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

(10) **DE 698 30 223 T2** 2006.02.02

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 917 318 B1**
(21) Deutsches Aktenzeichen: **698 30 223.0**
(96) Europäisches Aktenzeichen: **98 308 331.2**
(96) Europäischer Anmeldetag: **13.10.1998**
(97) Erstveröffentlichung durch das EPA: **19.05.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **18.05.2005**
(47) Veröffentlichungstag im Patentblatt: **02.02.2006**

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

(30) Unionspriorität:

61915 P	**14.10.1997**	**US**
138903	**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:
Feder, Peretz Moshes, Bergen, New Jersey 07631, US; Ner, Haim Shalom, Bergen, New Jersey 07410, US; Rai, Girish, Du Page, Illinois 60103, US

(54) Bezeichnung: **Punkt-zu-Punkt Protokoll Einkapselung in einem Ethernet-Rahmen**

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

Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich auf ein drahtloses Datennetz und insbesondere auf das Kommunizieren mit einem Pier-zu-Pier-Protokoll-Server im drahtlosen Datennetz.

Beschreibung des Standes der Technik

[0002] WO-A-96 21 984 offenbart ein Paketfunksystem, das Datenpakete von externen Datennetzen durch ein Punkt-zu-Punkt Protokoll PPP verkapselt und sie durch ein oder mehrere Sub-Netze an einen Punkt weitergibt, der das Protokoll des verkapselten Datenpakets unterstützt.

[0003] Fig. 1 stellt drei Geschäftseinheiten dar, deren Ausrüstungen, die zusammen arbeiten, typischerweise über die Benutzermodems **4** Internet-Fernzugang für die Benutzercomputer **2** bereitstellen. Die Benutzercomputer **2** und die Modems **4** bilden Endsysteme.

[0004] Die erste Geschäftseinheit ist die Telefongesellschaft (Telco), die das herkömmliche Einwahl-Telefonsystem (POTS) oder ISDN (Integrated Services Data Network) Netz besitzt und betreibt. Die Telco stellt das Medium in der Form des öffentlichen Telefonnetzes (PSTN) **6** bereit, über das Bits (oder Pakete) zwischen Benutzern und den zwei anderen Geschäftseinheiten fließen können.

[0005] Die zweite Geschäftseinheit ist der Internet Service Provider (ISP). Der ISP verteilt und verwaltet einen oder mehrere Points of Presence (POPs) **8** in seinem Servicebereich, mit denen sich die Endbenutzer für die Netzdienste verbinden. Ein ISP richtet typischerweise einen POP in jedem bedeutenden lokalen Anrufbereich, in dem der ISP erwartet, Abonnenten zu finden, ein. Der POP wandelt den Nachrichtenverkehr vom durch die Telco betriebenen PSTN in eine digitale Form um, um über den Intranet-Backbone **10**, der sich im Besitz des ISP befindet oder von einem Intranet-Backbone-Provider wie MCI Inc. gemietet wird, getragen zu werden. Ein ISP mietet typischerweise ganze T1-Leitungen oder Teile davon oder ganze T3-Leitungen oder Teile davon von der Telco für die Konnektivität mit dem PSTN. Die POPs und das Datenzentrum **14** des ISP-Mediums sind durch den Router **12A** über den Intranet-Backbone miteinander verbunden. Das Datenzentrum beherbergt die Webserver, Mailserver, Accounting-Server und Registrierungsserver des ISP, was es dem ISP ermöglicht, Netzinhalte, E-Mail- und Webhostingdienste für die Endbenutzer bereitzustellen. Zukünftige Mehrwertdienste können durch das Verteilen von zusätzlichen Typen von Servern im Datenzentrum hinzugefügt werden. Der ISP unterhält ebenfalls den Router **12A** zum Verbinden mit dem öffentlichen Internet-Backbone **20**. Im gegenwärtigen Modell für Fernzugang haben die Endbenutzer Dienstleistungsverhältnisse mit ihrer Telco und ihrem ISP und erhalten gewöhnlich getrennte Rechnungen von beiden. Die Endbenutzer greifen auf den ISP, und über den ISP, auf das öffentliche Internet **20** zu, indem der nächste POP gewählt wird und ein Kommunikationsprotokoll ausgeführt wird, das als Internet Engineering Task Force (IETF) Punkt-zu-Punkt-Protokoll (PPP) bekannt ist.

[0006] Die dritte Geschäftseinheit ist die private Gesellschaft, die aus geschäftlichen Gründen über den Router **12B** ihr eigenes privates Intranet **18** besitzt und betreibt. Angestellte der Gesellschaft können auf das Netz **18** der Gesellschaft (z. B. von zu Hause oder von unterwegs) zugreifen, indem sie POTS/ISDN-Anrufe auf den Fernzugangsserver **16** der Gesellschaft machen und das IETF PPP Protokoll ausführen. Für den Unternehmenszugang zahlen die Benutzer nur die Kosten der Verbindung mit dem Fernzugangsserver **16** der Gesellschaft. Der ISP ist nicht beteiligt. Die private Gesellschaft unterhält den Router **12B** zum Verbinden eines Endbenutzers entweder mit den Intranet **18** der Gesellschaft oder dem öffentlichen Internet **20** oder beiden.

[0007] Die Endbenutzer bezahlen die Telco für die Kosten der Telefonanrufe und für die Kosten einer Telefonleitung zu ihnen nach Hause. Die Endbenutzer bezahlen ebenfalls den ISP für den Zugang auf das Netz und die Dienstleistungen des ISP. Die vorliegende Erfindung wird Wireless Service Providern, wie Sprint PCS, PrimeCo, usw. zugute kommen und Internet Service Providern wie AOL, AT&T Worldnet usw. zugute kommen.

[0008] Heute stellen Internet Service Provider Internetzugangsdienste, Netzinhalt-Dienste, E-Mail-Dienste, Content-Hosting-Dienste und Roaming für Endbenutzer bereit. Wegen niedriger Margen und keinem Spielraum für Marktsegmentierung basierend auf Merkmalen und Preis, suchen ISPs nach Mehrwertdiensten zum Verbessern der Margen. Kurzfristig werden Lieferanten von Ausrüstungen imstande sein, den ISPs Lösungen zu bieten, um ihnen das Anbieten von schnellerem Zugang, virtuellen privaten Netzwerken (was die Fähigkeit ist, öffentliche Netze so sicher wie private Netze zu verwenden und Intranet-Verbindungen herzustellen), Roa-

ming-Konsortien, Push-Technologien und Quality of Service zu ermöglichen. Langfristiger werden ebenfalls Voice over Internet und Mobilität angeboten werden. ISPs werden diese Mehrwertdienste verwenden, um der Zwangsjacke niedriger Margen zu entkommen. Viele dieser Mehrwertdienste fallen in die Kategorie der Netzdienste und können nur über die Netzinfrastrukturausrüstung angeboten werden. Andere fallen in die Kategorie der Anwendungsdienste, die Unterstützung von der Netzinfrastruktur erfordern, während andere keine Unterstützung durch die Netzinfrastruktur erfordern. Sämtliche Dienstleistungen wie schnellerer Zugang, virtuelle private Netzwerke, Roaming, Mobilität, Voice, Quality of Service, Quality of Service basiertes Accounting benötigen eine verbesserte Netzinfrastruktur. Das hier beschriebene System wird diese verbesserten Dienste entweder direkt bereitstellen oder Hooks bereitstellen, derart, dass diese Dienste später als zukünftige Verbesserungen hinzugefügt werden können. Wireless Service Provider werden imstande sein, einen größeren Teil des Einkommensstroms einzufangen. Der ISP wird imstande sein, mehr Dienste und mit besserer Marktsegmentierung anzubieten.

Kurzdarstellung der Erfindung

[0009] Ein drahtloses Datennetz gemäß der Erfindung wird in Anspruch 1 festgehalten. Bevorzugte Formen sind in den abhängigen Ansprüchen festgehalten.

[0010] Die vorliegende Erfindung stellt drahtlosen Fernzugang auf das öffentliche Internet, private Intranets und Internet Service Provider für Endbenutzer bereit. Drahtloser Zugang wird durch Basisstationen in einem Heimatnetz und Basisstationen in Fremdnetzen mit Austauschvereinbarungen bereitgestellt.

[0011] Eine Aufgabe des vorliegenden System ist es, ein drahtloses paketvermitteltes Datennetz für Endbenutzer bereitzustellen, das das Mobilitätsmanagement in lokale, Mikro-, Makro- und globale Verbindungsübergabekategorien unterteilt und Handoffaktualisierungen in Übereinstimmung mit der Handoffkategorie minimiert. Eine andere Aufgabe ist das Integrieren von MAC-Handoff-Nachrichten mit Netz-Handoff-Nachrichten. Des Weiteren ist eine Aufgabe des vorliegenden Systems, Registrierungsfunktionen separat an einen Registrierungsserver zu richten und Routingfunktionen an Interworking-Funktionseinheiten zu richten. Es ist noch eine weitere Aufgabe, einen XTunnel-Zwischenkanal zwischen einem drahtlosen Hub (ebenfalls AH Access Hub genannt) und einer Interworking-Funktionseinheit (IWF-Einheit) in einem Fremdnetz bereitzustellen. Noch eine andere Aufgabe ist, einen IXTunnel-Kanal zwischen der Interworking-Funktionseinheit in einem Fremdnetz und einer Interworking-Funktionseinheit in einem Heimatnetz bereitzustellen. Eine weitere Aufgabe ist die Verbesserung des Layer-2-Tunneling-Protokolls (L2TP), um ein mobiles Endsystem zu unterstützen. Eine weitere Aufgabe ist das Durchführen der Netzschichtregistrierung vor dem Start einer PPP-Kommunikationssession. Eine weitere Aufgabe ist das Verkapseln der Pier-zu-Pier-Protokoll (PPP) Informationen, die von einem PPP-Server für mindestens ein Endsystem gesendet werden, in einen Ethernet-Rahmen und das Senden der PPP-Informationen an dieses mindestens eine Endsystem über eine Ethernet-Verbindung.

[0012] Gemäß einer Ausführungsform der Erfindung wird ein drahtloses Datennetz, das Kommunikationen mit einem Pier-zu-Pier-Protokollserver bereitstellt, offenbart. Das Netz enthält ein Heimatnetz, das eine Heimat-Mobilvermittlungsstelle, ein drahtloses Modem und ein oder mehrere Endsysteme umfasst. Das drahtlose Modem und die Endsysteme sind über eine Ethernet-Verbindung miteinander verbunden. Das Netz enthält ebenfalls einen PPP-Server, wobei die PPP-Informationen, die vom PPP-Server für die Endsysteme gesendet werden, durch das drahtlose Modem in einem Ethernet-Rahmen verkapselt und über die Ethernet-Verbindung an die Endsysteme gesendet werden.

Kurzbeschreibung der Zeichnungen

[0013] Das System wird in der nachfolgenden Beschreibung von bevorzugten Ausführungsformen unter Bezugnahme auf die nachfolgenden Figuren im Detail beschrieben, in denen:

[0014] Fig. 1 ein Konfigurationsdiagramm einer bekannten Fernzugangsarchitektur durch ein öffentliches Telefonnetz ist;

[0015] Fig. 2 ein Konfigurationsdiagramm einer Fernzugangsarchitektur durch ein drahtloses paketvermitteltes Datennetz gemäß der vorliegenden Erfindung ist;

[0016] Fig. 3 ein Konfigurationsdiagramm von ausgewählten Teilen der Architektur des Netzes von Fig. 2 ist, das ein Roaming-Szenario zeigt;

[0017] Fig. 4 ein Konfigurationsdiagramm einer Basisstation mit lokalen Zugangspunkten ist;

[0018] Fig. 5 ein Konfigurationsdiagramm einer Basisstation mit Fernzugangspunkten ist;

[0019] Fig. 6 ein Konfigurationsdiagramm einer Basisstation mit Fernzugangspunkten, von denen einige unter Verwendung einer drahtlosen Trunk-Verbindung verbunden sind, ist;

[0020] Fig. 7 ein Diagramm eines Protokollstapels für einen lokalen Zugangspunkts ist;

[0021] Fig. 8 ein Diagramm eines Protokollstapels für einen Fernzugangspunkt mit einem drahtlosen Trunk ist;

[0022] Fig. 9 ein Diagramm eines Protokollstapels für eine Relayfunktion in der Basisstation zum Unterstützen von Fernzugangspunkten mit drahtlosen Trunks ist;

[0023] Fig. 10 ein Diagramm von Protokollstapeln zum Ausführen der in Fig. 9 veranschaulichten Relayfunktion ist;

[0024] Fig. 11 ein Diagramm von Protokollstapeln für eine Relayfunktion in der Basisstation zum Unterstützen von lokalen Zugangspunkten ist;

[0025] Fig. 12 ein Konfigurationsdiagramm von ausgewählten Teilen der Architektur des Netzes von Fig. 2 ist, das ein erstes Endsystem, das sich vom Heimatnetz aus im Heimatnetz registriert und ein zweites System, das sich von einem Fremdnetz aus unter Verwendung einer Heimat-Interworking-Funktion für einen Anker im Heimatnetz registriert, zeigt;

[0026] Fig. 13 ein Konfigurationsdiagramm von ausgewählten Teilen der Architektur des Netzes von Fig. 2 ist, das ein erstes Endsystem, das sich vom Heimatnetz aus im Heimatnetz registriert und ein zweites System, das sich von einem Fremdnetz aus unter Verwendung einer dienenden Interworking-Funktion für einen Anker im Heimatnetz registriert, zeigt;

[0027] Fig. 14 ein Leiterdiagramm der von einem Fremdnetz aus in einem Heimatnetz zu registrierenden Anfrage- und Antwortnachrichten und zum Herstellen, Authentifizieren und Konfigurieren einer Datenverbindung ist;

[0028] Fig. 15 ein Konfigurationsdiagramm von ausgewählten Teilen der Architektur des Netzes von Fig. 2 ist, das Registrierungsanfragen und Antworten zum Registrieren einer mobilen Einheit vom Heimatnetz aus in einem Heimatnetz zeigt;

[0029] Fig. 16 ein Konfigurationsdiagramm von ausgewählten Teilen der Architektur von Fig. 2 ist, das Registrierungsanfragen und Antworten zum Registrieren einer mobilen Einheit von einem Fremdnetz aus in einem Heimatnetz zeigt;

[0030] Fig. 17. ein Konfigurationsdiagramm von Protokollstapeln ist, die Kommunikationen zwischen einem Endsystem in einem Heimatnetz und einer Interworking-Funktion im Heimatnetz, wo der Zellenstandort lokale Zugangspunkte hat, zeigt;

[0031] Fig. 18 ein Konfigurationsdiagramm von Protokollstapeln ist, die Kommunikationen zwischen einem Endsystem in einem Heimatnetz und einer Interworking-Funktion im Heimatnetz zeigt, wo der Zellenstandort Fernzugangspunke hat, die durch einen drahtlosen Trunk an einen drahtlosen Hub gekoppelt sind;

[0032] Fig. 19 ein Konfigurationsdiagramm von Protokollstapeln ist, das die Kommunikationen zwischen einer Basisstation, die an ein roamendes Endsystem gekoppelt ist, und einer Heimat-Interworking-Funktion zeigt;

[0033] Fig. 20 ein Konfigurationsdiagramm von Protokollstapeln ist, das die Kommunikationen zwischen einem Endsystem in einem Heimatnetz durch eine Interworking-Funktion im Heimatnetz und einen Internet Service Provider zeigt;

[0034] Fig. 21 ein Konfigurationsdiagramm von Protokollstapeln ist, das die Kommunikationen zwischen ei-

nem Endsystem in einem Fremdnetz und einem Heimatregistrierungsserver in einem Heimatnetz während der Registrierungsphase zeigt;

[0035] Fig. 22 ein Verarbeitungsflussdiagramm ist, das die Verarbeitung von Accounting-Daten durch das Kundenabrechnungssystem, zeigt;

[0036] Fig. 23 und Fig. 24 Leiterdiagramme sind, die das Registrierungsverfahren für in dieser Reihenfolge ein Endsystem in einem Heimatnetz und in einem Fremdnetz veranschaulichen;

[0037] Fig. 25 und Fig. 26 Protokollstapeldiagramme sind, die eine Endsystemverbindung in einem Heimatnetz veranschaulichen, wo ein PPP-Protokoll in einer Interworkingfunktion des Heimatnetzes endet und wo das PPP-Protokoll in dieser Reihenfolge in einem ISP oder Intranet endet;

[0038] Fig. 27 und Fig. 28 Protokollstapeldiagramme sind, die eine Endsystemverbindung in einem Fremdnetz veranschaulichen, wo ein PPP-Protokoll in einer Interworkingfunktion des Fremdnetzes endet und wo das PPP-Protokoll in dieser Reihenfolge in einem ISP oder Intranet endet;

[0039] Fig. 29 Endsysteme veranschaulicht, die über Ethernet mit einem drahtlosen Modem verbunden sind, wo ein PPP-Protokoll in einem Ethernet-Rahmen verkapselt ist;

[0040] Fig. 30 ein Ethernet-Rahmenformat veranschaulicht;

[0041] Fig. 31 XWD-Kopffelder veranschaulicht;

[0042] Fig. 32 Endsysteme veranschaulicht, die über ein lokales Netz mit einem drahtlosen Router verbunden sind, wo das PPP-Protokoll am drahtlosen Router endet;

[0043] Fig. 33, Fig. 34 und Fig. 35 Leiterdiagramme sind, die in dieser Reihenfolge ein lokales Handoff-Szenario, ein Mikro-Handoff-Szenario und ein Makro-Handoff-Szenario veranschaulichen;

[0044] Fig. 36 ein Leiterdiagramm ist, das ein globales Handoff-Szenario veranschaulicht, wo die Heimat-Interworking-Funktion sich nicht ändert; und

[0045] Fig. 37 ein Leiterdiagramm ist, das ein globales Handoff-Szenario veranschaulicht, wo sowohl der Fremdregistrierungsserver als auch die Heimat-Interworking-Funktion sich ändern.

