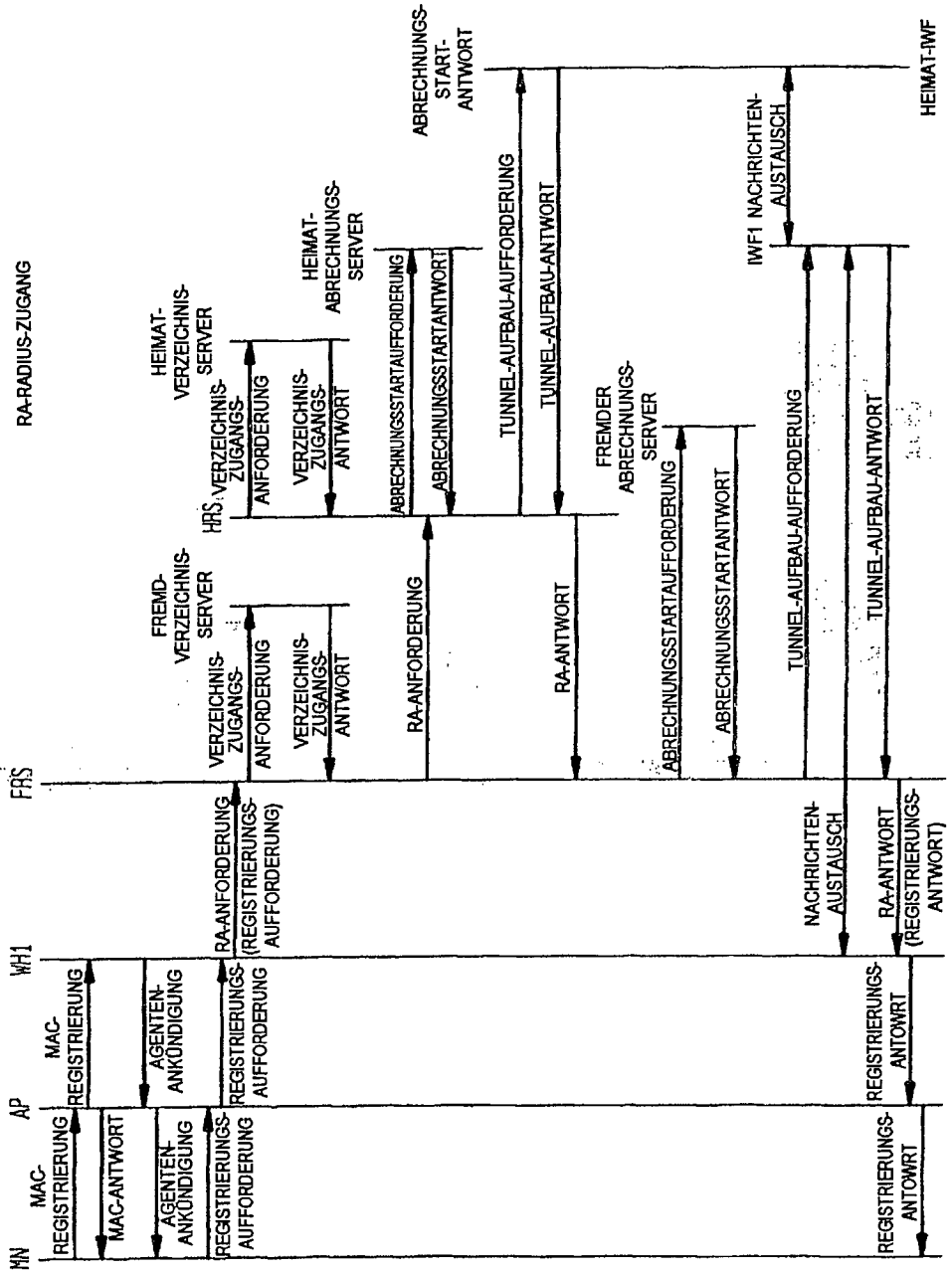

MN
AP
WH1
FRS
HRS
RA-RADIUS-ZUGANG
MAC-REGISTRIERUNG
MAC-ANTWORT
AGENTEN-ANKÜNDIGUNG
REGISTRIERUNGS-AUFFORDERUNG
RA-ANFORDERUNG (REGISTRIERUNGS-AUFFORDERUNG)
FREMD-VERZEICHNIS-SERVER
VERZEICHNIS-ZUGANGS-ANFORDERUNG
VERZEICHNIS-ZUGANGS-ANTWORT
HEIMAT-VERZEICHNIS-SERVER
VERZEICHNIS-ZUGANGS-ANFORDERUNG
VERZEICHNIS-ZUGANGS-ANTWORT
HEIMAT-ABRECHNUNGS-SERVER
RA-ANFORDERUNG
ABRECHNUNGSSTARTAUFFORDERUNG
ABRECHNUNGSSTARTANTWORT
ABRECHNUNGS-START-ANTWORT
TUNNEL-AUFBAU-AUFFORDERUNG
TUNNEL-AUFBAU-ANTWORT
RA-ANTWORT
FREMDER ABRECHNUNGS-SERVER
ABRECHNUNGSSTARTAUFFORDERUNG
ABRECHNUNGSSTARTANTWORT
IWF1 NACHRICHTEN-AUSTAUSCH
TUNNEL-AUFBAU-AUFFORDERUNG
TUNNEL-AUFBAU-ANTWORT
HEIMAT-IWF
NACHRICHTEN-AUSTAUSCH
RA-ANTWORT (REGISTRIERUNGS-ANTWORT)
REGISTRIERUNGS-ANTOWRT
REGISTRIERUNGS-ANTOWRT

FIG. 27

FIG. 28

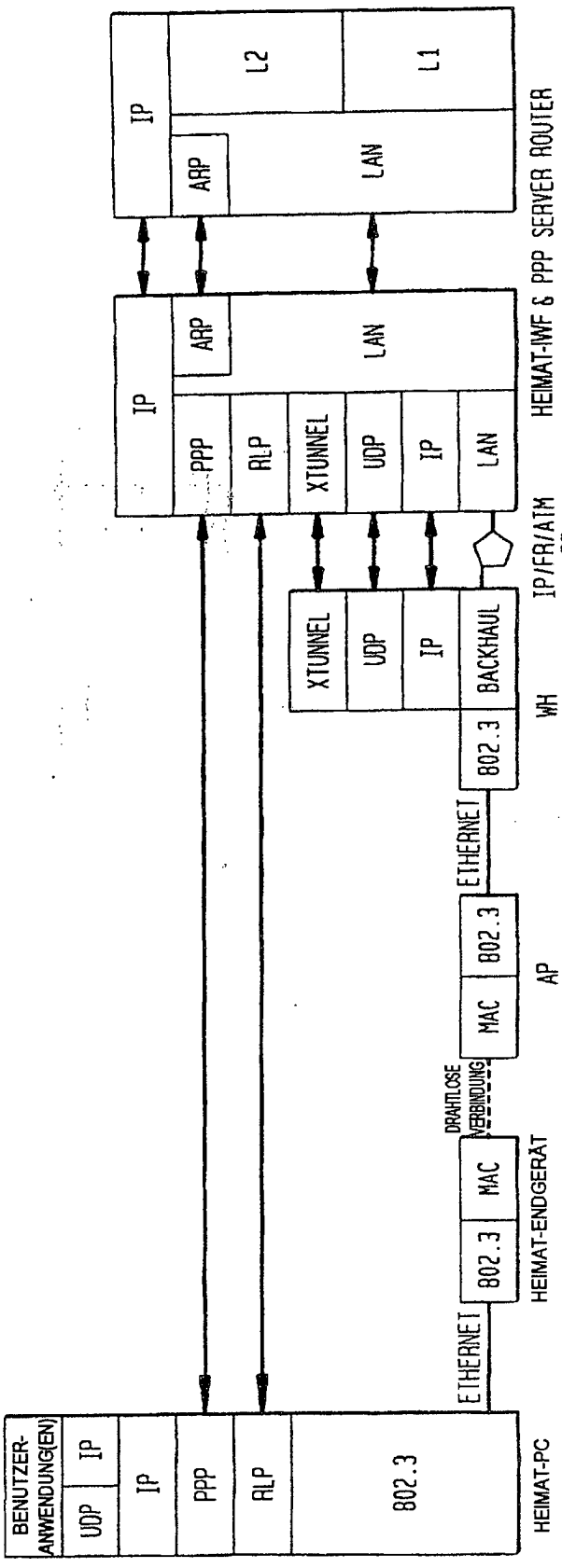

IP
L2
L1
ARP
LAN
HEIMAT-IWF & PPP SERVER ROUTER
PPP
RLP
XTUNNEL
UDP
IP
LAN
IP/FR/ATM NET
BACKHAUL
802.3
WH
ETHERNET
MAC
AP
DRAHTLOSE VERBINDUNG
HEIMAT-ENDGERÄT
BENUTZER-ANWENDUNG(EN)
HEIMAT-PC

FIG. 29

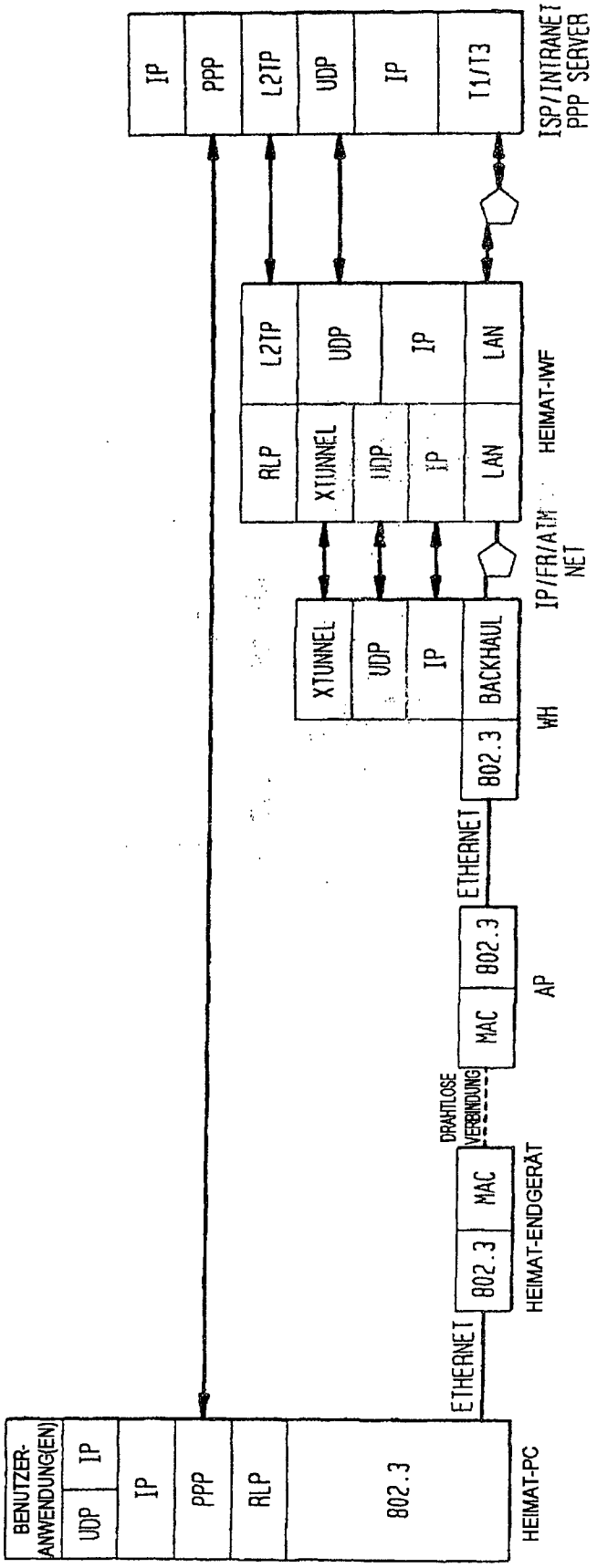

IP
PPP
L2TP
UDP
IP
T1/T3
ISP/INTRANET PPP SERVER
L2TP
UDP
IP
LAN
RLP
XTUNNEL
UDP
IP
LAN
HEIMAT-IWF
IP/FR/ATM NET
XTUNNEL
UDP
IP
BACKHAUL
802.3
WH
ETHERNET
802.3
MAC
AP
DRAHTLOSE VERBINDUNG
802.3
MAC
HEIMAT-ENDGERÄT
ETHERNET
BENUTZER-ANWENDUNG(EN)
UDP
IP
IP
PPP
RLP
802.3
HEIMAT-PC