Detaillierte Beschreibung bevorzugter Ausführungsformen

[0046] Das vorliegende System verschafft Computerbenutzern einen Fernzugang auf das Internet und auf private Intranets unter Verwendung von virtuellen privaten Netzdiensten über eine Hochgeschwindigkeits-, paketvermittelte, drahtlose Datenverbindung. Diese Benutzer sind imstande, über eine drahtlose Verbindung auf das öffentliche Internet, private Intranets und ihre Internet Service Provider zuzugreifen. Das Netz unterstützt Roaming, das heißt, die Fähigkeit, unter Verwendung von virtuellen privaten Netzdiensten von überall, wo die durch das vorliegende System angebotenen Dienste verfügbar sind, auf das Internet und private Intranets zuzugreifen. Das Netz unterstützt ebenfalls Handoffs, das heißt, die Fähigkeit, den Anschlusspunkt des Benutzers an das Netz zu wechseln, ohne die PPP-Verbindung zwischen dem PPP-Client und dem PPP-Server zu stören. Das Netz zielt auf Benutzer ab, die horizontale Internet- und Intranetanwendungen ausführen. Diese Anwendungen umfassen E-Mail, Dateitransfer, browserbasierten WWW-Zugang und andere um das Internet aufgebaute kommerzielle Anwendungen. Da das Netz auf den IETF-Standards basiert, ist es möglich, Streaming-Media-Protokolle wie RTP und Conferencing-Protokolle wie H.323 auf ihm auszuführen.

[0047] Andere Internet-Fernzugangstechnologien, die bereits verteilt oder in unterschiedlichen Verteilungsphasen sind, umfassen: auf POTS und ISDN basierender Drahtleitungseinwahl-Zugang, XDSL-Zugang, drahtloser, leitungsvermittelter Zugang basierend auf GSM/CDMA/TDMA, drahtloser, punktvermittelter Zugang basierend auf GSM/CDMA/TDMA Kabelmodems, und Verteilung, Wartungsfreundlichkeit, eine große Reihe von Merkmalen, Skalierbarkeit, eine Fähigkeit zum eleganten Abbau unter schweren Belastungsbedingungen und Unterstützung für verbesserte Netzdienste wie virtuelle private Netzdienste, Roaming, Mobilität und Quality of Service zum jeweiligen Nutzen der Benutzer und Service Provider.

[0048] Für Wireless Service Provider, die ein eigenes Personal Communications System (PCS) Spektrum ha-

ben, wird das vorliegende System die Möglichkeit bereitstellen, drahtlose paketvermittelte Datenzugangsdienste anzubieten, die mit Diensten konkurrieren können, die durch die herkömmlichen Drahtleitungs-Telcos, die das PSTN besitzen und betreiben, bereitgestellt werden. Wireless Service Provider können ebenfalls entscheiden, selbst Internet Service Provider zu werden, und in diesem Fall werden sie das gesamte Netz besitzen und betreiben, und End-to-End-Dienste für die Benutzer bereitstellen.

[0049] Internet Service Providern wird das vorliegende System ermöglichen, die Telcos zu umgehen (vorausgesetzt sie kaufen oder mieten das Spektrum) und den Benutzern direkt End-to-End-Dienste anzubieten und vielleicht Zugangsgebühren an die Telcos zu sparen, die in der Zukunft zunehmen können, da das Internet wächst, um noch größer zu werden als es heute ist.

[0050] Das vorliegende System ist so flexibel, derart, dass es Wireless Service Providern, die keine Internet Service Provider sind und die für Endbenutzer lediglich ISP, Internet oder privaten Intranetzugang bereitstellen, Nutzen bringen kann. Das System kann ebenfalls Service Providern Nutzen bringen, die drahtlosen Zugang und Internetdienste für Endbenutzer bereitstellen. Das System kann ebenfalls Service Providern Nutzen bringen, die drahtlosen Zugang und Internetdienste bereitstellen aber ebenfalls die Verwendung des drahtlosen Teils des Netzes zum Zugang auf andere ISPs oder auf private Intranets ermöglichen.

[0051] In Fig. 2, verbinden sich die Endsysteme **32** (z.B. basierend auf beispielsweise WIN **95** Personalcomputern) mit dem drahtlosen Netz **30** unter Verwendung von externen oder internen Modems. Diese Modems ermöglichen es den Endsystemen, Medium Access Control (MAC) Rahmen über den Air Link **34** zu senden und zu empfangen. Externe Modems verbinden sich mit dem PC über eine Draht- oder drahtlose Verbindung. Die externen Modems sind befestigt und zum Beispiel gemeinsam mit Dachrichtantennen untergebracht. Die externen Modems können mit dem PC des Benutzers unter Verwendung von einem der nachfolgenden Mittel verbunden werden: 802.3, universeller serieller Bus, Parallel-Port, Infrarot-, oder sogar eine ISM-Funkverbindung. Die internen Modems sind vorzugsweise PCMCIA-Karten für Laptops und werden in die Rückwand des Modems eingesteckt. Unter Verwendung einer kleinen Rundstrahlantenne, können sie über den Air Link MAC-Rahmen senden und empfangen. Endsysteme können ebenfalls Laptops mit einer Richtantenne, eine feste drahtlose Station in einem Haus mit einer Richtantenne, die über AC-Leitungen verbunden ist, und andere Alternativen sein.

[0052] Eine drahtlose Abdeckung eines großen Bereichs wird durch die Basisstationen **36** bereitgestellt. Die Basisstation **36** kann ein 5-Kanal-Wiederverwendungskommunikationsschema verwenden, wie in der U.S.-Patentanmeldung mit der Seriennummer 08/998,505, eingereicht am 26. Dezember 1997 beschrieben. Der Abdeckungsbereich, der durch die Basisstationen **36** bereitgestellt wird, ist abhängig von Faktoren wie Leistungsbilanz, Kapazität und Abdeckung. Basisstationen werden typischerweise durch PCS (Personal Communication Services) Wireless Service Provider an Zellenstandorten installiert. Basisstationen bündeln den Endsystemverkehr von ihrem Abdeckungsbereich über Drahtverbindung oder das Mikrowellen-Backhaulnetz **38** an die Mobilvermittlungsstelle (MSC) **40**.

[0053] Das System ist unabhängig von der MAC- und PHY (physischen) Schicht des Air Links und dem Typ des Modems. Die Architektur ist ebenfalls unabhängig von der physischen Schicht und der Topologie des Backhaul-Netzes **38**. Die einzigen Voraussetzungen für das Backhaul-Netz sind, dass es imstande sein muss, Internetprotokoll (IP) Pakete zwischen Basisstationen und der MSC mit angemessener Leistung zu routen. Bei der Mobilvermittlungsstelle **40** (MSC **40**), beendet die Paketdaten-Interworking-Funktion (IWF) **52** die drahtlosen Protokolle für dieses Netz. Der IP-Router **42** verbindet die MSC **40** mit dem öffentlichen Internet **44**, privaten Intranets **46** oder Internet Service Providern **46**. Die Accounting- und Directory-Server **48** in der MSC **40** speichern Accounting-Daten und Directory-Informationen. Der Element-Verwaltungsserver **50** verwaltet die Ausrüstung, die die Basisstationen, die IWFs und die Accounting-/Directory-Server enthält.

[0054] Der Accounting-Server sammelt Accounting-Daten über Benutzer und sendet die Daten an das Abrechnungssystem des Service Providers. Die Schnittstelle, die durch einen Accounting-Server unterstützt wird, sendet Accounting-Informationen im Abrechnungseintragsformat der American Management Association (AMA) oder in irgend einem anderen geeigneten Abrechnungsformat über einen TCP/IP (Transportkontrollprotokoll/Internetprotokoll) Transport an das Abrechnungssystem (das nicht in der Figur gezeigt wird).

[0055] Die Netzinfrastruktur stellt PPP (Punkt-zu-Punkt-Protokoll) Dienste für Endsysteme bereit. Das Netz stellt (1) festen drahtlosen Zugang mit Roaming (Login überall dort, wo die drahtlose Abdeckung verfügbar ist) für Endsysteme und (2) Mobilität und Handoffs mit niedriger Geschwindigkeit bereit. Wenn ein Endsystem einen Login in ein Netz vornimmt, kann es entweder einen festen Dienst (d.h. stationär und ohne erforderliche

Handoff-Dienste) oder einen mobilen Dienst (d.h. mit erforderlichen Handoff-Diensten) anfordern. Ein Endsystem, das nicht fest oder mobil angibt, wird als einen mobilen Dienst angebend betrachtet. Die tatsächliche Registrierung des Endsystems ist das Ergebnis einer Verhandlung mit einem Heimat-Registrierungsserver basierend auf dem angeforderten Dienstniveau, dem Dienstniveau, das der Benutzer des Endsystems abboniert hat und der Ausstattung, die im Netz verfügbar ist.

[0056] Wenn das Endsystem eine feste Dienstregistrierung (d.h., eine, die keine Handoff-Dienste erfordert) aushandelt und das Endsystem im Heimatnetz angeordnet ist, wird eine IWF (Interworking-Funktion) in der Basisstation ausgeführt, um den Verkehr zwischen dem Endbenutzer und einem Kommunikationsserver, wie beispielsweise einem PPP-Server weiterzugeben (d.h., der Punkt, mit dem die Verbindung vorgenommen werden soll, zum Beispiel ein ISP PPP-Server oder ein PPP-Server eines Unternehmensintranets oder ein PPP-Server, der durch den Wireless Service Provider betrieben wird, um für die Kunden Direktzugang zum öffentlichen Internet bereitzustellen). Es wird vorweggenommen, dass vielleicht 80 % des Nachrichtenverkehrs in dieser Kategorie stattfinden wird und folglich verteilt diese Architektur IWF-Verarbeitung in die Basisstationen und vermeidet einen Stau des Nachrichtenverkehrs in einer zentralen Mobilvermittlungsstelle.

[0057] Wenn das Endsystem mobile Dienste anfordert (von einem Heimatnetz oder einem Fremdnetz) oder wenn das Endsystem Roaming-Dienste anfordert (d.h., Dienste vom Heimatnetz durch das Fremdnetz), werden zwei IWFs eingerichtet: eine dienende IWF, die typischerweise in der Basisstation des Netzes, mit dem das Endsystem verbunden ist, eingerichtet wird (das Heimatnetz oder das Fremdnetz) und eine Heimat-IWF, die typischerweise in der Mobilvermittlungsstelle (MSC) des Heimatnetzes eingerichtet wird. Da vorweggenommen wird, dass diese Situation nur ungefähr 20 % des Nachrichtenverkehrs einbezieht, wird der Stau des Nachrichtenverkehrs um die Mobilvermittlungsstelle minimiert. Die dienende IWF und der drahtlose Hub können gemeinsam im gleichen Nest von Computern angeordnet sein, derart, dass ein Tunnel, der ein XTunnel-Protokoll verwendet, nicht zwischen dem drahtlosen Hub und der dienenden IWF angeordnet werden muss.

[0058] Basierend auf den verfügbaren Einrichtungen und dem angeforderten Typ und der angeforderten gualität des Dienstes kann eine dienende IWF in einem Fremdnetz indes alternativ von Einrichtungen in der Fremd-MSC gewählt werden. Allgemein wird die Heimat-IWF zu einem Ankerpunkt, der während der Kommunikationssession nicht geändert wird, während die dienende IWF sich ändern kann, wenn sich das Endsystem ausreichend bewegt.

[0059] Die Basisstation umfasst einen Access Hub und mindestens einen Zugangspunkt (fern oder gemeinsam mit dem Access Hub untergebracht). Typischerweise bedient der Access Hub mehrere Zugangspunkte. Während das Endsystem durch einen Draht oder ein Kabel gemäß den Lehren dieser Erfindung an einen Zugangspunkt angebunden werden kann, ist das Endsystem in einer bevorzugten Ausführungsform durch einen drahtlosen „Air Link" an den Zugangspunkt angebunden, und in diesem Fall wird gewöhnlich mit drahtloser Hub auf den Access Hub Bezug genommen. Obwohl über die gesamte Beschreibung hierin mit „drahtloser Hub" auf den Access Hub Bezug genommen wird, wird man verstehen, dass ein Endsystem, das über einen Zugangspunkt über Draht oder Kabel an einen Access Hub gekoppelt ist, eine gleichwertige Ausführungsform ist und durch den Begriff „Access Hub" betrachtet wird.

[0060] In der Erfindung enthält ein Endsystem einen Endbenutzer-Registrierungsagent (z.B. eine Software, die auf einem Computer des Endsystems, seinem Modem oder beiden ausgeführt wird), der mit einem Zugangspunkt und durch den Zugangspunkt mit einem drahtlosen Hub kommuniziert. Der drahtlose Hub umfasst einen Proxy-Registrierungsagent (z.B. eine Software, die auf einem Prozessor im drahtlosen Hub ausgeführt wird), der als Proxy für den Endbenutzer-Registrierungsagent agiert. Auf gleichartige Konzepte, die zum Beispiel im durch die IETF vorgeschlagenen Mobile IP Standard verwendet werden, wird allgemein als Fremdagent (FA) Bezug genommen. Aus diesem Grund wird auf den Proxy-Registrierungsagent des vorliegenden Systems mit Fremdagent Bezug genommen und Aspekte des Fremdagenten des vorliegenden Systems, die sich vom Fremdagent der Mobile IP unterscheiden, sind wie durchweg in dieser Beschreibung beschrieben.

[0061] Durch die Verwendung eines Proxy-Registrierungsagenten (d.h. Fremdagent FA) in einer Basisstation, ist der Benutzerregistrierungsagent eines Endsystems imstande, einen Anschlusspunkt an das Netz zu entdecken und bei einem Registrierungsserver in der MSC (Mobilvermittlungsstelle) des Heimatnetzes zu registrieren. Der Heimatregistrierungsserver bestimmt die Verfügbarkeit von jedem der mehrfachen Interworking-Funktionsmodule (IWFs) im Netz (tatsächlich jede Softwaremodule, die auf Prozessoren sowohl in der MSC als auch im drahtlosen Hub ausgeführt werden) und weist die IWF(s) an das registrierte Endsystem zu. Für jedes registrierte Endsystem wird (unter Verwendung des XTunnel Protokolls) ein Tunnel zwischen dem drahtlosen

Hub in der Basisstation und einer Interworking-Funktion (IFW) in der Mobilvermittlungsstelle (MSC) erzeugt, wobei dieser Tunnel PPP-Rahmen zwischen dem Endsystem und der IWF transportiert.

[0062] Wie hierin verwendet, ist das XTunnel Protokoll ein Protokoll, das den in Reihe Transport der PPP-Datenrahmen mit Flusskontrolle bereitstellt. Dieses Protokoll kann über Standard-IP-Netze oder über Punkt-zu-Punkt-Netze oder über vermittelte Netze, wie ATM-Datennetze oder Frame-Relay-Datennetze ausgeführt werden. Solche Netze können auf T1- oder T3-Verbindungen basieren oder auf Funkverbindungen basieren, entweder landbasiert oder raumbasiert. Das XTunnel-Protokoll kann durch Anpassen der Algorithmen von L2TP (Layer-2-Transferprotokoll) gebildet werden. In Netzen, die auf Verbindungen basieren, wo verlorenen Datenpaketen begegnet wird, kann ein Wiederübermittlungsmerkmal eine erwünschte Option sein.

[0063] Der PPP-Peer des Endsystems (d.h. ein Kommunikationsserver) kann in der IWF oder in einem Unternehmensintranet oder einem Netz eines ISP residieren. Wenn der PPP-Peer in der IWF residiert, wird das Endsystem mit direktem Internetzugang versehen. Wenn der PPP-Peer in einem Intranet oder ISP residiert, wird ein Endsystem mit Intranetzugang oder Zugang auf einen ISP versehen. Zum Unterstützen des Intranet- oder ISP-Zugangs verwendet die IWF das Layer-2-Tunneling-Protokol (L2TP) zur Verbindung mit dem Intranet oder dem PPP-Server des ISP. Aus der Perspektive des Intranets oder des PPP-Servers des ISP, sieht die IWF aus, wie ein Network Access Server (NAS). Der PPP-Verkehr zwischen dem Endsystem und der IWF wird durch den Fremdagent in der Basisstation übertragen.

[0064] In der umgekehrten Richtung (Up-Link) werden PPP-Rahmen, die vom Endsystem an die IWF reisen, über den MAC und Air-Link an die Basisstation gesendet. Die Basisstation überträgt diese Rahmen an die IWF in der MSC unter Verwendung des XTunnel-Protokolls. Die IWF liefert sie zur Verarbeitung an einen PPP-Server. Für den Internetzugang kann sich der PPP-Server auf der gleichen Maschine befinden, wie die IWF. Für ISP oder Intranet-Zugang, ist der PPP-Server in einem privaten Netz und die IWF verwendet das Layer-2-Tunneling-Protokoll (L2TP) zur Verbindung damit.

[0065] In der Vorwärtsrichtung (Down-Link) werden die PPP-Rahmen vom PPP-Server durch die IWF unter Verwendung des XTunnel-Protokolls an die Basisstation übertragen. Die Basisstation enttunnelt die Down-Link-Rahmen und übermittelt sie über den Air Link an das Endsystem, wo sie durch die PPP-Schicht des Endsystems verarbeitet werden.

[0066] Zum Unterstützen von Mobilität, wird Unterstützung von Handoffs einbezogen. Die MAC-Schicht unterstützt die Mobilitätsmanagementsoftware in der Basisstation und dem Endsystem, um Handoffs effizient auszuführen. Handoffs werden transparent von den Peer-PPP-Einheiten und dem L2TP-Tunnel verarbeitet. 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 durchqueren den neuen Pfad transparent.

[0067] Das Netz unterstützt Roaming (d.h., wenn sich der Endbenutzer über einen Fremd-wireless-Service-Provider mit seinem Heimat-Wireless-Service-Provider verbindet). Durch die Verwendung dieses Merkmals sind die Endsysteme imstande, vom Heimatnetz weg zu einem Fremdnetz zu roamen und immer noch den Dienst zu bekommen, vorausgesetzt natürlich, dass der Fremd-wireless-Service-Provider und der Heimat-Wireless-Service-Provider des Endsystems eine Servicevereinbarung haben.

[0068] In Fig. 3 ist das roamende Endsystem **60** an einen Standort gereist, an dem der Fremd-Wireless-Service-Provider **62** Abdeckung bereitstellt. Das roamende Endsystem **60** hat indes ein Abonnentenverhältnis mit dem Heimat-Wireless-Service-Provider **70**. In der vorliegenden Erfindung hat der Heimat-Wireless-Service-Provider **70** ein Vertragsverhältnis mit dem Fremd-Wireless-Service-Provider **62** zum Bereitstellen von Zugangsdiensten. Deshalb verbindet sich das roamende Endsystem **60** über den Air Link mit der Basisstation **64** des Fremd-Wireless-Service-Providers **62**. Dann werden Daten vom roamenden Endsystem **60** durch die Basisstation **64** durch die dienende IWF **66** des Fremd-Wireless-Service-Providers **62** an die Heimat-IWF **72** des Heimat-Wireless-Service-Providers **70**, oder möglicherweise durch die Heimat-IWF **72** des Heimat-Wireless-Service-Providers **70** an den Internet Service Provider **74**, übertragen.

[0069] Eine Internet-Service-Provider-Schnittstelle, I-Schnittstelle genannt, wird für Kommunikationen über Grenzen von Wireless Service Providern (WSP) hinweg verwendet, um Roaming zu unterstützen. Diese Schnittstelle wird zum Authentifizieren, Registrieren und zum Transportieren der PPP-Rahmen des Endsystems zwischen dem Fremd-WSP und dem Heimat-WSP verwendet.

[0070] PPP-Rahmen in den Up-Link- und Down-Link-Richtungen reisen durch den Heimat-Wireless-Service-Provider (WSP) des Endsystems. Alternativ reisen die PPP-Rahmen direkt vom Fremd-WSP zum Zielnetz. Die Basisstation im Fremd-WSP ist der Anschlusspunkt des Endsystems im Fremdnetz. Diese Basisstation sendet (und empfängt) PPP-Rahmen zu (und von) einer dienenden IWF in der Mobilvermittlungsstelle des Fremd-WSP. Die dienende IWF verbindet sich über die I-Schnittstelle mit der Heimat-IWF unter Verwendung eines Layer2Tunnels zum Transportieren der PPP-Rahmen des Endsystems in beide Richtungen. Die dienende IWF im Fremd-WSP sammelt Accounting-Daten für das Auditing. Die Heimat-IWF und der Heimat-WSP sammeln Accounting-Daten für die Abrechnung.

[0071] Die dienende IWF im Fremd-WSP kann mit der Basisstation im gleichen System kombiniert werden, wodurch die Notwendigkeit des X-Tunnels beseitigt wird.

[0072] Während der Registrierungsphase bestimmt ein Registrierungsserver im Fremd-WSP die Identität des Heimatnetzes des roamenden Endsystems. Unter Verwendung dieser Informationen kommuniziert der Fremd-Registrierungsserver mit dem Heimat-Registrierungsserver zum Authentifizieren und Registrieren des Endsystems. Diese Registrierungsnachrichten fließen über die I-Schnittstelle. Nachdem das Endsystem authentifiziert und registriert wurde, wird ein Layer2Tunnel zwischen der Basisstation und der dienenden IWF unter Verwendung des XTUNNEL-Protokolls erzeugt und ein zweiter Layer2Tunnel wird über die I-Schnittstelle zwischen der dienenden IWF und der Heimat-IWF erzeugt. Die Heimat-IWF verbindet sich mit dem PPP-Peer des Endsystems wie zuvor, unter Verwendung des L2TP (Level2Tunnel-Protokoll). Während der Handoffs bleibt der Standort des IWF und des L2TP-Tunnels fest. Wenn das Endsystem sich von einer Basisstation zu einer anderen Basisstation bewegt, wird zwischen der neuen Basisstation und der dienenden IWF ein neuer Tunnel erzeugt und der alte Tunnel zwischen der alten Basisstation und der dienenden IWF wird gelöscht. Wenn sich das Endsystem weit genug bewegt, derart, dass eine neue dienende IWF benötigt wird, wird ein neuer Tunnel zwischen der neuen dienenden IWF und der Heimat-IWF erzeugt. Der alte Tunnel zwischen der alten dienenden IFW und der Heimat wird gelöscht.

[0073] Zum Unterstützen von Roaming, unterstützt die I-Schnittstelle Authentifizierungs-, Registrierungs- und Datentransportdienste über Grenzen von Wireless Service Providern hinweg. Die Authentifizierungs- und Registrierungsdienste werden unterstützt unter Verwendung des IETF-Radius-Protokols. Datentransportdienste zum Übertragen von PPP-Rahmen über einen Layer2Tunnel werden unter Verwendung des I-XTunnel-Protokolls unterstützt. Dieses Protokoll ist auf dem IETF-L2TP-Protokoll basiert.

[0074] Wie in dieser Beschreibung verwendet, bezieht sich der Begriff Heimat-IWF auf die IWF im Heimatnetz des Endsystems. Der Begriff dienende IWF bezieht sich auf eine IWF im Fremdnetz, die zeitweilig Dienste für das Endsystem bereitstellt. In gleicher Art und Weise bezieht sich der Begriff Heimat-Registrierungsserver auf den Registrierungsserver im Heimatnetz des Endsystems und der Begriff Fremd-Registrierungsserver bezieht sich auf den Registrierungsserver im Fremdnetz, durch den das Endsystem sich registriert, während es roamt.

[0075] Das Netz unterstützt sowohl die feste als auch die dynamische Zuweisung von IP-Adressen für Endsysteme. Es gibt zwei Typen von IP-Adressen, die berücksichtigt werden müssen. Die erste ist die Identität des Endsystems in seinem Heimatnetz. Dies kann ein strukturierter Benutzername im Format Benutzer@Domäne sein. Dieser 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 verfahren des Aushandelns der PPP IPCP-Adresse zugewiesen wird. Das Domänen-Subfeld der Heimatadresse wird verwendet, um die Heimat-Domäne des Benutzers zu identifizieren und ist ein vollständig qualifizierter Domänenname. Das Benutzer-Subfeld der Heimat-Adresse wird verwendet, um den Benutzer in der Heimat-Domäne zu identifizieren. Der Benutzername wird im Endsystem und in der Abonnentendatenbank in der MSC gespeichert und wird dem Benutzer zugewiesen, wenn er oder sie das System abonniert. Das Domänen-Subfeld des Benutzernamens wird während dem Roaming verwendet, um Roaming-Verhältnisse und den Heimat-Registrierungsserver zu Registrierungs- und Authentifizierungszwecken zu identifizieren. Anstatt eines strukturierten Benutzernamens kann ein anderer eindeutiger Identifikator verwendet werden, um das Heimatnetz des Benutzers und die Identität des Benutzers im Heimatnetz zu identifizieren. Dieser Identifikator wird in der Registrierungsanfrage durch das Endsystem gesendet.

[0076] Die PPP IPCP wird verwendet, um die IP-Adresse für das Endsystem auszuhandeln. Durch die Verwendung des IP-Konfigurationsprotokolls IPCP ist das Endsystem imstande, eine feste oder dynamische IP-Adresse auszuhandeln.

[0077] Obwohl die Verwendung eines strukturierten Benutzernamensfelds und die Nichtverwendung einer

IP-Adresse als die Heimatadresse ein Merkmal ist, das die vorliegende Erfindung gegenüber einem bekannten Mobile IP kennzeichnet, kann das Netz verbessert werden, um ebenfalls Endsysteme zu unterstützen, die keinen Benutzernamen und nur eine Nicht-Null-Heimatadresse haben, wenn Mobile IP und seine Verwendung in Verbindung mit PPP-Endsystemen beliebt wird. Der PPP-Server kann durch den Service Provider konfiguriert werden, um während der IPCP-Adressen-Zuweisungsphase IP-Adressen zuzuweisen, die gleich sind wie die Heimat-IP-Adresse des Endsystems. In diesem Fall werden die Heimatadresse und die IPCP zugeteilte IP-Adresse identisch sein.

[0078] In Fig. 4 bilden die Basisstationen **64** und die Air Links von den Endsystemen das drahtlose Sub-Netz **80**, das die Air Links für den Endbenutzerzugang, mindestens eine Basisstation (z.B. Station **64**) und mindestens ein Backhaul-Netz (z.B. **38** von Fig. 2) von der Basisstation zur MSC **40** (Fig. 2) aufweist. Die drahtlose Sub-Netz-Architektur von beispielsweise einer aus drei Sektoren bestehenden Basisstation enthält die nachfolgenden logischen Funktionen.

1. Zugangspunktfunktion. Die Zugangspunkte **82** führen die MAC-Schicht-Bridging- und MAC-Schicht-Verbindungs- und Trennungsverfahren durch. Ein Zugangspunkt enthält einen Prozessor (vorzugsweise in der Form eines Custom Application Specific Integrated Circuit ASIC), eine Verbindung zu einem drahtlosen Hub (vorzugsweise in der Form einer Ethernet-Verbindung auf einer Karte oder im ASIC gebildet), eine Verbindung zu einer Antenne (vorzugsweise in der Form einer Karte mit einem Daten-Modulator/-Demodulator und einem Sender/Empfänger) und die Antenne, an die das Endsystem gekoppelt ist. Der Prozessor führt Software aus, um eine Daten-Bridging-Funktion und verschiedene andere Funktionen in der Unterstützung der Registrierungs- und Mobilitätsübergaben auszuführen, wie hierin weiter beschrieben werden wird. Siehe Erläuterung in Bezug auf Fig. 7, Fig. 8 und Fig. 11.

   Die Zugangspunkte (APs) nehmen die MAC-Schicht-Rahmen vom Air Link und übertragen sie an den drahtlosen Hub und umgekehrt. Die MAC-Schicht-Verbindungs- und Trennungsverfahren werden durch APs verwendet, um eine Liste von Endsystem-MAC-Adressen in ihrer MAC-Adressen-Filtertabelle beizubehalten. Ein AP führt nur MAC-Schicht-Bridging für Endsysteme aus, deren MAC-Adressen in der Tabelle vorhanden sind. Ein Zugangspunkt und sein verbundener drahtloser Hub sind typischerweise gemeinsam untergebracht. In seiner einfachsten Form ist ein Zugangspunkt einfach ein Port in einen drahtlosen Hub. Wenn die APs und der drahtlose Hub gemeinsam im gleichen Zellenstandort untergebracht sind, können sie über eine IEEE 802.3 Verbindung miteinander verbunden werden. Manchmal sind die Zugangspunkte weit vom drahtlosen Hub entfernt angeordnet und über eine Fernverbindung wie einen Draht-T1-Trunk oder sogar einen drahtlosen Trunk verbunden. Für Zellen mit mehreren Sektoren, werden mehrere Zugangspunkte (d.h. einer pro Sektor) verwendet.

2. Drahtlos-Hub-Funktion. Der drahtlose Hub **84** führt die Fremdagent (FA) Prozeduren, den Backhaul-Belastungsausgleich (z.B. über mehrere T1), die Backhaul-Netzschnittstellenbildung und die XTunnel-Prozeduren aus. Wenn die Unterstützung von Quality of Service (QOS) vorhanden ist, führt der drahtlose Hub die Unterstützung für QOS durch Ausführen des XTunnel-Protokolls über Backhauls mit unterschiedlichen QOS-Attributen aus. In einem Zellenstandort mit mehreren Sektoren, wird eine einzelne Drahtlos-Hub-Funktion typischerweise durch mehrere Zugangspunkte geteilt.

   Ein drahtloser Hub umfasst einen Prozessor, eine Verbindung zu einem oder mehreren Zugangspunkten (vorzugsweise in der Form einer Ethernet-Verbindung auf einer Karte oder in einer ASIC gebildet) und eine Verbindung zu einer Backhaul-Leitung. Die Backhaul-Leitung ist typischerweise eine T1- oder T3-Kommunikationsleitung, die in der Mobilvermittlungsstelle des Wireless Service Providers endet. Die Verbindung zur Backhaul-Leitung formatiert Daten in ein bevorzugtes Format, zum Beispiel, ein Ethernet-Format, ein Frame-Relay-Format oder ein ATM-Format. Der Prozessor des drahtlosen Hubs führt Software aus, um Daten-Bridging und verschiedene andere Funktionen wie hierin beschrieben auszuführen. Siehe Erläuterung in Bezug auf Fig. 9, Fig. 10 und Fig. 11.

[0079] Die Konstruktion der Basisstation unterstützt die folgenden Typen von Zellenarchitekturen.

1. Lokale AP-Architektur. In einer lokalen AP-Architektur haben Zugangspunkte eine große Reichweite (typischerweise > = 2km). Sie sind gemeinsam in der Zelle zum drahtlosen Hub unter Verwendung eines IEEE 802.3 Netzes untergebracht oder können direkt in die Rückwand des drahtlosen Hubs eingesteckt oder mit dem drahtlosen Hub unter Verwendung von irgendeinem anderen Mechanismus (z.B. universeller serieller Bus, Druckerport, Infrarot, usw.) verbunden werden. Es wird angenommen, dass die erste Alternative für den Rest dieser Erläuterung verwendet wird. Der Zellenstandort kann rundstrahlend oder unter Hinzufügen von mehreren Zugangspunkten und sektorierten Antennen zu einem drahtlosen Hub sektoriert werden.

2. Fern-AP-Architektur. In einer Fern-AP-Architektur haben Zugangspunkte gewöhnlich eine sehr kleine Reichweite, typischerweise einen Radius von ungefähr 1 km. Sie sind fern vom drahtlosen Hub angeordnet (entweder drinnen oder draußen). Ein T1- oder drahtloser Trunk verbindet vorzugsweise die Fernzugangspunkte mit dem Zellenstandort, wo der drahtlose Hub angeordnet ist. Vom Zellenstandort wird ein Drahtlei-

tungs-Backhaul oder eine Mikrowellenverbindung typischerweise zur Verbindung mit der IWF oder der MSC verwendet. Wenn zwischen dem Fern-AP und dem drahtlosen Hub Wireless Trunking verwendet wird, werden rundstrahlende oder sektorierte drahtlose Funkvorichtungen für das Trunking verwendet. Die Vorrichtungen für das Trunking zu den Fernzugangspunkten werden vorzugsweise gemeinsam mit dem drahtlosen Hub untergebracht und können mit ihm unter Verwendung eines IEEE 802.3 Netzes verbunden werden oder direkt in die Rückwand des drahtlosen Hubs eingesteckt werden. Auf diese Vorrichtungen wird mit dem Begriff Trunk-AP Bezug genommen.

3. Gemischte AP-Architektur. In einer gemischten Architektur muss das drahtlose Sub-Netz ferne und lokale Zugangspunkte unterstützen. Fernzugangspunkte können hinzugefügt werden, um Löcher zu füllen oder aus anderen Kapazitätsgründen. Wie vorhergehend beschrieben, können T1 oder drahtlose Trunks verwendet werden, um den Fern-AP mit dem drahtlosen Hub zu verbinden.

[0080] Fig. 5 zeigt eine Zelle mit drei Sektoren, die nur lokale APs verwendet. Die Zugangspunkte und der drahtlose Hub sind gemeinsam in der Basisstation untergebracht und mit 802.3 Verbindungen miteinander verbunden.

[0081] Fig. 6 zeigt eine Architektur mit den Fernzugangspunkten **82**, die mit dem drahtlosen Hub **84** unter Verwendung der drahtlosen Trunks **86** verbunden sind. Jeder Trunk-Zugangspunkt in der Basisstation stellt eine drahtlose Punkt-zu-Mehrpunkt-Funkverbindung mit den Fern-Mikrozugangspunkten (in der Figur R-AP) bereit. Die Fernzugangspunkte stellen Air Link Dienst für die Endsysteme bereit. Der drahtlose Hub und die Trunk-Zugangspunkte sind gemeinsam in der Basisstation untergebracht und über 802.3 Verbindungen miteinander verbunden. Diese Figur zeigt ebenfalls die Fernzugangspunkte **82R**, die über die Punkt-zu-Punkt-T1-Verbindungen mit dem drahtlosen Hub verbunden sind. In diesem Szenario sind keine Trunk-APs erforderlich.

[0082] Zum Unterstützen von allen der vorhergehend genannten Zellenarchitekturen und der unterschiedlichen Typen von Zugangspunkten, die jede Zelle verwenden kann, befolgt die Netzarchitektur die nachfolgenden Regeln:

1. Zugangspunktfunktionen wie MAC-Layer-Bridges. Fernzugangspunkte führen MAC-Bridging zwischen dem Air Link zu den Endsystemen und dem drahtlosen oder T1-Trunk zum Zellenstandort aus. Lokale Zugangspunkte führen MAC-Bridging zwischen dem Air Link zu den Endsystemen und dem drahtlosen Hub aus.
2. Trunk-Zugangspunkte funktionieren wie MAC-Layer-Bridges. Sie führen das MAC-Bridging zwischen dem Trunk (der zum Zugangspunkt geht) und dem drahtlosen Hub aus.
3. Der drahtlose Hub ist mit allen gemeinsam untergebrachten MAC-Bridges (d.h. lokale Zugangspunkte oder Trunk-Zugangspunkte) unter anfänglicher Verwendung einer 802.3 Verbindung verbunden.