FIG. 30

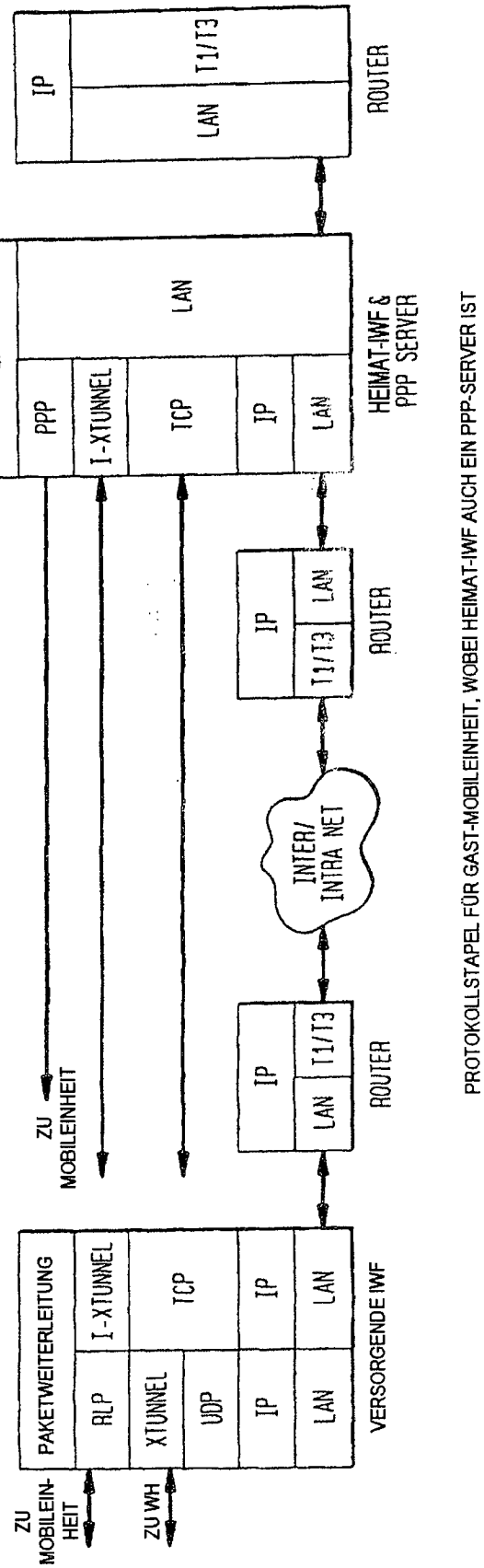

ZU MOBILEINHEIT
ZU WH
PAKETWEITERLEITUNG
RLP
I-XTUNNEL
XTUNNEL
UDP
TCP
IP
LAN
VERSORGENDE IWF
ROUTER
INTER/ INTRA NET
ROUTER
HEIMAT-IWF & PPP SERVER
PPP
ROUTER
T1/T3
PROTOKOLLSTAPEL FÜR GAST-MOBILEINHEIT, WOBEI HEIMAT-IWF AUCH EIN PPP-SERVER IST

FIG. 31

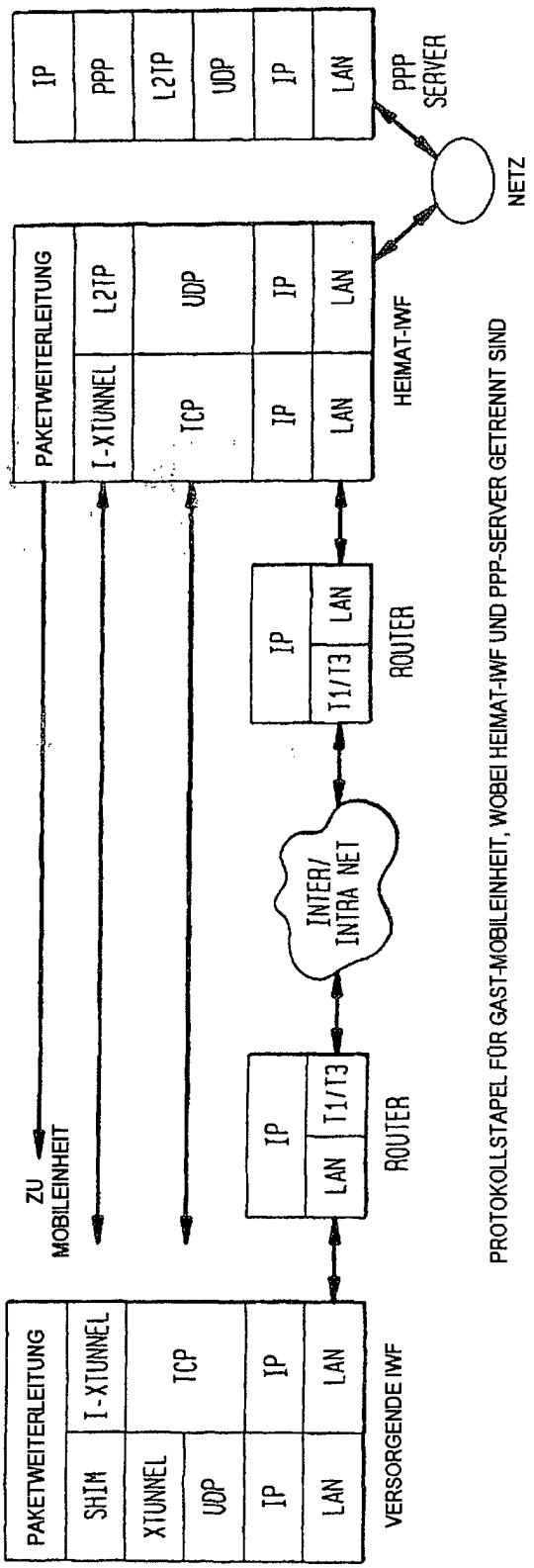

PAKETWEITERLEITUNG
SHIM
I-XTUNNEL
XTUNNEL
UDP
TCP
IP
IP
LAN
LAN
VERSORGENDE IWF
ROUTER
T1/T3
LAN
IP
INTER/
INTRA NET
ROUTER
T1/T3
LAN
IP
ZU
MOBILEINHEIT
PAKETWEITERLEITUNG
I-XTUNNEL
L2TP
TCP
UDP
IP
IP
LAN
LAN
HEIMAT-IWF
NETZ
IP
PPP
L2TP
UDP
IP
LAN
PPP
SERVER
PROTOKOLLSTAPEL FÜR GAST-MOBILEINHEIT, WOBEI HEIMAT-IWF UND PPP-SERVER GETRENNT SIND

FIG. 32

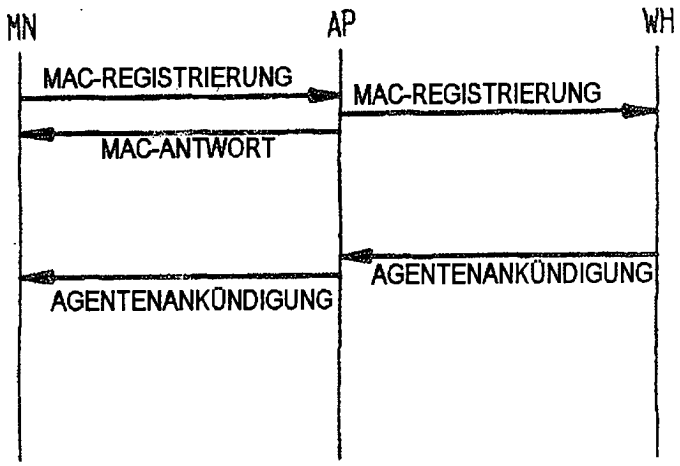

MN
AP
WH
MAC-REGISTRIERUNG
MAC-REGISTRIERUNG
MAC-ANTWORT
AGENTENANKÜNDIGUNG
AGENTENANKÜNDIGUNG
LOKALE WEITERSCHALTUNG

FIG. 33

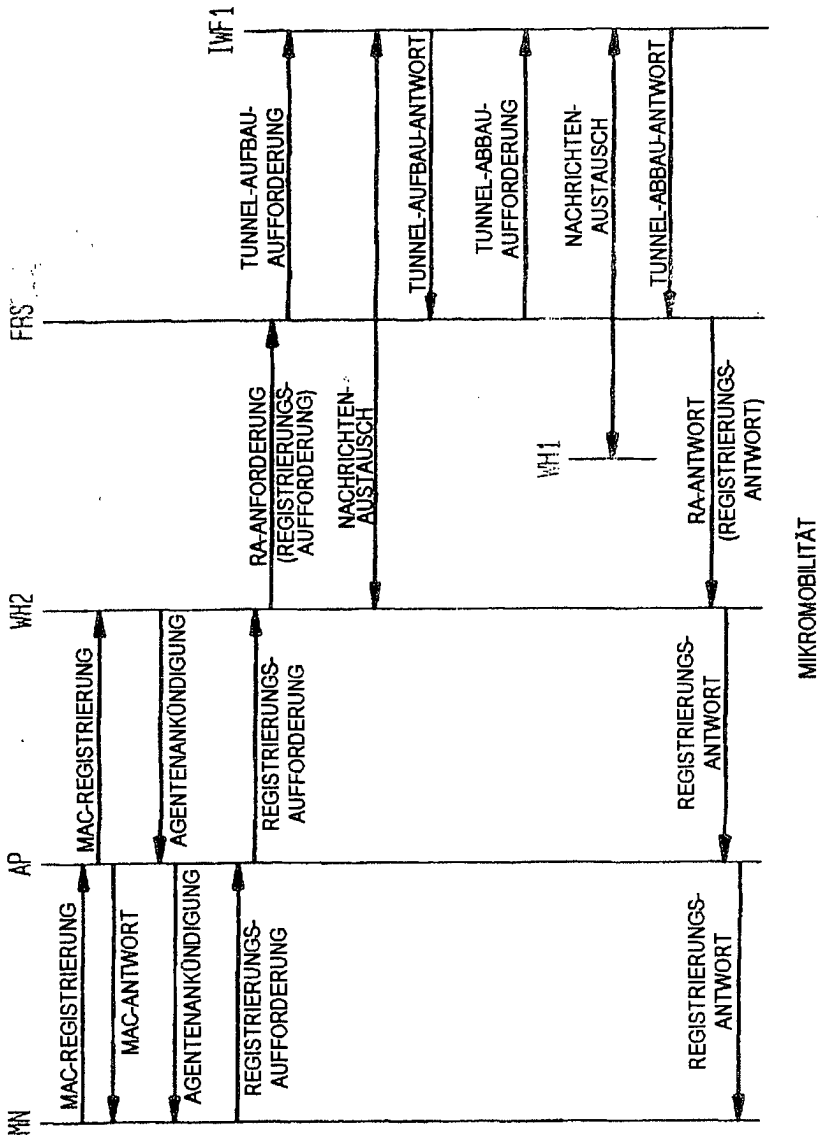

MN
AP
WH2
FRS
IWF1
MAC-REGISTRIERUNG
MAC-ANTWORT
AGENTENANKÜNDIGUNG
AGENTENANKÜNDIGUNG
REGISTRIERUNGS-AUFFORDERUNG
REGISTRIERUNGS-AUFFORDERUNG
MAC-REGISTRIERUNG
RA-ANFORDERUNG (REGISTRIERUNGS-AUFFORDERUNG)
NACHRICHTEN-AUSTAUSCH
TUNNEL-AUFBAU-AUFFORDERUNG
TUNNEL-AUFBAU-ANTWORT
TUNNEL-ABBAU-AUFFORDERUNG
NACHRICHTEN-AUSTAUSCH
TUNNEL-ABBAU-ANTWORT
WH1
RA-ANTWORT (REGISTRIERUNGS-ANTWORT)
REGISTRIERUNGS-ANTWORT
REGISTRIERUNGS-ANTWORT
MIKROMOBILITÄT