[0083] Zusätzlich werden, wo lokale Zugangspunkte oder Fernzugangspunkte mit T1-Trunks verwendet werden, die folgenden Regeln befolgt:

1. Die lokalen Zugangspunkte werden gemeinsam mit dem drahtlosen Hub untergebracht und unter Verwendung von Punkt-zu-Punkt 802.3 Verbindungen oder einem Shared 802.3 Netz damit verbunden. Die Fernzugangspunkte sind unter Verwendung von Punkt-zu-Punkt-T1-Trunks mit dem drahtlosen Hub verbunden.
2. Sektorisierung wird durch Hinzufügen von Zugangspunkten mit sektorierten Antennen zu den Zellenstandorten unterstützt.
3. Für jeden mit dem drahtlosen Hub verbundenen Zugangspunkt gibt es eine Systemregistrierung. Die MAC-Schicht-Verbindungsprozeduren werden verwendet, um die MAC-Adressfiltertabellen der Zugangspunkte auf dem Laufenden zu halten und um das MAC-Schicht-Bridging effizient auszuführen. Der drahtlose Hub wirkt an den MAC-Verbindungsprozeduren mit, derart, dass nur gültige MAC-Adressen zu den MAC-Adressfiltertabellen der Zugangspunkte hinzugefügt werden.
4. Der Fremdagent im drahtlosen Hub überträgt Rahmen von den Zugangspunkten an die MSC IFW und umgekehrt unter Verwendung des xtunnel-Protokolls. Die MAC-Adressfiltertabelle wird verwendet, um diese Unicast-MAC-Datenrahmen, deren MAC-Adressen nicht in der Tabelle enthalten sind, herauszufiltern. Die APs leiten die gesendeten MAC-Rahmen und MAC-Rahmen, die mit Registrierungsfunktionen des Endsystems verbunden sind immer weiter, unabhängig von den Inhalten der MAC-Adressfitertabelle.
5. Die lokalen Zugangspunkte verwenden ARP, um MAC-Adressen für das Routing des IP-Verkehrs zum drahtlosen Hub aufzulösen. Umgekehrt verwendet der drahtlose Hub ebenfalls ARP, um IP-Pakete an Zugangspunkte zu routen. UDP/IP wird für das Netzmanagement der Zugangspunkte verwendet.
6. Die Fernzugangspunkte, die über T1 verbunden sind, verwenden kein ARP, da die Verbindung eine Punkt-zu-Punkt-Verbindung ist.

7. Die Unterstützung für Handoffs wird mit Hilfe der MAC-Schicht bereitgestellt.

[0084] In einer Zellenarchitektur, die drahtlose Trunks und Trunk-APs bereitstellt, werden die nachfolgenden Regeln befolgt.

1. Die Trunk-Zugangspunkte sind gemeinsam mit dem drahtlosen Hub untergebracht und mit ihm unter Verwendung von Punkt-zu-Punkt 802.3 Verbindungen oder anderen geeigneten Mitteln verbunden.
2. Die Sektorisierung des drahtlosen Trunks wird durch Hinzufügen von Trunk-Zugangspunkten mit sektorierten Antennen zum Zellenstandort unterstützt.
3. Die Handoffs durch die Backhaul-Sektoren werden unter Verwendung des Fremdagenten im drahtlosen Hub vorgenommen. Für jeden Backhaul-Sektor besteht ein Fremdagent, der im drahtlosen Hub ausgeführt wird.
4. Die Trunk-APs müssen nicht bei der Verbindung und den Handoff-Prozeduren des MAC-Schicht-Endsystems teilnehmen. Ihre MAC-Adressfiltertabellen werden dynamisch durch den drahtlosen Hub programmiert, wenn die Endsysteme sich beim Netz registrieren. Die MAC-Adressfiltertabelle wird verwendet, um Unicast-MAC-Rahmen herauszufiltern. Den gesendeten MAC-Rahmen oder MAC-Rahmen, die Registrierungspakete enthalten, wird der Durchgang immer erlaubt.
5. Die Trunk-APs verwenden ARP, um MAC-Adressen zum Routen des IP-Verkehrs an den drahtlosen Hub aufzulösen. Umgekehrt verwenden die drahtlosen Hubs ARP, um IP-Pakete an Trunk-APs zu routen. UDP/IP wird für das Netzmanagement der Trunk-APs verwendet.
6. In einem einzelnen drahtlosen Trunk-Sektor, erfolgen MAC-Verbindung und Handoffs von einem Zugangspunkt zum anderen unter Verwendung der MAC-Schicht mit der Unterstützung des Fremdagenten im drahtlosen Hub. Unter Verwendung dieser MAC-Schicht-Prozeduren verbinden sich die Endsysteme mit den Zugangspunkten. Wenn sich die Endsysteme von einem Zugangspunkt zu einem anderen Zugangspunkt bewegen, verwenden die Zugangspunkte MAC-Handoff-Protokolle, um ihre MAC-Adressfiltertabellen zu aktualisieren. Der drahtlose Hub am Zellenstandort stellt Unterstützung für die Zugangspunkte zum Ausführen dieser Funktion bereit. Diese Unterstützung enthält das Übertragen der MAC-Schicht-Handoff-Nachrichten (da die Zugangspunkte nicht imstande sind, direkt über die MAC-Schicht miteinander zu kommunizieren) und das Authentifizieren des Endsystems für MAC-Schicht-Registrierung und Handoff und zum Aktualisieren der MAC-Adressfiltertabellen der Zugangspunkte.
7. Der Fremdagent für einen drahtlosen Trunk-Sektor ist verantwortlich für das Übertragen von Rahmen von seinem Trunk-AP an die MSC und umgekehrt unter Verwendung des Xtunnel-Protokolls. Daher achtet der Fremdagent für einen Trunk-AP nicht auf den Standort des Endsystems in Bezug auf die Zugangspunkte innerhalb von diesem drahtlosen Trunk-Sektor. In der Down-Link-Richtung leitet er lediglich die Rahmen vom Tunnel an den geeigneten Trunk-AP weiter, der MAC-Schicht-Bridging verwendet, um die Rahmen an alle Fernzugangspunkte, die in diesem Backhaul-Sektor verbunden sind, zu senden. Die Zugangspunkte konsultieren ihre MAC-Adressfiltertabellen und leiten die MAC-Rahmen entweder über das Zugangsnetz weiter oder lassen die MAC-Rahmen fallen. Wie vorhergehend beschrieben, werden die MAC-Adressfiltertabellen unter Verwendung der MAC-Schichtverbindungs- und Handoffprozeduren auf dem Laufenden gehalten. In der Up-Link-Richtung, werden die MAC-Rahmen durch die Zugangspunkte an die Backhaul-Bridge weitergeleitet, die sie unter Verwendung der 802.3 Verbindung an den Fremdagent im drahtlosen Hub weiterleitet.
8. ARP wird nicht für das Senden oder Empfangen von IP-Paketen an die Fernzugangspunkte verwendet. Die Zugangspunkte bestimmen die MAC-Adresse des drahtlosen Hubs unter Verwendung der BOOTP-Prozeduren. Umgekehrt ist der drahtlose Hub mit der MAC-Adresse der Fernzugangspunkte konfiguriert. UDP/IP wird für das Netzmanagement der Zugangspunkte und für die Systemverbindungs- und Handoffnachrichten verwendet.

[0085] Die IEEE Standard 802.3 Verbindungen im Zellenstandort können durch andere Geschwindigkeitsverbindungen ersetzt werden.

[0086] Fig. 7 zeigt den Protokollstapel für einen lokalen Zugangspunkt. An der Basis des Stapels befindet sich die physische Schicht PHY. Die physische Schicht PHY trägt Daten zu und von einem Endsystem unter Verwendung von zum Beispiel Funkwellen über den Äther. Wenn von einem Endsystem empfangen, empfängt der AP Daten von der physischen Schicht und entpackt sie von den MAC-Rahmen (der MAC-Schicht). Die Datenrahmen des Endsystems werden dann erneut in ein physisches Ethernet-Schicht-Format (IEEE 802.3 Format) gepackt, wo sie über die Ethernet-Verbindung an den drahtlosen Hub gesendet werden. Wenn der AP-Prozessor vom drahtlosen Hub Daten über seine Ethernet-Verbindung (d.h. die physische Schicht) empfängt, die an das Endsystem zu übertragenen Daten, packt der AP die Daten in ein Medium Access Control (MAC) Format und sendet der MAC-Schicht an das Endsystem zu übermittelnde Daten unter Verwendung der PHY Schicht an ihren Modulator.

[0087] In Fig. 8 werden die MAC- und PHY-Schichten an das/vom Endsystem von Fig. 7 durch ein MAC und PHY für den Trunk zum Zellenstandort für einen Fernzugangspunkt ersetzt. Spezifisch für einen T1-Trunk wird das High Level Data Link Control Protokoll (HDLC-Protokoll) vorzugsweise über der T1 verwendet.

[0088] Fig. 9 veranschaulicht den Protokollstapel für den drahtlosen Hub, der das Bridging der Backhaul-Leitung und des Trunks an den Fernzugangspunkt ausführt. Der Trunk zu den Fern-APs ist nur erforderlich, um die Fernzugangspunkte (da getrennt von den Ethernet gekoppelten Zugangspunkten) zu unterstützen. Die MAC- und PHY-Schichten für den drahtlosen Trunk zu den Fern-APs stellen eine Punkt-zu-Mehrpunkt-Verbindung bereit, derart, dass ein Trunk verwendet werden kann, um mit vielen Fern-APs im gleichen Sektor zu kommunizieren.

[0089] Der drahtlose Hub führt das Bridging des Trunks an die Fern-APs und die Backhaul-Leitung (z.B. T1 oder T3) zur Mobilvermittlungsstelle (MSC) des Netzes durch. Der Protokollstapel im drahtlosen Hub führt MAC- und PHY-Schichten auf der MSC aus, auf der eine IP (Internetprotokoll) Schicht ausgeführt ist, auf der eine UDP-Schicht (Universal Datagram Protokoll, auf das kombiniert als UPD/IP Bezug genommen wird) für das Netzmanagement ausgeführt ist, auf der ein xTunnel-Protokoll ausgeführt ist. Das XTunnel-Protokoll ist ein neues Format, das Aspekte von Mobilität (z.B. wie in Mobile IP) und Aspekte des Level2Tunnel-Protokolls (L2TP) aufweist. Das XTunnel-Protokoll wird verwendet, um vom drahtlosen Hub an die MSC und zwischen Interworking-Funktionen (IWFs) in unterschiedlichen Netzen oder dem gleichen Netz zu kommunizieren.

[0090] In Fig. 10 wird der Protokollstapel für die Relayfunktion in der Basisstation zum Unterstützen von Fernzugangspunkten gezeigt. Die Relayfunktion enthält eine Schnittstelle zur Backhaul-Leitung (als drahtloser Hub veranschaulicht) und eine Schnittstelle zum Fern-AP (als ein Trunk-AP veranschaulicht). Aus der Perspektive des drahtlosen Hubs, verhält sich der Trunk-AP (in Fig. 7 und Fig. 10 veranschaulicht) tatsächlich wie der AP, der in Fig. 7 veranschaulicht ist. Vorzugsweise werden die Protokollstapel der Basisstation in einen drahtlosen Hub und einen Trunk-AP mit einem Ethernet dazwischen aufgespaltet. In einem drahtlosen Trunk mit N Sektoren, bestehen N drahtlose Trunk-APs im Zellenstandort und ein drahtloser Hub.

[0091] In Fig. 11 wird der Protokollstapel der Basisstation für eine Zellenarchitektur, die einen lokalen AP verwendet, gezeigt. Die Relayfunktion enthält eine Schnittstelle zur Backhaul-Leitung (als der drahtlose Hub veranschaulicht) und eine Air Link Schnittstelle zum Endsystem (als ein AP veranschaulicht). Aus der Perspektive des drahtlosen Hubs, verhält sich der AP (in Fig. 8 und Fig. 11 veranschaulicht) tatsächlich wie der Trunk-AP, der in Fig. 8 veranschaulicht ist. Vorzugsweise werden die Protokollstapel der Basisstation in einen drahtlosen Hub und einen Trunk-AP mit einem Ethernet dazwischen aufgespaltet. In einer Zelle mit N Sektoren, bestehen N Zugangspunkte im Zellenstandort und ein einzelner drahtloser Hub.

[0092] Das Backhaul-Netz von der Basisstation an die MSC hat die nachfolgenden Attribute.

1. Das Netz ist imstande, IP-Datagramme zwischen der Basisstation und der MSC zu routen.
2. Das Netz ist sicher. Es ist kein öffentliches Internet. Verkehr von vertrauenswürdigen Knoten ist nur auf das Netz hinauf erlaub, da das Netz nicht nur für den Transport des Verkehrs des Endsystems, sondern ebenfalls zum Transportieren von Authentifizierungs-, Accounting-, Registrierungs- und Managementverkehr, verwendet wird.
3. Das Netz hat die notwendigen Leistungseigenschaften.

[0093] In der typischen Anwendung ist der Service Provider verantwortlich für das Installieren und Beibehalten des Backhaul-Netzes auf dem die Ausrüstung installiert ist.

[0094] 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 T3-Teilverbindungen.
2. Die Basisstationen unterstützen IP über Frame-Relay unter Verwendung von T1- oder T3-Teilverbindungen.
3. Die Basisstationen unterstützen IP über AAL5/ATM unter Verwendung von T1- oder T3-Teilverbindungen.
4. Die Basisstationen unterstützen IP über Ethernet-Verbindungen.

[0095] Da alle der vorhergehend genannten Schnittstellen auf IETF-Standard-Einkapselungen basieren, können in der MSC kommerzielle Router verwendet werden, um die physischen Verbindungen des Backhaul-Netzes abzuschließen. Höhere Schichten werden weitergeleitet und durch die verschiedenen Server und andere

Prozessoren verarbeitet.

[0096] Die Endsystem-Registrierungsprozeduren über der MAC-Schicht werden unterstützt. Nachfolgend werden die Endsystem-Registrierungsprozeduren an der MAC-Schicht ignoriert, außer dort, wo sie eine Auswirkung auf die oberen Schichten haben.

[0097] Die Endsysteme können sich für den Dienst auf ihrem Heimatnetz oder von einem Fremdnetz aus registrieren. In beiden Szenarien verwendet das Endsystem einen Fremdagent (FA) in der Basisstation, um einen Anschlusspunkt an das Netz und zum Registrieren zu entdecken. Im ersten Fall ist der FA im Heimatnetz des Endsystems. In letzteren Fall ist der FA in einem Fremdnetz. In beiden Fällen verwendet das Netz eine IWF im Heimatnetz des Endsystems als einen Ankerpunkt (d.h. während der gesamten Session gleich bleibend trotz Mobilität). Die PPP-Rahmen zum und vom Endsystem reisen mit dem FA in der Basisstation an die IWF im Heimatnetz. Wenn das Endsystem in der Heimat ist, wird die Heimat-IWF direkt mittels eines Xtunnel-Protokolls an die Basisstation angeschlossen. Zu beachten ist, dass die Heimat-IWF. mit der Basisstation im gleichen Knoten kombiniert werden kann. Wenn dass Endsystem roamt, wird eine dienende IWF im Fremdnetz über eine I-Schnittstelle mit der Heimat-IWF verbunden. Die dienende IWF überträgt Rahmen zwischen der Basisstation und der Heimat-IWF. Zu beachten ist, dass die Heimat-IWF mit der Basisstation im gleichen Knoten kombiniert werden kann. Von der Heimat-IWF werden Daten an einen PPP-Server, der in der gleichen IWF residieren kann, oder an einen getrennten Server, der das L2TP-Protokoll verwendet, gesendet. Der getrennte Server kann einem privaten Netzbetreiber (z.B. ISP oder Unternehmensintranet), der sich vom Wireless Service Provider unterscheidet, gehören und von ihm betrieben werden. Für die Dauer der Session, bleibt der Standort der Heimat-IWF und des PPP-Servers fest. Wenn sich das Endsystem bewegt während es verbunden ist, muss es sich erneut mit einem Fremdagent registrieren. Es werden indes die gleiche Heimat-IWF und der gleiche PPP-Server weiter verwendet. Ein neuer Xtunnel wird zwischen dem neuen FA und der IWF erzeugt und der alte Xtunnel zwischen dem alten Fremdagent und der IFW wird zerstört.

[0098] Fig. 12 zeigt diese Netzkonfiguration für zwei Endsysteme A und B, deren Heimat-Wireless-Service-Provider der Wireless Service Provider A (WSP-A) ist. Ein Endsystem wird vom drahtlosen Heimat-Netz und das andere von einem drahtlosen Fremdnetz aus registriert. Die Heimat-IWF im WSP-A dient als der Ankerpunkt für beide Endsysteme. Für beide Endsysteme werden Daten an die Heimat-IWF übertragen. Die Heimat-IWF verbindet sich an den PPP-Server eines Internet Service Providers, der ISP-A gehört. Hier wird angenommen, dass beide Endsysteme den gleichen ISP abonniert haben. Wenn dies nicht der Fall wäre, würde die Heimat-IWF ebenfalls mit einer Verbindung zu einem anderen ISP gezeigt.

[0099] Innerhalb des Netzes eines Wireless Service Providers, werden die Daten zwischen den Basisstationen und der IWF unter Verwendung des Xtunnel-Protokolls getragen. Die Daten zwischen der IWF und dem PPP-Server werden unter Verwendung des Level2Tunneling-Protokolls (L2TP) getragen. Die Daten zwischen der dienenden IFW und der Heimat-IWF werden unter Verwendung des I-Xtunnel-Protokolls getragen.