FIG. 34

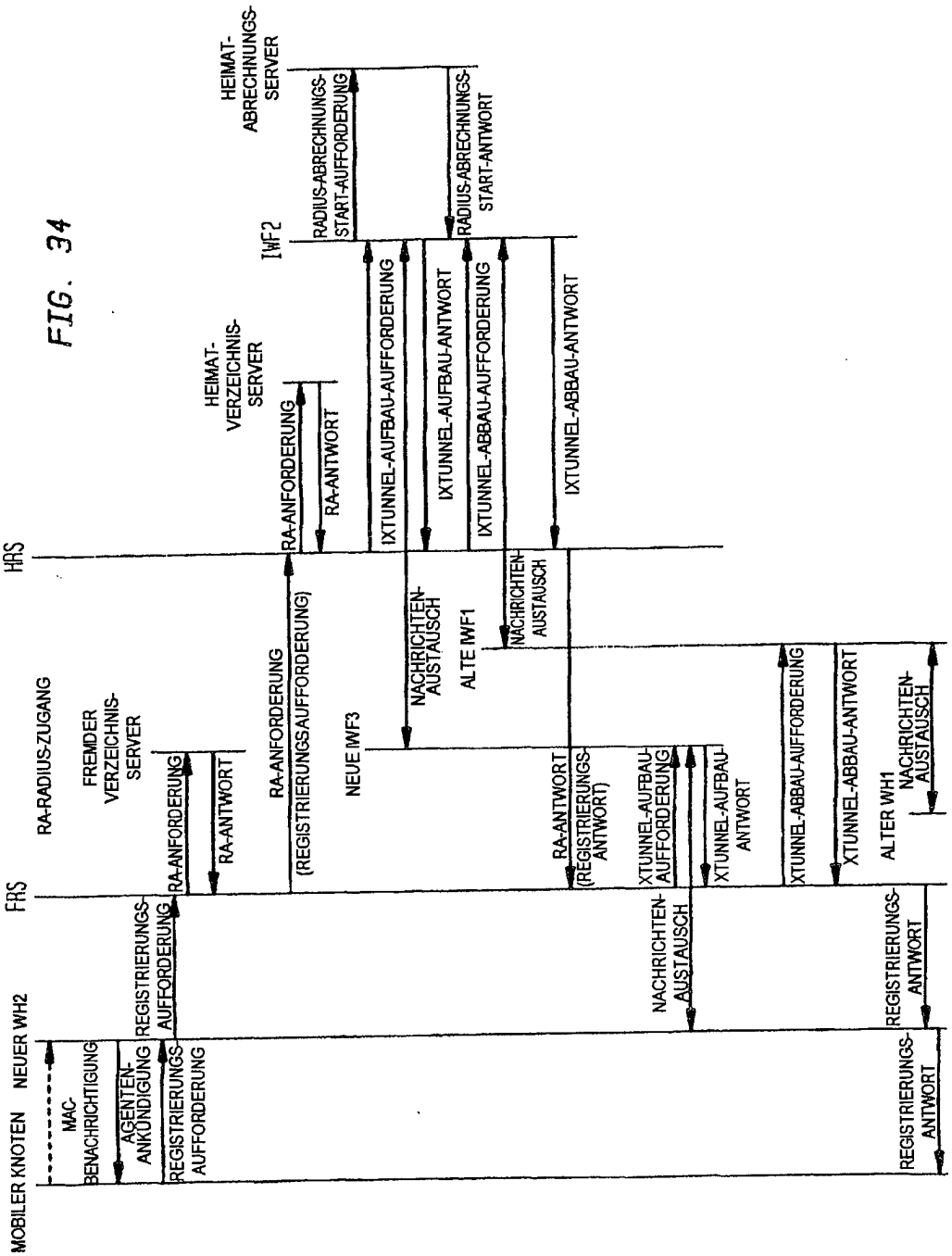
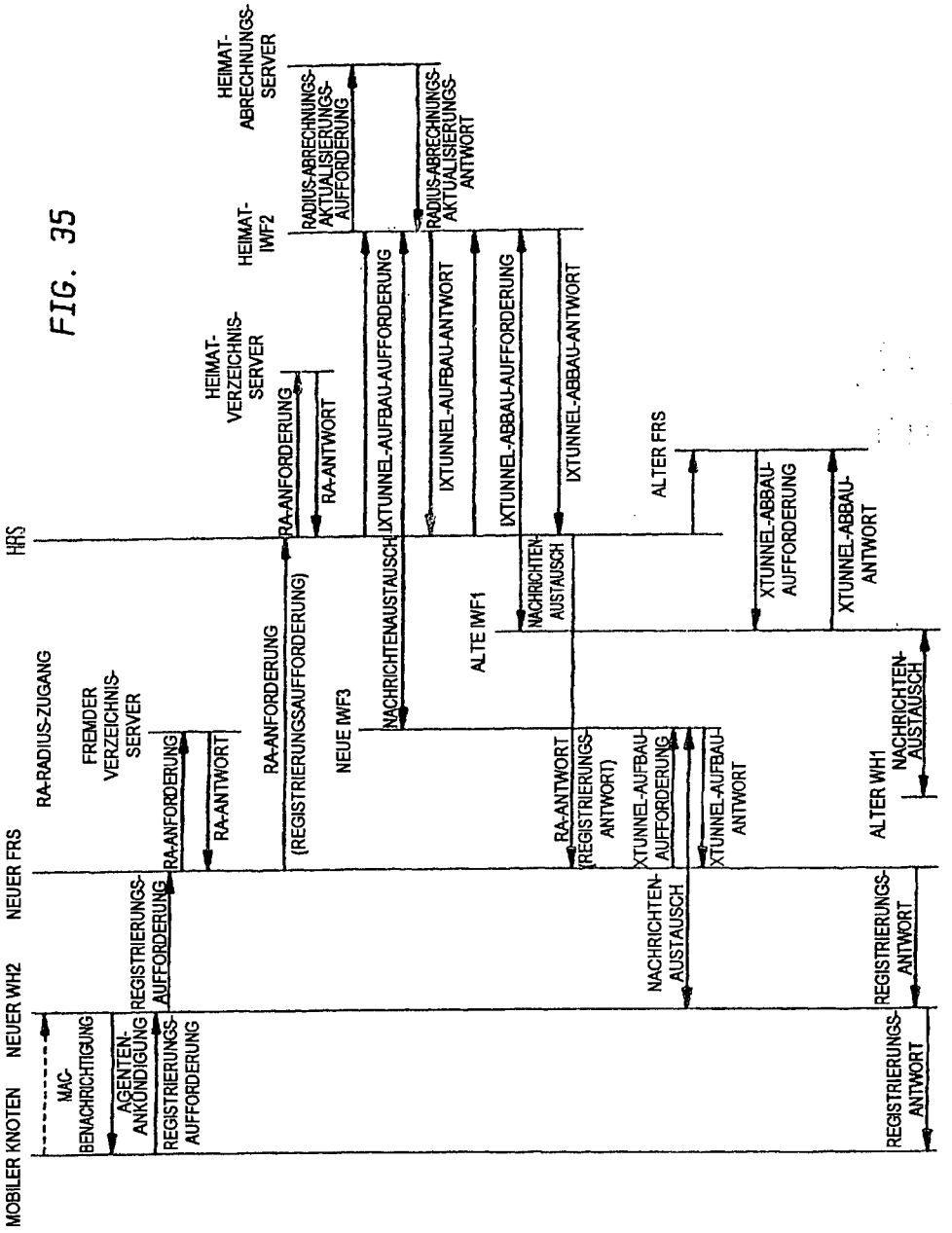

MOBILER KNOTEN
NEUER WH2
FRS
HRS
RA-RADIUS-ZUGANG
FREMDER VERZEICHNIS-SERVER
HEIMAT-VERZEICHNIS-SERVER
IWF2
HEIMAT-ABRECHNUNGS-SERVER
MAC-BENACHRICHTIGUNG
AGENTEN-ANKÜNDIGUNG
REGISTRIERUNGS-AUFFORDERUNG
RA-ANFORDERUNG
RA-ANTWORT
RA-ANFORDERUNG (REGISTRIERUNGSAUFFORDERUNG)
RA-ANTWORT (REGISTRIERUNGS-ANTWORT)
RADIUS-ABRECHNUNGS-START-AUFFORDERUNG
RADIUS-ABRECHNUNGS-START-ANTWORT
IXTUNNEL-AUFBAU-AUFFORDERUNG
IXTUNNEL-AUFBAU-ANTWORT
IXTUNNEL-ABBAU-AUFFORDERUNG
IXTUNNEL-ABBAU-ANTWORT
NEUE IWF3
NACHRICHTEN-AUSTAUSCH
ALTE IWF1
NACHRICHTEN-AUSTAUSCH
XTUNNEL-AUFBAU-AUFFORDERUNG
XTUNNEL-AUFBAU-ANTWORT
XTUNNEL-ABBAU-AUFFORDERUNG
XTUNNEL-ABBAU-ANTWORT
ALTER WH1
NACHRICHTEN-AUSTAUSCH
NACHRICHTEN-AUSTAUSCH
REGISTRIERUNGS-ANTWORT
REGISTRIERUNGS-ANTWORT

FIG. 35


MOBILER KNOTEN
NEUER WH2
NEUER FRS
RA-RADIUS-ZUGANG
FREMDER VERZEICHNIS-SERVER
HRS
HEIMAT-VERZEICHNIS-SERVER
HEIMAT-IWF2
HEIMAT-ABRECHNUNGS-SERVER
MAC-BENACHRICHTIGUNG
AGENTEN-ANKÜNDIGUNG
REGISTRIERUNGS-AUFFORDERUNG
RA-ANFORDERUNG
RA-ANTWORT
RA-ANFORDERUNG
(REGISTRIERUNGSAUFFORDERUNG)
RA-ANFORDERUNG
RA-ANTWORT
RADIUS-ABRECHNUNGS-AKTUALISIERUNGS-AUFFORDERUNG
RADIUS-ABRECHNUNGS-AKTUALISIERUNGS-ANTWORT
NEUE IWF3
IXTUNNEL-AUFBAU-AUFFORDERUNG
IXTUNNEL-AUFBAU-ANTWORT
NACHRICHTENAUSTAUSCH
ALTE IWF1
IXTUNNEL-ABBAU-AUFFORDERUNG
IXTUNNEL-ABBAU-ANTWORT
NACHRICHTEN-AUSTAUSCH
ALTER FRS
XTUNNEL-ABBAU-AUFFORDERUNG
XTUNNEL-ABBAU-ANTWORT
RA-ANTWORT (REGISTRIERUNGS-ANTWORT)
XTUNNEL-AUFBAU-AUFFORDERUNG
XTUNNEL-AUFBAU-ANTWORT
NACHRICHTEN-AUSTAUSCH
ALTER WH1
NACHRICHTEN-AUSTAUSCH
REGISTRIERUNGS-ANTWORT
REGISTRIERUNGS-ANTWORT