[0100] In einem einfachen Szenario kann die Heimat-IWF-Funktion für einen Benutzer im Heimat-Netz, das einen festen Dienst erfordert, in der Basisstation dynamisch aktiviert werden. Die dienende IWF-Funktion kann ebenfalls für einen roamenden Benutzer in der Basisstation aktiviert werden.

[0101] Im Heimatnetz immer eine IWF zu verwenden hat Vorteile und Nachteile. Ein offensichtlicher Vorteil ist die Unkompliziertheit. Ein Nachteil ist, dass Daten immer zu und von einer möglicherweise fernen Heimat-IWF übertragen werden müssen. Die Alternative ist, alle notwendigen Informationen an die dienende IWF zu senden, derart, dass sie sich mit dem ISP/Intranet des Endsystems verbinden kann und die dienende IWF Accounting-Informationen nahezu in Echtzeit zurück an den Accounting-Server im Heimatnetz senden kann. Diese Funktion ist komplexer auszuführen aber effizienter, da sie die Notwendigkeit, Daten über potentiell große Distanzen vom Fremdnetz an das Heimatnetz zu übertragen, reduziert.

[0102] Ziehen wir zum Beispiel einen Fall in Betracht, in dem ein Benutzer von Chicago nach Hongkong roamt. Wenn sich das Heimatnetz des Benutzers in Chicago befindet und sich der Benutzer unter Verwendung eines Wireless Service Providers in Hongkong registriert, wird der Ankerpunkt in der ersten Konfiguration die Heimat-IWF in Chicago sein und alle Daten müssen von Hongkong nach Chicago und umgekehrt übertragen werden. Die Heimat-IWF in Chicago wird sich mit dem ISP des Benutzers in Chicago verbinden. Bei der zweiten Konfiguration wird dem Benutzer des Endsystems ein ISP in Hongkong zugewiesen. Somit müssen die Daten nicht immer zwischen Chicago und Hongkong hin und her übertragen werden. In der zweiten Konfiguration dient die dienende IWF als der Anker und ändert sich über die Dauer der Session nie, auch wenn sich das Endsystem bewegt. Der Standort des FA kann sich indes als Ergebnis der Bewegung des Endsystems in

Hongkong ändern.

[0103] Fig. 13 zeigt die zweite Netzkonfiguration. In dieser Figur ist das Heimatnetz für die Endsysteme A und B WSP-A. Das Endsystem A registriert sich von seinem Heimatnetz aus unter Verwendung seiner Heimat-IWF als Ankerpunkt und verbindet sich ebenfalls mit seinem ISP-A unter Verwendung des PPP-Servers des ISP. Das Endsystem B registriert sich vom Fremdnetz des WSP-B und verwendet eine dienende IWF, die als Ankerpunkt dient und das Endsystem unter Verwendung des PPP-Servers des ISP mit einem ISP verbindet. In dieser Konfiguration müssen die Daten für das Endsystem B nicht vom Fremdnetz an das Heimatnetz und umgekehrt übertragen werden.

[0104] Damit diese Konfiguration funktionieren kann, müssen nicht nur Roamingvereinbarungen zwischen den Heimat- und Fremd-Wireless-Service-Providern bestehen, sondern ebenfalls Vereinbarungen zwischen dem Fremd-Wireless-Service-Provider und dem Internet Service Provider des Endsystems entweder direkt oder über einen Vermittler bestehen. Im vorhergehenden Beispiel muss nicht nur der Wireless Service Provider in Hongkong eine Geschäftsvereinbarung mit dem Wireless Service Provider in Chicago haben, sondern der WSP in Hongkong muss eine Geschäftsvereinbarung mit dem ISP des Benutzers in Chicago haben und auf den PPP-Server des ISP von Chicago in Hongkong zugreifen oder lokal eine Geschäftsbeziehung mit einem anderen ISP in Hongkong haben, der eine Geschäftsbeziehung für das Roaming mit dem ISP des Benutzers in Chicago hat. Zusätzlich muss der WSP in Hongkong imstande sein, diese Roamingverhältnisse dynamisch zu entdecken, um Benutzerauthentifizierung und Accounting durchzuführen und die geeigneten Tunnel einzurichten.

[0105] Es ist für diese Unternehmen, die im Internet-Infrastrukturgeschäft tätig sind, schwierig, für alle diese Szenarien geeignete Standards im IETF auszuarbeiten. Somit ist eine zu bevorzugende Ausführungsform für die vorliegenden Systeme das Ausführen der einfacheren, potentiell weniger effizienten Konfiguration, wo die IWF im Heimatnetz immer als der Ankerpunkt verwendet wird. Beim Vorhandensein von geeigneten Industriestandardisierungen von Protokollen für Internet-Roaming sollte indes die zweite Konfigurierung als gleichwertige oder alternative Ausführungsform angesehen werden.

[0106] Ein Endsystem muss sich beim drahtlosen Netz registrieren, bevor es PPP starten und Daten senden und empfangen kann. Das Endsystem geht zuerst durch die FA-Entdeckungs- und Registrierungsphasen. Diese Phasen authentifizieren und registrieren das Endsystem beim Wireless Service Provider. Nachdem diese Phasen vorüber sind, startet das Endsystem PPP. Dies enthält die PPP-Verbindungsaufbauphase, die PPP-Authentifizierungsphase und die PPP-Netz-Steuerungsprotokollphase. Nachdem diese Phasen vorüber sind, ist das Endsystem imstande, IP-Pakete unter Verwendung von PPP zu senden und zu empfangen.

[0107] Die nachfolgende Erläuterung nimmt an, dass das Endsystem von einem Fremdnetz aus roamt und sich registriert. Während der FA-Entdeckungsphase, wartet das Endsystem (über seinen Benutzerregistrierungsagent) auf eine Ankündigung durch den Fremdagent oder fordert diese an. Der Benutzerregistrierungsagent verwendet Ankündigungsnachrichten, die durch einen Nah- oder Fremdagent gesendet werden, um die Identität des FA zu enthalten und sich zu registrieren. Während dieser Phase wählt der Benutzerregistrierungsagent des Endsystems einen FA und gibt eine Registrierungsanfrage an ihn aus. Der FA, der als Proxy-Registrierungsagent agiert, leitet die Registrierungsanfrage an seinen Registrierungsserver (den Registrierungsserver im Fremd-WSP) weiter. Der Registrierungsserver verwendet den Benutzernamen von der Anfrage des Benutzerregistrierungsagents, um das Heimatnetz des Endsystems zu bestimmen und leitet die Registrierungsanfrage zur Authentifizierung an einen Registrierungsserver im Heimatnetz weiter. Beim Empfang der Registrierungsanfrage, die durch den Fremd-Registrierungsserver übertragen wird, authentifiziert der Heimat-Registrierungsserver die Identität des Fremd-Registrierungsservers und authentifiziert ebenfalls die Identität des Endsystems. Wenn die Authentifizierung und Registrierung erfolgreich ist, wählt der Heimat-Registrierungsserver eine IWF im Heimatnetz aus, um eine I-Xtunnel-Verbindung zwischen der Heimat-IWF und der dienenden IWF (im Fremd-WSP) zu erzeugen. Die IWF im Heimatnetz dient als der Ankerpunkt für die Dauer der PPP-Session.

[0108] Nachdem die Authentifizierungs- und Registrierungsphasen vorüber sind, werden die verschiedenen PPP-Phasen gestartet. Beim Start des PPP, wird eine L2TP-Verbindung zwischen der Heimat-IWF und dem angeforderten ISP/Intranet PPP-Server erzeugt. In der PPP-Authentifizierungsphase, werden PPP-Passwörter unter Verwendung von Password Authentication Protocol (PAP) oder Challenge Authentication Protocol CHAP ausgetauscht und der ISP oder Intranet PPP-Server authentifiziert die Identität des Endsystems unabhängig.

[0109] Wenn dies erfolgreich ist, wird die PPP-Netzsteuerungsphase gestartet. In dieser Phase, wird eine IP-Adresse ausgehandelt und dem Endsystem durch den PPP-Server zugewiesen und die Verwendung von TCP/IP-Header-Kompression wird ebenfalls ausgehandelt. Wenn dies abgeschlossen ist, ist das Endsystem imstande, IP-Pakete unter Verwendung von PPP an seinen ISP oder ein Unternehmensintranet zu senden und zu empfangen.

[0110] Es ist anzumerken, dass zwei Ebenen von Authentifizierung ausgeführt werden. Die erste Authentifizierung authentifiziert die Identität des Endsystems für den Registrierungsserver im Heimatnetz und die Identitäten des Fremdnetzes und des Heimatnetzes füreinander. Um diese Funktion durchzuführen, leitet der Fremdagent die Registrierungsanfrage des Endsystems unter Verwendung von, zum Beispiel, einem IETF-Radius-Protokoll an einen Registrierungsserver in seiner lokalen MSC in einem Radius-Access-Request-Paket weiter. Durch Verwendung des Domänennamens des Endsystems bestimmt der Fremd-Registrierungsserver die Identität des Heimatnetzes und des Heimat-Registrierungsservers des Endsystems und verkapselt und leitet die Anfrage an den Heimat-Registrierungsserver des Endsystems weiter, indem er wie ein Radius-Proxy agiert. Wenn der Fremd-Registrierungsserver die Identität der Heimat des Endsystems nicht bestimmen kann, kann er die Radius-Anfrage wahlweise an einen Registrierungsserver weiterleiten, der wie ein Broker agiert (z.B. einer, der einem Konsortium von Wireless Service Providern gehört), der wiederum das Proxying des Radius Access Request an den endgültigen Heimat-Registrierungsserver vornehmen kann. Wenn der lokale Registrierungsserver nicht imstande ist, die Registrierungsanfrage lokal oder durch Proxying zu bedienen, weist er die Registrierungsanfrage des Fremdagenten zurück und der Fremdagent weist die Registrierungsanfrage des Endsystems zurück. Beim Empfang des Radius Access Requests, führt der Heimat-Registrierungsserver die erforderliche Authentifizierung der Identitäten des Fremdnetzes und des Endsystems durch. Wenn die Authentifizierung und die Registrierung erfolgreich sind, antwortet der Heimat-Registrierungsserver mit einem Radius-Access-Response-Paket an den Fremdregistrierungsserver, der eine Antwort an den Fremdagent sendet, derart, dass ein Round Trip abgeschlossen werden kann. Die Registrierungsanfrage wird zurückgewiesen, wenn der Heimat-Registrierungsserver aus irgendeinem Grund nicht imstande ist, den Bedingungen zu entsprechen.

[0111] Die zweite Ebene der Authentifizierung überprüft die Identität des Endsystems für den PPP-Server des Intranets oder ISP. Die PPP-Authentifizierung separat von der Mobilitätsauthentifizierung, ermöglicht es der Infrastrukturausrüstung, separat vom ISP verteilt und besessen zu werden.

[0112] Fig. 14 ist ein Leiterdiagramm, das die Registrierungsabfolge für ein roamendes Endsystem zeigt. Es wird angenommen, dass der PPP-Server und die Heimat-IWF im gleichen Server sind und dass L2TP nicht erforderlich ist. Es ist anzumerken, dass die Interaktionen mit den Accounting-Servern zum Starten des Accountings für das registrierende Endsystem und ebenfalls die Directory-Server ausgeführt wird, um die Identität des Heimat-Registrierungsservers zu bestimmen und die Identität des Endsystems zu authentifizieren. Mehr Informationen über Accounting, Abrechnung, Roaming (zwischen Service Providern) und Bereinigung werden nachstehend bereitgestellt.

[0113] Zum Initiieren von Agent Solicitation können MAC-Schicht-Nachrichten vom Benutzer-Registrierungsagent des Endsystems verwendet werden. Die MAC-Schicht-Nachrichten werden nicht zur Verdeutlichung gezeigt.

[0114] In Fig. 14 fordert das (mobile) Endsystem anfangs eine Ankündigung an und der Fremdagent antwortet mit einer Ankündigung, die das Endsystem mit Informationen über das Netz, zu dem der Fremdagent gehört, einschließlich einer Care-of-Adresse des Fremdagents, versieht. Alternativ kann diese Phase entfernt werden und alle Netzankündigungen können durch eine kontinuierlich ausgegebene MAC-Schicht-Beacon-Nachricht ausgeführt werden. In diesem Fall wird angenommen, dass das Netz ein Fremd-Wireless-Service-Provider ist. Dann nimmt ein Benutzer-Registrierungsagent (im Endsystem) die Informationen über den Fremdagent (einschließlich Benutzername und anderer Security Credentials) und sein Netz in eine Anfrage auf und sendet die Anfrage an den Fremdagent. Der Fremdagent, als ein Proxy-Registrierungsagent, übermittelt die Anfrage an den Fremd-Registrierungsserver (d.h. den Registrierungsserver für den Wireless Service Provider). Dann greift der Fremd-Registrierungsserver, der erkennt, dass er nicht in der Heimat-Directory ist, auf den Fremd-Directory-Server mit der FDD im Fremd-Wireless-Service-Provider zu, um zu erfahren, wie die Registrierungsanfrage an den Heimat-Registrierungsserver des Wireless Service Providers, zu dem das Endsystem gehört, zu richten ist. Der Fremdregistrierungsserver antwortet mit den erforderlichen Weiterleitungsinformationen. Dann verkapselt der Fremd-Registrierungsserver die Registrierungsanforderung des Endsystems in einem Radius Access Request und übermittelt die verkapselte Anfrage an den Heimat-Registrierungsserver des Wireless Service Providers, zu dem das Endsystem gehört. Der Heimat-Registrierungsserver greift

auf den Heimat-Directory-Server mit der HDD des Heimat-Registrierungsservers zu, um mindestens Authentifizierungsinformationen über den Fremd-Service-Provider zu erfahren. Wahlweise greift der Heimat-Registrierungsserver auf die Directory des Abonnenten zu, um detaillierte Abonennten-Serviceprofil-Informationen (z.B. abonnierte Quality of Service Optionen, usw.) zu erkennen. Wenn alle Parteien authentifiziert sind, sendet der Heimat-Registrierungsserver eine Start-IWF-Anfrage an Heimat-IWF und PPP-Server. Heimat-IWF und PPP-Server starten den Heimat-Accounting-Server und senden dann eine Start-IWF-Antwort an den Heimatregistrierungsserver. Der Heimatregistrierungsserver sendet dann eine Radius Access Response an den Fremdregistrierungsserver. Der Fremdregistrierungsserver sendet dann eine Start-IFW-Anfrage an den dienenden IWF-Server. Der dienende IWF-Server startet den dienenden Accounting-Server und sendet dann eine Start-IWF-Antwort an den Fremdregistrierungsserver. Der Fremd-Registrierungsserver sendet eine Registrierungsantwort an den Fremdagent und der Fremdagent übermittelt die Registrierungsantwort an das Endsystem.

[0115] Eine Link Control Protokoll (LCP) Konfigurierungsanfrage wird durch das Endsystem über den Fremd-Registrierungsserver an Heimat-IWF und PPP-Server gesendet. Heimat-IWF und PPP-Server senden eine LCP-Konfigurierungsbestätigung durch den Fremd-Registrierungsserver an das Endsystem.

[0116] In ähnlicher Weise wird eine Password Authentication Protokoll (PAP) Authentifizierungsanfrage an Heimat-IWF und PPP-Server gesendet und durch sie bestätigt. Alternativ kann ein Challenge Authentication Protokoll (CHAP) zum Authentifizieren verwendet werden. Beide Protokolle können verwendet werden, oder diese Phase kann übersprungen werden.

[0117] In ähnlicher Weise wird eine IP Configuration Protokoll (IPCP) Konfigurierungsanfrage an Heimat-IWF und PPP-Server gesendet und durch sie bestätigt.

[0118] Die Verbindung mit dem Endsystem kann aus einem der nachfolgenden Gründe beendet werden.

1. Durch den Benutzer eingeleitete Beendigung. Bei diesem Szenario beendet das System zuerst elegant das PPP. Dies enthält das Beenden des PPP Netzsteuerungsprotokolls (IPCP) gefolgt durch das Beenden des PPP-Verbindungsprotokolls. Wenn dies erfolgt ist, nimmt das Endsystem die Registrierung vom Netz durch Beenden der Funkverbindung zum Zugangspunkt zurück.
2. Verlust der drahtlosen Verbindung. Dieses Szenario wird durch das Modem ermittelt und an den Modemtreiber im Endsystem gemeldet. Die oberen Schichten der Software werden benachrichtigt, die Stapel zu beenden und den Benutzer zu benachrichtigen.
3. Verlust der Verbindung mit dem Fremdagent. Dieses Szenario wird durch den Mobility-Treiber im Endsystem ermittelt. Nachdem versucht wurde, den Kontakt mit einem (potentiell neuen) Fremdagenten wieder aufzunehmen und dies gescheitert ist, sendet der Treiber eine geeignete Benachrichtigung den Protokollstapel hinauf und signalisiert ebenfalls der Modemhardware unten, die drahtlose Verbindung zu beenden.
4. Verlust der Verbindung mit der IWF. Dies ist im Wesentlichen gleich wie der Verlust der Verbindung mit dem Fremdagent.
5. Beendigung von PPP durch IWF oder PPP-Server. Dieses Szenario wird durch die PPP-Software im Endsystem ermittelt. Der PPP-Treiber des Endsystems wird über dieses Ereignis benachrichtigt. Er initiiert die Aufhebung der Registrierung vom Netz, gefolgt von der Beendigung der drahtlosen Verbindung mit dem Zugangspunkt.