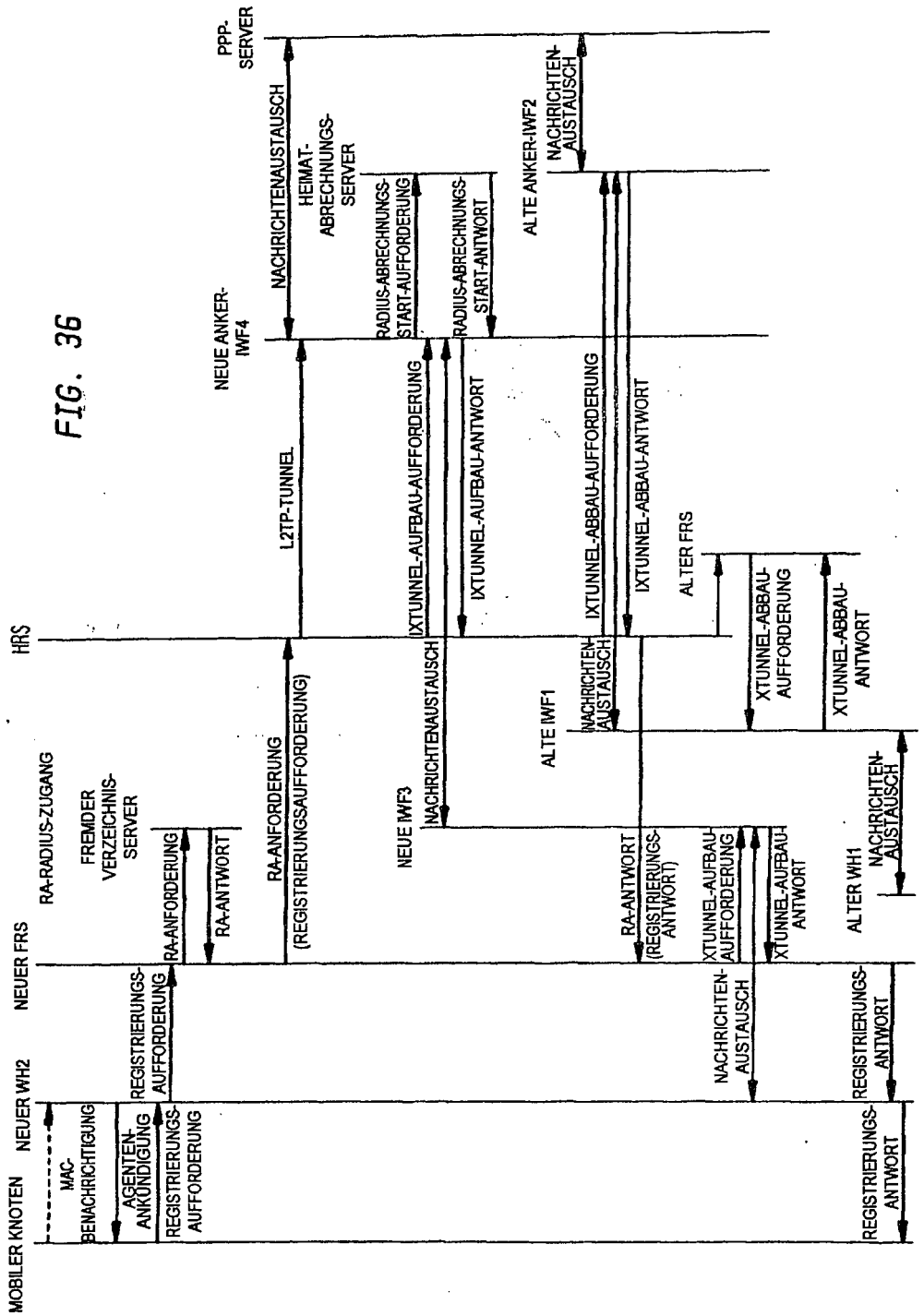

MOBILER KNOTEN
NEUER WH2
NEUER FRS
HRS
RA-RADIUS-ZUGANG
FREMDER VERZEICHNIS-SERVER
NEUE ANKER-IWF4
PPP-SERVER
MAC-BENACHRICHTIGUNG
AGENTEN-ANKÜNDIGUNG
REGISTRIERUNGS-AUFFORDERUNG
RA-ANFORDERUNG
RA-ANTWORT
RA-ANFORDERUNG (REGISTRIERUNGSAUFFORDERUNG)
L2TP-TUNNEL
NACHRICHTENAUSTAUSCH
HEIMAT-ABRECHNUNGS-SERVER
RADIUS-ABRECHNUNGS-START-AUFFORDERUNG
RADIUS-ABRECHNUNGS-START-ANTWORT
NEUE IWF3
NACHRICHTENAUSTAUSCH
IXTUNNEL-AUFBAU-AUFFORDERUNG
IXTUNNEL-AUFBAU-ANTWORT
ALTE ANKER-IWF2
NACHRICHTEN-AUSTAUSCH
ALTE IWF1
NACHRICHTEN-AUSTAUSCH
IXTUNNEL-ABBAU-AUFFORDERUNG
IXTUNNEL-ABBAU-ANTWORT
ALTER FRS
XTUNNEL-ABBAU-AUFFORDERUNG
XTUNNEL-ABBAU-ANTWORT
RA-ANTWORT (REGISTRIERUNGS-ANTWORT)
XTUNNEL-AUFBAU-AUFFORDERUNG
XTUNNEL-AUFBAU-ANTWORT
ALTER WH1
NACHRICHTEN-AUSTAUSCH
NACHRICHTEN-AUSTAUSCH
REGISTRIERUNGS-ANTWORT
REGISTRIERUNGS-ANTWORT
REGISTRIERUNGS-AUFFORDERUNG

FIG. 36

FIG. 37

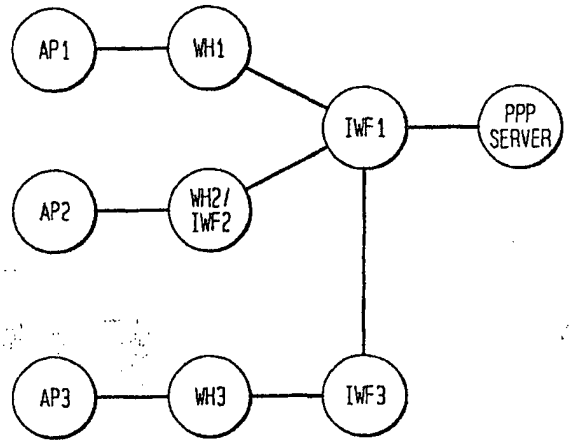
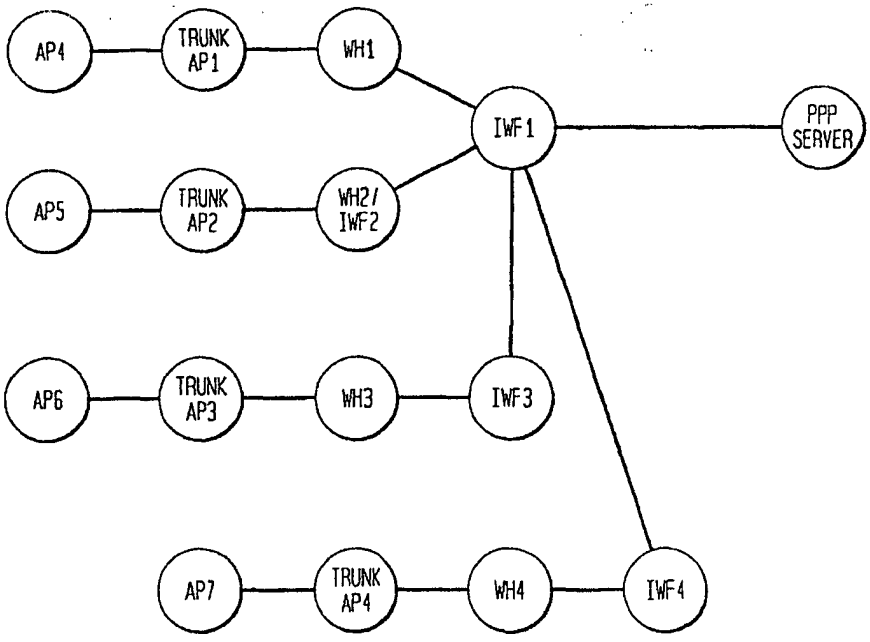