[0119] Die Endsystem-Dienstkonfiguration bezieht sich auf das Konzept des Konfigurierens des Netzdienstes für ein Endsystem basierend auf dem Serviceprofil des Abonnenten. Das Serviceprofil des Abonnenten ist in einer Abonnenten-Directory gespeichert. Das Service-Profil enthält Informationen, um es der Software zu ermöglichen, drahtlose Datendienste für den Abonnenten zu personalisieren. Dies beinhaltet Informationen zum Authentifizieren des Endsystems, und es dem Endsystem zu erlauben, zu roamen und Verbindungen mit dem Internet Service Provider des Endsystems einzurichten. vorzugsweise enthalten diese Informationen andere Parameter wie Quality of Service. Zusätzlich zur Directory des Abonnenten werden eine Heimat-Domänen-Directory (HDD) und eine Fremd-Domänen-Directory (FDD) für Roaming und das Authentifizieren der Fremd- und Heimat-Registrierungsserver miteinander verwendet. Die HDD speichert Informationen über das Heimatnetz des Endsystems und die FDD speichert Informationen über Fremdnetze, die der Abonnent besuchen kann.

[0120] Fig. 15 zeigt, wie diese Directories in die Netzarchitektur gemappt werden und während der Registrierung für ein Endsystem, das sich in der Heimat registriert, verwendet werden. Bei Schritt **0** fordert das (mobile) Endsystem eine Ankündigung vom Fremdagent an und empfängt sie, um das Endsystem mit Informationen über das Netz, zu dem der Fremdagent gehört, zu versorgen. In diesem Fall, ist das Netz der Heimat-Wire-

less-Service-Provider. Bei Schritt **1** gliedert der Benutzerregistrierungsagent (im Endsystem) die Informationen über den Fremdagent und sein Netz und seine Security Credentials in eine Anfrage ein und sendet die Anfrage an den Fremdagent. Bei Schritt **2** überträgt der Fremdagent als ein Proxy-Registrierungsagent die Anfrage an den Heimat-Registrierungsserver. Bei Schritt **3**, greift der Heimat-Registrierungsserver auf die HDD des Heimat-Wireless-Service-Providers zu, um mindestens die Authentifizierungsinformationen zu erfahren. Bei Schritt **4** greift der Heimat-Registrierungsserver auf die Abonnenten-Directory zu, um detaillierte Abonnenten-Serviceprofilinformationen (z.B. die abonnierten Quality of Service Optionen, usw.) zu erfahren. Bei Schritt **5**, benachrichtigt der Heimat-Registrierungsserver den Fremdagent über die Zugangsantwort. Bei den Schritten **6** und **7** benachrichtigt der Fremdagent das Endsystem (d.h. mobil).

[0121] Fig. 16 zeigt die Directory-Verwendung für ein Endsystem, das sich von einem Fremdnetz aus registriert. Bei Schritt **0** fordert das (mobile) Endsystem eine Ankündigung vom Fremdagent an und der Fremdagent kündigt an, was das Endsystem mit Informationen über das Netz, zu dem der Fremdagent gehört, versieht. In diesem Fall ist das Netz ein Wireless Service Provider. Bei Schritt **1** gliedert der Benutzerregistrierungsagent (im Endsystem) die Informationen über den Fremdagent und sein Netz und seine Security Credential in eine Anfrage ein und sendet die Anfrage an den Fremdagent. Bei Schritt **2** überträgt der Fremdagent als ein Proxy-Registrierungsagent die Anfrage an den Fremd-Registrierungsserver (d.h. der Fremd-Registrierungsserver für den Fremd-Wireless-Service-Provider). Bei Schritt **3** greift der Fremd-Registrierungsserver auf die HDD des Fremd-Wireless-Service-Providers zu, um das Netz zu erfahren, zu dem das Endsystem gehört. Bei Schritt **4** leitet der Fremd-Registrierungsserver die Anfrage des Endsystems an den Heimat-Registrierungsserver des Heimat-Wireless-Service-Providers des Endsystems weiter. Bei Schritt **5** greift der Heimat-Registrierungsserver auf die FDD des Heimat-Registrierungsservers zu, um mindestens Authentifizierungsinformationen über den Fremd-Service-Provider zu erfahren. Bei Schritt **6** greift der Heimat-Registrierungsserver auf die Abonnenten-Directory zu, um detaillierte Abonnenten-Serviceprofilinformationen (z.B. die abonnierten Quality of Service Optionen, usw.) zu erfahren. Bei Schritt **7** benachrichtigt der Heimat-Registrierungsserver den Fremd-Registrierungsserver über die Zugangsantwort. Bei Schritt **8** leitet der Fremd-Registrierungsserver die Zugangsantwort an den Fremdagent weiter. Bei Schritt **9** benachrichtigt der Fremdagent das Endsystem (d.h. mobil) über die Registrierungsantwort.

[0122] Protokoll-Handling-Szenarien verarbeiten Trägerdaten und die verbundenen Stapel zum Transportieren von Trägerdaten zu und von einem Endsystem. Die Protokollstapel für die Zellenarchitekturen verwenden lokale APs (Fig. 17) und Fern-APs (Fig. 18).

[0123] Fig. 17 zeigt die Protokollstapel zum Handhaben von Kommunikationen zwischen einem Endsystem (in seinem Heimatnetz) und einer Heimat-IWF für Endsystem @ Heimat. Fig. 17 zeigt das Protokoll-Handling für eine Zellenarchitektur, wo der Zugangspunkt und der drahtlose Hub gemeinsam untergebracht sind.

[0124] Fig. 18 zeigt das Protokoll-Handling für eine Zellenarchitektur, wo der Zugangspunkt fern vom drahtlosen Hub angeordnet ist. Wie gezeigt, endet das PPP in der IWF und die Konfiguration stellt direkten Internet-Zugang bereit. Die Konfiguration für den Fall, in dem der PPP-Server separat von der IWF angeordnet ist, wird später beschrieben.

[0125] In Fig. 18 sind PPP-Rahmen vom Endsystem in RLP (Funkverbindungsprotokoll) Rahmen verkapselt, die am Fernzugangspunkt in MAC-Rahmen zum Kommunizieren mit dem Trunk-Zugangspunkt (d.h. ein Zugangspunkt, der physisch in der Nähe des drahtlosen Hubs angeordnet ist) verkapselt sind, wobei der Fernzugangspunkt durch zum Beispiel einen drahtlosen Trunk an den Zugangspunkt gekoppelt ist) verkapselt sind. Der Zugangspunkt wirkt als eine MAC-Layer-Bridge und überträgt Rahmen vom Air Link zum Fremdagent im drahtlosen Hub. Der Fremdagent entkapselt die RLP-Rahmen aus den MAC-Rahmen und überträgt die RLP-Rahmen unter Verwendung des Xtunnel-Protokolls an die IWF. Ein gleichartiges, wenn auch umgekehrtes Verfahren erfolgt für das Übermitteln von Rahmen von der IWF an das Endsystem.

[0126] Wenn sich das Endsystem zu einem anderen Fremdagent bewegt, wird ein neuer Xtunnel automatisch zwischen dem neuen Fremdagent und der IWF erzeugt, derart, dass der PPP-Verkehr zwischen ihnen ohne Unterbrechung weiter fließt.

[0127] In der Fern-AP-Zellenarchitektur (Fig. 18), die drahtlose Trunks zwischen der Fern-AP und der Trunk-AP verwendet, kann der Air Link zwischen dem Endsystem und dem Zugangspunkt bei einer unterschiedlichen Frequenz (f1) wirken und eine im Vergleich zur Frequenz (f2) und der Funktechnologie des Trunks unterschiedliche Funktechnologie verwenden.

[0128] Fig. 19 zeigt die Protokollstapel für ein roamendes Endsystem. Die dienende IWF verwendet das I-Xtunnel-Protokoll zwischen der dienenden IWF und der Heimat-IWF. Der Rest der Protokollstapel bleibt unverändert und wird nicht gezeigt. Diese Architektur kann vereinfacht werden durch Einverleiben der dienenden IWF in die Basisstation, wodurch das XWD-Protokoll beseitigt wird.

[0129] Die RLP-Schicht verwendet Ablaufnummern, um doppelte PPP-Datagramme fallen zu lassen und die PPP-Datagramme zwischen dem Endsystem und der IWF in Reihe zu liefern. Sie stellt ebenfalls einen konfigurierbaren Keep-Alive-Mechanismus bereit, um die Verbindungskonnektivität zwischen dem Endsystem und der IWF zu überwachen. Zusätzlich stellt die RLP-Schicht in einer alternativen Ausführungsform ebenfalls Rückübertragungs- und Flusskontrolldienste bereit, um die Gesamtbitfehlerrate der Verbindung zwischen dem Endsystem und der IWF zu reduzieren. Das RLP zwischen dem Endsystem und der IWF wird am Anfang der Session gestartet und bleibt über die gesamte Session und sogar über die Handoffs hinweg aktiv.

[0130] Im Gegensatz zu der Spezifizierung in der Mobile IP RFC (RFC 2003), wird IP in der IP-Einkapselung nicht für das Tunneling zwischen dem Fremdagent und der Heimat-IWF verwendet. Stattdessen wird ein neues Tunneling-Protokoll verwendet, das zu Oberst auf dem UDP ausgeführt wird. Dieses Tunnelingprotokoll ist eine vereinfachte Version des L2TP-Protokolls. Die Gründe für diese Wahl sind die folgenden.

1. Das in RFC 2003 spezifizierte Einkapselungsprotokoll stellt keine Flusskontrolle oder Lieferung von Paketen in Reihe bereit. Das vorliegend beschriebene Netz kann diese Dienste im Tunnel über dem Backhaul benötigen. Flusskontrolle kann erforderlich sein, um die Menge an Rückübertragungen über den Air Link aufgrund von Paketverlust wegen Flusskontrollproblemen über dem Netz zwischen der Basisstation und der MSC oder aufgrund von Flusskontrollproblemen in der Basisstation oder der IWF zu reduzieren.
2. Mit der Verwendung eines UDP-basierten Tunnelingprotokolls kann die Ausführung auf Benutzerebene vorgenommen werden und dann aus Leistungsgründen in den Kernel eingefügt werden, nachdem sein Fehler beseitigt wurde.
3. Bei der Verwendung von RFC 2003 gibt es keine einfache Möglichkeit, unter Berücksichtigung von Quality of Service und Belastungsausgleich Tunnel zu erzeugen. Um QOS zu berücksichtigen, sollte es möglich sein, Tunnel über Verbindungen, die bereits die erforderliche QOS bereitstellen, einzurichten. Zweitens gibt es bei der Verwendung von RFC 2003 keine einfache Möglichkeit, Belastungsausgleich bereitzustellen, um Trägerverkehrsbelastung über mehrere Verbindungen zwischen der Basisstation und der MSC zu verteilen.
4. Zum Ausführen von IP in der IP-Verkapselung, wie in RFC 2003 spezifiziert, benötigen die Entwickler Zugang zum IP-Quellcode. In kommerziellen Betriebssystemen, ist der Quellcode des TCP/IP-Stapels allgemein proprietär von anderen Ausrüstungs-Herstellern. Der Kauf des TCP/IP-Stapels von einem Lieferanten und das Verändern der IP-Schicht zum Unterstützen von Mobile-IP-Tunneling würden erfordern, dass ein Entwickler eine kontinuierlich abweichende Version des TCP/IP-Stapels unterstützt. Dies führt zu zusätzlichen Kosten und Risiken.

[0131] Obwohl angemerkt wird, dass das Tunneling-Protokoll zwischen der Basisstation und der IWF nicht dem Standard entspricht und dass der Wireless Service Provider nicht imstande ist, Ausrüstungen von unterschiedlichen Lieferanten zu mischen und anzupassen, ist die Verwendung eines nicht dem Standard entsprechenden Tunneling-Protokolls innerhalb des Netzes eines Wireless Service Providers für die Endsysteme und Ausrüstungen von anderen Lieferanten transparent.

[0132] Das neue Tunneling-Protokoll basiert auf L2TP. L2TP selbst ist ein schwergewichtiges Tunneling-Protokoll, derart, dass, bei L2TP ein erheblicher Overhead mit der Tunnelerzeugung und Authentifizierung verbunden ist. Das neue Tunneling-Protokoll des vorliegenden Systems hat weniger Overhead. Das neue Xtunnel-Protokoll hat die nachfolgenden Merkmale.

1. Die Xtunnel-Erzeugung fügt Radius Access Request und Radius Access Response Nachrichten zwischen der Basisstation und dem Registrierungsserver lieferantenspezifische Erweiterungen hinzu. Diese Erweiterungen handeln Tunnelparameter aus und erzeugen den Tunnel.
2. Der Registrierungsserver ist imstande, die tatsächliche Arbeit des Tunnelings und des Übertragens der Pakete an eine unterschiedliche IP-Adresse und infolgedessen an einen unterschiedlichen Server in der MSC zu delegieren. Dies ermöglicht es dem Registrierungsserver, Belastungsausgleich über mehrere IWF-Server vorzunehmen und unterschiedliche QOS für verschiedene Benutzer bereitzustellen.
3. Das Xtunnel-Protokoll unterstützt In-Band-Kontrollnachrichten für Tunnelmanagement. Diese Nachrichten umfassen Echo-Anfrage/Antwort auf Testtunnelkonnektivität, Trennungs-Anfrage/Antwort/Benachrichtigung zum Trennen des Tunnels und Fehlerbenachrichtigen für Fehlerbenachrichtigungen. Diese Nachrichten werden über das Tunnelingmedium, zum Beispiel UDP/IP gesendet.
4. Das Xtunnel-Protokoll sendet Nutzlast-Daten über das Tunneling-Medium, zum Beispiel UPD/IP. Das Xtunnel-Protokoll unterstützt Flusskontrolle und in Reihe Lieferung von Paketen.

5. Das Xtunnel-Protokoll kann für Quality of Service über Medien ausgeführt werden, die sich von UDP/IP unterscheiden.

[0133] Das Netz unterstützt direkte Internet-Konnektivität durch Beendigung des PPP in der Heimat-IWF und Routing von IP-Paketen von der IWF an das Internet über einen Router, der Standard-IP-Routing-Techniken verwendet. Vorzugsweise führt die IWF Routing Information Process (RIP) aus und der Router führt ebenfalls RIP und möglicherweise andere Routing-Protokolle wie Open Shortest Path First (OSPF) aus.

[0134] Das Netz unterstützt eine erste Konfigurierung für einen Wireless Service Provider, der ebenfalls ein Internet Service Provider ist. In dieser Konfigurierung funktioniert die Heimat-IWF in der MSC ebenfalls als ein PPP-Server. Diese IWF führt ebenfalls Internet Routing Protokolle wie RIP aus und verwendet einen Router, um sich mit dem Backbone-Netz des Internet Service Providers zu verbinden.

[0135] Das Netz unterstützt eine zweite Konfigurierung für einen Wireless Service Provider, der es den Endsystemen ermöglichen möchte, sich mit einem oder mehreren Internet Service Providern zu verbinden, entweder, weil der WSP selbst kein ISP ist, oder, weil der WSP Vereinbarungen mit anderen ISPs hat, um Zugang für Endbenutzer bereitzustellen. Zum Beispiel kann ein Wireless Service Provider wählen, Netzzugang für einen Benutzer anzubieten und eine Vereinbarung mit einem dritten ISP haben, um es dem Benutzer, der ebenfalls ein Account bei einem dritten ISP hat, zu erlauben, vom WSP-Netz auf den ISP zuzugreifen. In dieser Konfiguration wird der PPP-Server nicht in der Heimat-IWF, die bei der MSC installiert ist, ausgeführt. Stattdessen wird ein Tunneling-Protokoll wie L2TP (Layer2Tunneling-Protokoll) zum Tunneln zurück zum PPP-Server des ISP verwendet. **Fig. 10** zeigt die Protokollstapel für diese Konfiguration für ein Endsystem, das in der Heimat ist.

[0136] Der Standort der Heimat-IWF und des PPP-Servers des ISP bleiben über die gesamte PPP-Session hinweg fest. Auch der L2TP-Tunnel zwischen der IWF und dem PPP-Server des ISP bleiben über die gesamte PPP-Session bestehen. Die physische Verbindung zwischen der IWF und dem PPP-Server erfolgt über einen Router unter Verwendung eines dedizierten T1- oder T3 oder Frame-Relays oder ATM-Netzes. Die tatsächliche Natur der physischen Verbindung ist aus der Perspektive der Architektur nicht wichtig.

[0137] Diese Konfiguration unterstützt ebenfalls Intranet-Zugang. Für den Intranet-Zugang residiert der PPP-Server im Unternehmensintranet und die Heimat-IWF verwendet L2TP, um zu ihm zu tunneln.

[0138] Für ein festes Endsystem ist das Protokoll-Handling für Intranet- oder ISP-Zugang wie in **Fig. 20** gezeigt, mit dem Unterschied, dass das roamende Endsystem eine dienende IWF verwendet, um sich mit seiner Heimat-IWF zu verbinden. Das Protokoll-Handling zwischen einer dienenden IWF und einer Heimat-IWF wurde vorhergehend beschrieben. In **Fig. 20** kann die dienende Heimat-IWF in den drahtlosen Hub integriert werden, wodurch das X-Tunnel-Protokoll beseitigt wird. Die dienende IWF kann ebenfalls in den drahtlosen Hub integriert werden, wodurch das X-Tunnel-Protokoll beseitigt wird.

[0139] **Fig. 21** zeigt die Protokollstapel, die während der Registrierungsphase (Endsystemregistrierung) für eine lokale AP-Zellenarchitektur verwendet werden. Der Stapel für eine Fern-AP-Zellenarchitektur ist sehr gleichartig.

[0140] Das vorhergehend gezeigte Szenario ist für ein roamendes Endsystem. Für ein Endsystem in der Heimat besteht kein Fremd-Registrierungsserver im Registrierungspfad.

[0141] Zu bemerken ist der Mobilitätsagent im Endsystem. Der Mobilitätsagent im Endsystem und der Fremdagent im drahtlosen Hub sind konzeptuell gleichartig wie die Mobile IP RFC 2002. Der Mobilitätsagent verarbeitet Netzfehler unter Verwendung von Timeouts und Wiederholungsversuchen. Anders als die bekannten Protokollstapel für Trägerdaten, wird RLP nicht verwendet. Der Fremdagent und die Registrierungsserver verwenden Radius über UDP/IP, um miteinander für die Registrierung des Endsystems zu kommunizieren.

[0142] Verschiedene Sicherheitsaspekte müssen beachtet werden. Als Erstes, das Authentifizieren der Identitäten des Endsystems und der Fremd-/Heimatnetze während der drahtlosen Registrierungsphase. Als Zweites das Authentifizieren der Identität des Endsystems mit seinem PPP-Server während der PPP-Authentifizierungsphase. Als Drittes die Authentifizierung zum Speichern von Accounting-Daten, zur Abrechnung und zum Aktualisieren der Heimat-Domäneninformationen. Als Viertes die Verschlüsselung des Trägerverkehrs, der an das und vom Endsystem übermittelt wird. Als Fünftes die Verschlüsselung zum Austauschen von Abrechnungsinformationen über die Grenzen der Service Provider hinweg.

[0143] Shared Secrets werden verwendet, um die Identität von Endsystemen mit ihren Heimatnetzen und die Identität der Heimat- und Fremdnetze miteinander während der drahtlosen Registrierung zu authentifizieren.

[0144] Die Authentifizierung des Endsystems verwendet ein 128-Bit Shared Secret, um einen Authentikator für ihre Registrierungsanfrage zu erzeugen. Der Authentikator wird unter Verwendung bekannter MD5-Message-Digest-Algorithmen, wie in der Mobile IP RFC 2002 beschrieben, erzeugt. Alternativ kann ein unterschiedlicher Algorithmus verwendet werden. Das Shared Secret wird nicht in der Registrierungsanfrage durch das Endsystem gesendet. Nur der Authentikator wird gesendet. Beim Empfangen der Registrierungsanfrage vom Endsystem berechnet der Heimat-Registrierungsserver den Authentikator über die Daten der Registrierungsanfrage unter Verwendung des Shared Secrets neu. Wenn der berechnete Authentikator-Wert zum durch das Endsystem gesendeten Authentikator-Wert passt, ermöglicht der Heimat-Registrierungsserver die Fortsetzung des Registrierungsverfahrens. Wenn die Werte nicht passen, logt der Server das Ereignis, erzeugt einen Sicherheitsverletzungsalarm und eine Nak (d.h. eine negative acknowledgement – negative Bestätigung) für die Anfrage.

[0145] In der Registrierungsantwort macht der Registrierungsserver das Gleiche – das heißt, er verwendet das Shared Secret, um einen Authentikator für die Registrierungsantwort, die er an das Endsystem sendet, zu erzeugen. Beim Empfangen der Antwort berechnet das Endsystem den Authentikator unter Verwendung des Shared Secrets neu. Wenn der berechnete Wert nicht zum Authentikator-Wert passt, der durch den Heimat-Registrierungsserver in der Antwort gesendet wurde, weist das Endsystem die Antwort zurück und startet einen neuen Versuch.

[0146] Diese Netzsicherheitskonzepte sind gleichartig wie die Konzepte, die im Mobile IP RFC 2002 definiert sind. Gemäß dem RFC, existiert zwischen jedem Endsystem und seinem Heimatnetz eine Mobility-Security-Association. Jede Mobility-Security-Association definiert eine Sammlung von Sicherheitskontexten. Jeder Sicherheitskontext definiert einen Authentifizierungsalgorithmus, einen Modus, ein Secret (Shared oder öffentlich-privat), einen Replay-Protection-Typ und den zu verwendenden Verschlüsselungstyp. Im Kontext des vorliegenden Netzes, wird der Benutzername des Endsystems (anstatt der Mobile IP Heimatadresse) verwendet, um die Mobility-Security-Association zwischen dem Endsystem und seinem Heimatnetz zu identifizieren. Ein anderer Parameter, Sicherheitsparameterindex (SPI) genannt, wird verwendet, um einen Sicherheitskontext innerhalb der Mobility-Security-Association auszuwählen. In einer Basis-Ausführungsform der Erfindung, werden nur der Default Mobile IP Authentifizierungsalgorithmus (MD5-verschlüsselt) und der Default-Modus („Präfix+Suffix") mit 128-Bit Shared Secrets unterstützt. Netzbenutzern wird es ermöglicht, mehrere Shared Secrets mit ihren Heimatnetzen zu definieren. Der Mechanismus zum Erzeugen von Sicherheitskontexten für Endbenutzer unter Zuteilung eines SPI an jeden Sicherheitskontext und zum Einstellen der Inhalte des Sicherheitskontexts (der ein Shared Secret enthält) und zum Verändern ihrer Inhalte werden untenstehend beschrieben. Während der Registrierung wird ein 128-Bit-Message-Digest im Präfix+Suffix-Modus unter Verwendung des MD5-Algorithmus durch das Endsystem berechnet. Das Shared Secret wird als das Präfix und das Suffix für die in der Registrierungsanfrage zu schützenden Daten verwendet. Der so berechnete Authentikator und der SPI und der Benutzername werden in der Registrierungsanfrage durch das Endsystem übertragen. Beim Empfang der Registrierungsanfrage des Endsystems, übermittelt der Fremd-Registrierungsserver die Anfrage gemeinsam mit dem Authentikator und dem SPI unverändert an den Heimat-Registrierungsserver. Beim Empfangen der Registrierungsanfrage direkt vom Endsystem oder indirekt über einen Fremd-Registrierungsserver, verwendet der Heimat-Registrierungsserver den SPI und den Benutzernamen, um den Sicherheitskontext auszuwählen. Der Heimatserver berechnet den Authentikator unter Verwendung des Shared Secrets neu. Wenn der Wert des berechneten Authentikators zum Wert des in der Anfrage durch das Endsystem gesendeten Authentikators passt, ist die Identität des Benutzers erfolgreich authentifiziert. Andernfalls gibt der Heimat-Registrierungsserver Naks (negative acknowledgements – negative Bestätigungen) für die durch das Endsystem gesendete Registrierungsanfrage aus.

[0147] Die Registrierungsantwort, die durch den Heimat-Registrierungsserver an das Endsystem gesendet wird, wird ebenfalls unter Verwendung des oben beschriebenen Algorithmus authentifiziert. Der SPI und der berechnete Authentikator-Wert werden in der Registrierungsantwortnachricht durch den Heimat-Server an das Endsystem übermittelt. Beim Empfang der Antwort, berechnet das Endsystem den Authentikator neu und, wenn der berechnete Wert nicht zum übermittelten Wert passt, wird es die Antwort zurückweisen und einen neuen Versuch starten.

[0148] Das Endsystem des Benutzers muss mit dem Shared Secret und den SPIs für alle Sicherheitskontexte, die der Benutzer mit seinem/seinen Registrierungsserver(n) teilt, konfiguriert werden. Diese Konfigurierungsinformationen sind vorzugsweise in einer Win **95** Registry für Windows **95** basierte Endsysteme gespei-

chert. Während der Registrierung, wird auf diese Informationen zugegriffen und sie werden für Authentifizierungszwecke verwendet.

[0149] Im Netz werden durch den Fremdagent FA Radius-Protokolle verwendet, um den Xtunnel zwischen dem drahtlosen Hub und der Heimat- und dienenden IWFs für das Endsystem zu konfigurieren. Beim Empfangen einer Registrierungsanfrage vom Endsystem erzeugt der FA ein Radius-Access-Request-Paket, speichert seine eigenen Attribute im Paket, kopiert die Registrierungsanfrageattribute des Endsystems unverändert in dieses Paket und sendet die kombinierte Anfrage an den Registrierungsserver in der MSC.

[0150] Die 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) ein Shared Secret für Authentifizierungszwecke teilen. Dieses Shared Secret wird ebenfalls verwendet, um private Informationen, die zwischen dem Radius-Client und dem Radius-Server kommuniziert werden, zu verschlüsseln. Das Shared Secret ist ein konfigurierbarer Parameter. Das Netz folgt den Empfehlungen im Radius-RFC und verwendet das Shared Secret und den MD5-Algorithmus für Authentifizierung und Verschlüsselung, wo Verschlüsselung erforderlich ist. Das Radius-Access-Request-Packet, das durch den FA gesendet wird, umfasst ein Radius-Benutzernamensattribut (das durch das Endsystem bereitgestellt wird) und ein Radius-Benutzerpasswortattribut. Der Wert des Benutzerpasswortattributs ist ebenfalls ein konfigurierbarer Wert und in der durch das Radius-Protokoll empfohlenen Art verschlüsselt. Andere netzspezifische Attribute, die aus der Perspektive der Radius-RFC-Standards keine Standard-Attribute sind, werden als lieferantenspezifische Radius-Attribute verschlüsselt und im Access-Request-Paket versendet.

[0151] Die nachfolgenden Attribute werden durch den FA an seinen Registrierungsserver im Radius-Access-Request-Paket gesendet.

1. Benutzernamensattribut. Dies ist der Benutzername des Endsystems, wie er durch das Endsystem in seiner Registrierungsanfrage geliefert wird.
2. Benutzerpasswortattribut. Dieses Benutzerpasswort wird durch die Basisstation/den drahtlosen Hub für den Benutzer geliefert. Es wird, wie im Radius-EFC beschrieben, unter Verwendung des Shared Secrets, das zwischen der Basisstation und seinem Registrierungsserver geteilt wird, verschlüsselt.
3. NAS-Port. Dies ist der Port auf der Basisstation.
4. NAS-IP-Adresse. Dies ist die IP-Adresse der Basisstation.
5. Dienst-Typ. Dies ist ein eingerahmter Dienst.
6. Eingerahmtes Protokoll. Dies ist ein PPP-Protokoll.
7. Xtunnel-Protokoll-Parameter. Diese Parameter werden durch die Basisstation gesendet, um die Parameter, die notwendig sind, um das Xtunnel-Protokoll für das Endsystem einzurichten, zu spezifizieren. Dies ist ein lieferantenspezifisches Attribut.
8. AP-IP-Adresse. Dies ist die IP-Adresse des AP durch den sich der Benutzer registriert. Dies ist ein lieferantenspezifisches Attribut.
9. AP-MAC-Adresse. Dies ist die MAC-Adresse des AP durch 10.
10. Registrierungsanfrage des Endsystems. Die Registrierungsanfrage vom Endsystem wird unverändert in dieses lieferantenspezifische Attribut kopiert.

[0152] Die nachfolgenden Attribute werden vom Registrierungsserver im Radius-Access-Response-Paket an den FA gesendet.

1. Dienst-Typ. Dies ist ein eingerahmter Dienst.
2. Eingerahmtes Protokoll. Dies ist ein PPP.
3. XTunnel-Protokoll-Parameter. Diese Parameter werden durch den Registrierungsserver gesendet, um die Parameter, die notwendig sind, um das Xtunnel-Protokoll für das Endsystem einzurichten, zu spezifizieren. Dies ist ein lieferantenspezifisches Attribut.
4. Registrierungsantwort des Heimat-Registrierungsservers. Dieses Attribut wird vom Heimat-Registrierungsserver an den FA gesendet. Der FA überträgt diese Attribute unverändert in einem Registrierungsantwortpaket an das Endsystem. Wenn im Pfad ein Fremd-Registrierungsserver ist, wird dieses Attribut durch ihn unverändert an den FA übertragen. Es wird als ein lieferantenspezifisches Attribut verschlüsselt.

[0153] Zum Bereitstellen von Dienst für die roamenden Endsysteme, werden das Fremdnetz und das Heimatnetz zu Accounting- und Abrechnungszwecken unter Verwendung des Radius-Protokolls für Authentifizierung und Konfigurierung füreinander authentifiziert. Diese Authentifizierung wird zum Zeitpunkt der Endsystemregistrierung ausgeführt. Wenn, wie vorhergehend beschrieben, der Registrierungsserver im Fremdnetz eine Registrierungsanfrage vom Endsystem empfängt (verkapselt als ein lieferantenspezifisches Attribut in einem Radius-Access-Paket durch den FA), verwendet es den Benutzernamen des Endsystems, um die Identität des

Heimat-Registrierungsservers des Endsystems durch Konsultieren seiner Heimat-Domänen-Directory HDD zu bestimmen. Die folgenden Informationen werden in der Heimat-Domänen-Directory HDD gespeichert und auf sie wird durch den Fremd-Registrierungsserver zugegriffen, um die Registrierungsanfrage des Endsystems weiterzuleiten.

1. IP-Adresse des Heimat-Registrierungsservers. Dies ist die IP-Adresse des Heimat-Registrierungsservers zum Weiterleiten der Registrierungsanfrage.
2. Maschinen-ID des Fremd-Registrierungsservers. Dies ist die Maschinen-ID des Fremd-Registrierungsservers im SMTP (Simplified Mail Transfer Protokoll) Format (z.B. Maschine@fqdn, wo Maschine der Name der Fremd-Registrierungsservermaschine und fqdn der vollständig qualifizierte Domänenname der Domäne des Fremdregistrierungsservers ist).
3. Tunneling-Protokollparameter. Dies sind Parameter für das Konfigurieren des Tunnels zwischen der dienenden IWF und der Heimat-IWF für das Endsystem. Diese enthalten das Tunneling-Protokoll, das zwischen ihnen und den Parametern für das Konfigurieren des Tunnels zu verwenden ist.
4. Shared Secret. Dies ist das Shared Secret, das für die Authentifizierung zwischen dem Fremd-Registrierungsserver und dem Heimat-Registrierungsserver zu verwenden ist. Dieses Secret wird für das Berechnen der Radius-Benutzerpasswortattribute im Radius-Paket, das vom Fremd-Registrierungsserver an den Heimat-Registrierungsserver gesendet wird, verwendet. Es wird zwischen den zwei Wireless Service Providern definiert.
5. Benutzer-Passwort. Dies ist das Benutzerpasswort, das für das roamende Endsystem zu verwenden ist. Dieses Benutzerpasswort wird zwischen den zwei Wireless Service Providern definiert. Dieses Passwort wird unter Verwendung des Shared Secrets, wie im Radius-RFC beschrieben, verschlüsselt.
6. Accounting-Parameter. Dies sind Parameter zum Konfigurieren des Accountings für das Endsystem, das sich registriert. Diese Parameter werden durch den Registrierungsserver an seine IWF zum Konfigurieren des Accountings für das Endsystem gesendet.

[0154] Unter Verwendung dieser Informationen, erzeugt der Fremd-Registrierungsserver ein Radius-Access-Request, fügt dem Radius-Access-Request seine eigenen Registrierungs- und Authentifizierungsinformationen hinzu, kopiert die Registrierungsinformationen, die durch das Endsystem gesendet werden, unverändert in das Radius-Access-Request und sendet die kombinierte Anfrage an den Heimat-Registrierungsserver.

[0155] Beim Empfangen des Radius-Access-Requests vom Fremd-Registrierungsserver (für ein roamendes Endsystem) oder direkt vom FA (für ein Endsystem in der Heimat), konsultiert der Heimat-Registrierungsserver seinen eigenen Directory-Server wegen der Shared Secrets, um die Identität des Endsystems und die Identität des Fremd-Registrierungsservers in einem Roaming-Szenario durch Neuberechnung der Authentikatoren zu überprüfen.

[0156] Nach dem erfolgreichen Verarbeiten der Anfrage erzeugt der Heimat-Registrierungsserver ein Radius-Access-Accept-Antwort-Paket und sendet es an den Fremd-Registrierungsserver, wenn das Endsystem roamt, oder direkt an den FA, von dem er die Radius-Access-Request empfangen hat. Die Antwort enthält das Registrierungsantwortattribut, das der FA an das Endsystem überträgt.

[0157] Wenn die Anfrage nicht erfolgreich verarbeitet werden kann, erzeugt der Heimat-Registrierungsserver ein Radius-Access-Reject-Antwortpaket und sendet es an den Fremd-Registrierungsserver, wenn das Endsystem roamt, oder direkt an den FA, von dem er die Radius-Access-Request empfangen hat. Die Antwort enthält die Registrierungsantwortattribute, die der FA an das Endsystem überträgt.

[0158] In einem Roaming-Szenario, wird die Antwort vom Heimat-Registrierungsserver durch den Fremd-Registrierungsserver empfangen. Sie wird durch den Fremd-Registrierungsserver unter Verwendung des Shared Secrets authentifiziert. Nach dem Authentifizieren verarbeitet der Fremd-Registrierungsserver die Antwort und erzeugt wiederum ein Radius-Antwortpaket (Accept oder Reject) zum Senden an den FA. Der Fremdregistrierungsserver kopiert das Registrierungsantwortattribut vom Radius-Antwortpaket vom Heimat-Registrierungsserver unverändert in sein Radius-Antwortpaket.

[0159] Wenn der FA das Radius-Access-Response- oder Radius-Access-Reject-Antwortpaket empfängt, erzeugt er ein Registrierungsantwortpaket unter Verwendung der Registrierungsantwortattribute von der Radius-Antwort und sendet die Antwort an das Endsystem und vervollständigt somit den Round Trip Registrierungsablauf.

[0160] Der Mobile IP Standard spezifiziert, dass Replay-Protection für Registrierungen unter Verwendung von

Zeitstempeln oder, wahlweise, Noncen ausgeführt werden. Da Replay-Protection unter Verwendung von Zeitstempeln indes entsprechend synchronisierte Systemuhren zwischen den entsprechenden Knoten erfordert, führt das vorliegende System Replay-Protestion während der Registrierung unter Verwendung von Noncen aus, obwohl die Replay-Protestion unter Verwendung von Zeitstempeln in den Mobile IP Standards obligatorisch ist und die Verwendung von Noncen wahlfrei ist. Replay-Protestion unter Verwendung von Zeitstempeln als eine alternative Ausführungsform ist indes möglich.