AP1
WH1
IWF1
PPP SERVER
AP2
WH2/ IWF2
AP3
WH3
IWF3

FIG. 38


AP4
TRUNK AP1
WH1
IWF1
PPP SERVER
AP5
TRUNK AP2
WH2/ IWF2
AP6
TRUNK AP3
WH3
IWF3
AP7
TRUNK AP4
WH4
IWF4

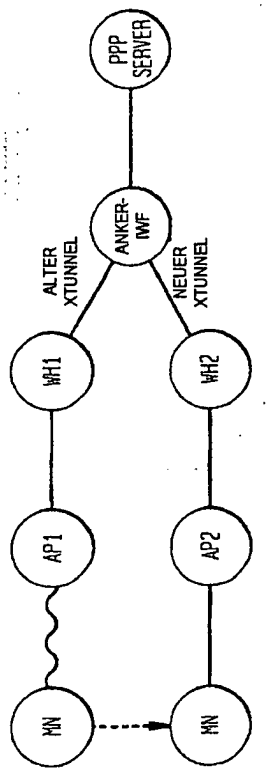

PPP SERVER
ANKER-IWF
ALTER XTUNNEL
NEUER XTUNNEL
WH1
WH2
AP1
AP2
MN
MN

FIG. 39

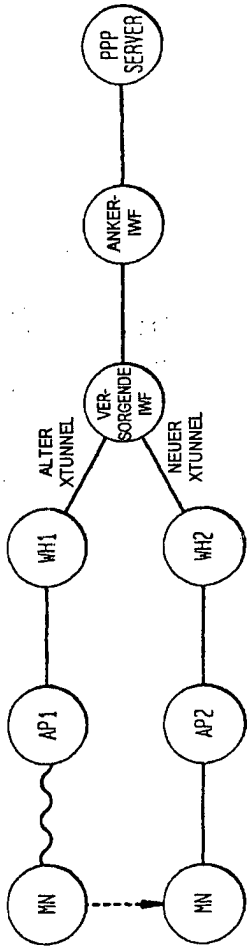

PPP SERVER
ANKER-IWF
VER-SORGENDE IWF
ALTER XTUNNEL
NEUER XTUNNEL
WH1
WH2
AP1
AP2
MN
MN

FIG. 40

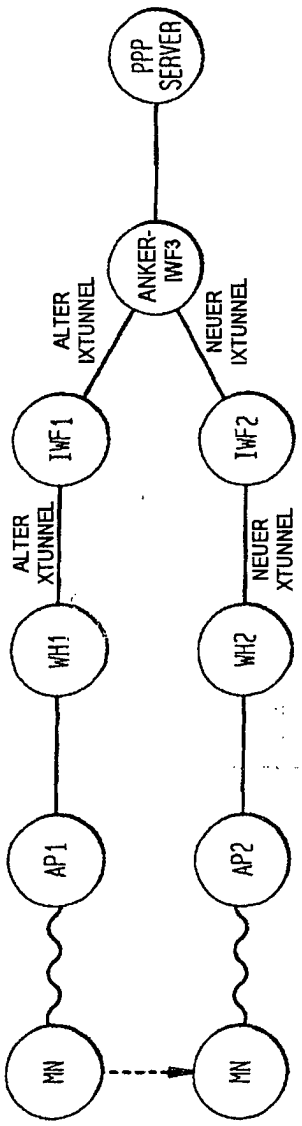

PPP SERVER
ANKER-IWF3
ALTER IXTUNNEL
NEUER IXTUNNEL
IWF1
IWF2
ALTER XTUNNEL
NEUER XTUNNEL
WH1
WH2
AP1
AP2
MN
MN

FIG. 41

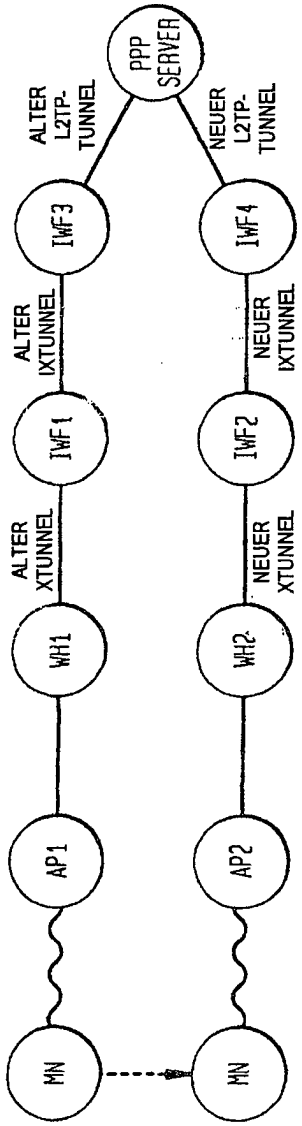

PPP SERVER
ALTER L2TP-TUNNEL
NEUER L2TP-TUNNEL
IWF3
IWF4
ALTER IXTUNNEL
NEUER IXTUNNEL
IWF1
IWF2
ALTER XTUNNEL
NEUER XTUNNEL
WH1
WH2
AP1
AP2
MN
MN

FIG. 42