[0161] Die Art der Replay-Protestion, die zwischen Knoten verwendet wird, wird im Sicherheitskontext zusätzlich zum Authentifizierungskontext, Modus, Secret und Verschlüsselungstyp gespeichert.

[0162] Das Netz unterstützt die Verwendung von PPP PAP (Passwortauthentifizierung) und CHAP (Challenge Authenticated Password) zwischen dem Endsystem und seinem PPP-Server. Dies wird unabhängig von den vorhergehend beschriebenen Authentifizierungsmechanismen vorgenommen. Dies ermöglicht einem privaten Intranet oder einem ISP das unabhängige Überprüfen der Identität des Benutzers.

[0163] Authentifizierung für Accounting- und Directory-Dienste wird untenstehend in Bezug auf Accounting-Sicherheit beschrieben. Zugang zu Directory-Servern von Netzwerkausrüstung in der gleichen MSC muss nicht authentifiziert werden.

[0164] Das Netz unterstützt Verschlüsselung von Trägerdaten, die zwischen dem Endsystem und der Heimat-IWF gesendet werden. Die Endsysteme handeln das Anwenden oder Nichtanwenden von Verschlüsselung durch Auswählen des geeigneten Sicherheitskontexts aus. Beim Empfangen der Registrierungsanfrage, bewilligt der Heimat-Registrierungsserver die Anfrage des Endsystems nach Verschlüsselung basierend auf dem Sicherheitskontext. Zusätzlich zum Speichern von Authentifizierungsalgorithmus, Modus, Shared Secret und Art der Replay-Protection, wird der Sicherheitskontext ebenfalls verwendet, um die Art des zu verwendenden Verschlüsselungsalgorithmus zu spezifizieren. Wenn Verschlüsselung zwischen dem Endsystem und dem Heimatagent ausgehandelt wird, wird der gesamte PPP-Rahmen vor der Verkapselung in RLP so verschlüsselt.

[0165] Die IWF, der Accounting-Server und das Abrechnungssystem sind Teil der gleichen vertrauenswürdigen Domäne in der MSC. Diese Einheiten sind entweder auf dem gleichen LAN verbunden oder Teil eines vertrauenswürdigen Intranets, das sich im Besitz des Wireless Service Providers befindet und durch ihn betrieben wird. Der Transfer der Accounting-Statistiken zwischen der IWF und dem Accounting-Server und zwischen dem Accounting-Server und dem Abrechnungssystem des Kunden kann unter Verwendung von Internet-IP-Sicherheitsprotokollen wie IP-Sec verschlüsselt werden.

[0166] Das Netz macht es schwieriger, den Standort des Endsystems zu überwachen, da es erscheint, dass alle PPP-Rahmen, die sich zum und vom Endsystem bewegen, durch die Heimat-IWF gehen, unabhängig vom aktuellen Standort der Endsystemvorrichtung.

[0167] Accounting-Daten werden durch die dienende IWF und die Heimat-IWF im Netz gesammelt. Accounting-Daten, die durch die dienende IWF gesammelt werden, werden an einen Accounting-Server in der MSC der dienenden IWF gesendet. Die durch die Heimat-IWF gesammelten Accounting-Daten werden an einen Accounting-Server in der MSC der Heimat-IWF gesendet. Die Accounting-Daten, die durch die dienende IWF gesammelt werden, werden durch den Fremd-Wireless-Service-Provider für das Auditing und die Bereinigung von Rechnungen über Grenzen von Wireless Service Providern (zum Unterstützen von Roaming und Mobilität) hinweg verwendet. Die durch die Heimat-IWF gesammelten Accounting-Daten werden zur Abrechnung für die Endbenutzer und ebenfalls für die Bereinigung über Grenzen von Wireless Service Providern hinweg verwendet, um Roaming und Mobilität zu handhaben.

[0168] Da der gesamte Datenverkehr unabhängig vom Standort des Endsystems und dem Standort des Fremdagenten durch die Heimat-IWF fließt, hat die Heimat-IWF alle Informationen zum Erzeugen der Abrechnungen für die Kunden und ebenfalls Bereinigungsinformationen für die Verwendung auf Fremdnetzen.

[0169] Die dienende IWF und die Heimat-IWF verwenden vorzugsweise das Radius-Accounting-Protokoll zum Senden der Accounting-Einträge für registrierte Endsysteme. Das Radius-ACCOUnting-Protokoll ist wie im Entwurf des IETF RFC dokumentiert. Für die vorliegende Erfindung muss das Protokoll durch Hinzufügen von lieferantenspezifischen Attributen für das Netz und durch Hinzufügen von Check-Pointing zum Radius-Accounting-Protokoll ausgeweitet werden. Check-Pointing bezieht sich in diesem Kontext auf das periodische Aktualisieren von Accounting-Daten, um das Risiko des Verlustes von Accounting-Einträgen zu minimieren.

[0170] Das Radius-Accounting-Protokoll läuft über UDP/IP und verwendet Wiederholungsversuche basierend auf Bestätigung und Timeaouts. Der Radius-Accounting-Client (dienende IWFs oder Heimat-IWFs) senden UDP-Accounting-Anfragepakete zu ihren Accounting-Servern, die Bestätigungen zurück zu den Accounting-Clients senden.

[0171] Im Netz geben die Accounting-Clients (dienende IWF und Heimat-IWF) eine Accounting-Startangabe am Start der Benutzersession und eine Accounting-Stopangabe am Ende der Benutzersession aus. Mitten in der Session geben die Accounting-Clients Acccounting-Checkpoint-Angaben aus. Umgekehrt spezifiziert der Radius-Accounting-RFC keine Accounting-Checkpoint-Angabe. Die Software des vorliegenden Systems erzeugt ein lieferantenspezifisches Accounting-Attribut für diesen Zweck. Dieses Accounting-Attribut ist in allen Radius-Accounting-Request Paketen, die Acct-Status-Type of Start (Accounting-Startangaben) haben, enthalten. Der Wert dieses Attributs wird verwendet, um dem Accounting-Server zu übermitteln, ob ein Accounting-Eintrag ein Checkpointing-Eintrag ist oder nicht. Checkpointing-Accounting-Berichte haben ein Zeitattribut und enthalten Accounting-Daten, die seit dem Start der Session angesammelt wurden. Die Frequenz der Übertragung von Checkpoint-Paketen ist in der vorliegenden Erfindung konfigurierbar.

[0172] Die dienende IWF und die Heimat-IWF sind durch ihre entsprechenden Registrierungsserver zum Verbinden mit ihren Accounting-Servern während der Registrierungsphase konfiguriert. Die konfigurierbaren Accounting-Parameter enthalten die IP-Adresse und den UDP-Port des Accounting-Servers, die Frequenz des Checkpointings, die Sessions-/Mehrfach-Sessions-ID und das Shared Secret, das zwischen dem Accounting-Client und dem Accounting-Server zu verwenden ist.

[0173] Das Netz zeichnet die nachfolgenden Accounting-Attribute für jedes registrierte Endsystem auf. Diese Accounting-Attribute werden in Radius-Accounting-Paketen am Start der Session, am Ende der Session und mitten in der Session (Checkpoint) durch Accounting-Clients an ihre Accounting-Server berichtet.

1. Benutzername. Dies ist das vorhergehend erläuterte Radius-Benutzernamensattribut. Dieses Attribut wird verwendet, um den Benutzer zu identifizieren und ist in allen Accounting-Berichten vorhanden. Das Format ist „Benutzer@Domäne", wo Domäne der vollständig qualifizierte Domänenname der Heimat des Benutzers ist.
2. NAS-IP-Adresse. Diese ist wie das vorhergehend erläuterte Radius NAS-IP-Adressattribut. Dieses Attribut wird verwendet, um die IP-Adresse der Maschine, die die Heimat-IWF oder die dienende IWF ausführt, zu identifizieren.
3. Funkport. Dieses Attribut identifiziert den Funkport auf dem Zugangspunkt, der den Dienst für den Benutzer bereitstellt. Dieses Attribut wird wie ein lieferantenspezifisches Attribut verschlüsselt.
4. Zugangspunkt-IP-Adresse. Dieses Attribut identifiziert die IP-Adresse des Zugangspunkts, der Dienste für den Benutzer bereitstellt. Dieses Attribut ist als lieferantenspezifisches Attribut verschlüsselt.
5. Diensttyp. Dieser ist wie das vorhergehend beschriebene Radius-Diensttypattribut. Der Wert dieses Attributs ist eingerahmt.
6. Eingerahmtes Protokoll. Dies ist wie das vorhergehend beschriebene eingerahmte Radius-Protokollattribut. Der Wert dieses Attributs ist gesetzt, um PPP anzugeben.
7. Accounting-Statustyp. Dieser ist wie das vorhergehend beschriebene Radius Acct-Status-Type Attribut. Der Wert dieses Attributs kann Start sein, um den Start der Benutzersession beim Radius-Client zu markieren und Stop, um das Ende der Benutzersession beim Radius-Client zu markieren. Für Accounting-Clients wird das Acct-Status-Type/Start Attribut erzeugt, wenn sich das Endsystem registriert. Das Acct-Status-Type/Stop Attribut wird erzeugt, wenn sich das Endsystem aus irgendeinem Grund abmeldet. Für Checkpoints ist der Wert dieses Attributs ebenfalls Start und das Accounting Checkpoint Attribut ist ebenfalls vorhanden.
8. Accounting-Sessions-ID. Diese ist wie die vorhergehend beschriebene Radius Acct-Session-ID. In einem Roaming-Szenario wird diese Sessions-ID durch den Fremd-Registrierungsserver zugewiesen, wenn das Endsystem eine Registrierungsanfrage ausgibt. Sie wird durch den Fremd-Registrierungsserver während dem Registrierungsablauf an den Heimat-Registrierungsserver kommuniziert. Das Heimatnetz und das Fremdnetz kennen beide das Acct-Session-ID Attribut und sind imstande, dieses Attribut auszugeben, während sie Accounting-Einträge an ihre entsprechenden Accounting-Server senden. In einem „Endsystem-in-der-Heimat"-Szenario wird dieses Attribut durch den Heimat-Registrierungsserver erzeugt. Der Registrierungsserver kommuniziert den Wert dieses Attributs an die IWF, die sie in allen Accounting-Einträgen ausgibt.
9. Accounting-Multi-Session-ID. Diese ist wie die vorhergehend erläuterte Radius Acct-Multi-Session-ID. Diese ID wird durch den Heimat-Registrierungsserver zugewiesen, wenn eine Registrierungsanfrage direkt von einem FA oder über einen Fremd-Registrierungsserver für ein Endsystem empfangen wird. Sie wird durch den Heimat-Registrierungsserver in der Registrierungsantwortnachricht an den Fremd-Registrierungsserver kommuniziert. Der/die Registrierungsserver kommuniziert/kommunizieren den Wert dieses At-

tributs an die IWF(s), die es in alle Accounting-Einträge ausgibt/ausgeben.

[0174] Wenn True-Mobility zur Architektur hinzugefügt wird, wird die ID verwendet, um die Accounting-Einträge von unterschiedlichen IWFs für das gleiche Endsystem miteinander zu verknüpfen, wenn das Endsystem sich von einer IWF zur anderen bewegt. Für Handoffs über IWF-Grenzen hinweg, ist die Acct-Session-ID für Accounting-Einträge, die aus unterschiedlichen IWFs kommen, unterschiedlich. Das Acct-Multi-Session-ID Attribut ist indes das gleiche für Accounting-Einträge, die durch alle IWFs ausgegeben werden, die Dienste für den Benutzer bereitgestellt haben. Da die Sessions-ID und die Multi-Sessions-ID sowohl dem Fremdnetz als auch dem Heimatnetz bekannt sind, sind sie imstande, diese Attribute in Accounting-Berichten an ihre entsprechenden Accounting-Server auszugeben. Mit der Sessions-ID und der Multi-Sessions-ID sind Abrechnungssysteme imstande, Accounting-Einträge über IWF-Grenzen im gleichen Wireless Service Provider hinweg und sogar über die Grenzen von Wireless Service Providern hinweg zuzuordnen.

1. Accounting-Verzögerungszeit. Siehe Radius Acct-Verzögerungszeitattribut.
2. Accounting-Eingangsoktets. Siehe Radius Acct-Eingangsoktets. Dieses Attribut wird verwendet, um die Anzahl von Oktets, die durch das Endsystem gesendet werden (Eingang vom Endsystem in das Netz) aufzuzeichnen. Diese Zählung wird verwendet, um nur die PPP-Rahmen aufzuzeichnen. Der Verbindungs-Overhead oder irgendein durch das RLP bedingter Overhead, usw., wird nicht gezählt.
3. Accounting-Ausgangsoktets. Siehe Radius Acct-Ausgangsoktets. Dieses Attribut wird verwendet, um die Anzahl von Oktets, die an das Endsystem gesendet werden (Ausgang vom Netz in das Endsystem) aufzuzeichnen. Diese Zählung wird verwendet, um nur die PPP-Rahmen aufzuzeichnen. Der Verbindungs-Overhead oder irgendein durch das RLP bedingter Overhead, usw. wird nicht gezählt.
4. Accounting Authentic. Siehe Radius Acct-Authentic Attribut. Der Wert dieses Attributs ist lokal oder fern, in Abhängigkeit davon, ob die dienende IWF oder die Heimat-IWF den Accounting-Eintrag erzeugt.
5. Accounting-Sessionszeit. Siehe Radius Acct-Sessionszeit Attribut. Dieses Attribut zeigt die Dauer der Zeit an, während der der Benutzer Dienste erhalten hat. Wenn es durch die dienende IWF gesendet wird, zeichnet dieses Attribut die Dauer der Zeit auf, während der der Benutzer Dienste von dieser dienenden IWF erhalten hat. Wenn es von der Heimat-IWF gesendet wird, zeichnet dieses Attribut die Dauer der Zeit auf, während der der Benutzer Dienste von der Heimat-IWF erhalten hat.
6. Accounting-Eingangspakete. Siehe Radius Acct-Eingangspakete Attribut. Dieses Attribut zeigt die Anzahl der Pakete an, die vom Endsystem empfangen wurden. Für eine dienende IWF zeichnet dieses Attribut die Anzahl der PPP-Rahmen auf, die von einem Endsystem in die dienende IWF eingehen. Für eine Heimat-IWF zeichnet dieses Attribut die Anzahl von PPP-Rahmen auf, die von einem Endsystem in die Heimat-IWF eingehen.
7. Accounting-Ausgangspakete. Siehe Radius Acct-Ausgangspaket Attribut. Dieses Attribut zeigt die Anzahl der Pakete an, die an das Endsystem gesendet wurden. Für eine dienende IWF zeichnet dieses Attribut die Anzahl der PPP-Rahmen auf, die durch die dienende IWF an das Endsystem ausgehen. Für eine Heimat-IWF zeichnet dieses Attribut die Anzahl der PPP-Rahmen auf, die von der Heimat-IWF an das Endsystem gesendet wurden.
8. Accounting-Beendigungsgrund. Siehe Radius Acct-Beendigungsgrund Attribut. Dieses Attribut zeigt den Grund für die Beendigung einer Benutzersession an. Zusätzlich ist ebenfalls ein spezifischer Grundcode vorhanden, um zusätzliche Details bereitzustellen. Dieses Attribut ist nur in Accounting-Berichten am Ende der Session vorhanden.
9. Netz-Accounting-Beendigungsgrund. Dieses Attribut zeigt einen detaillierten Grund für die Beendigung einer Session an. Dieses spezifische Attribut ist als ein lieferantenspezifisches Attribut verschlüsselt und wird nur in einem Radius-Accounting-Attribut am Ende der Session berichtet. Das Standard-Radius-Attribut Acct-Beendigungsgrund ist ebenfalls vorhanden. Dieses Attribut stellt spezifische Grundcodes bereit, die nicht durch das Acct-Beendigungsgrund-Attribut abgedeckt werden.
10. Netz-Air-Link-Zugangsprotokoll. Dieses Attribut zeigt das Air-Link-Zugangsprotokoll, das durch das Endsystem verwendet wird, an. Dieses Attribut wird als ein lieferantenspezifisches Attribut verschlüsselt.
11. Netz-Backhaul-Zugangsprotokoll. Dieses Attribut zeigt das Backhaul-Zugangsprotokoll an, das durch den Zugangspunkt verwendet wird, um Daten zum und vom Endsystem zu befördern. Dieses Attribut ist als ein lieferantenspezifisches Attribut verschlüsselt.
12. Netzagent-Maschinenname. Dieses Attribut ist der vollständig qualifizierte Domänenname der Maschine, die die Heimat-IWF oder die dienende IWF ausführt. Dieses spezifische Attribut ist in einem lieferantenspezifischen Format verschlüsselt.
13. Netz-Accounting-Checkpoint. Da das Radius-Accounting-RFC kein Checkpoint-Paket definiert, verwendet die vorliegende Netzausführungsform ein Radius-Accounting-Startpaket mit diesem Attribut, um einen Checkpoint zu markieren. Das Fehlen eines Checkpoint-Attributs bedeutet ein herkömmliches Accounting-Startpaket. Das Vorhandensein dieses Attributs in einem Accounting-Startpaket bedeutet ein Accounting-Checkpoint-Paket. Accounting-Stoppakete haben dieses Attribut nicht.

[0175] In der bevorzugten Ausführungsform muss jedes Accounting-Paket und die entsprechende Antwort unter Verwendung von MD5 und einem Shared Secret authentifiziert werden. Die IWFs sind mit einem Shared Secret konfiguriert, das von ihnen während der Kommunikation mit ihrem Radius-Accounting-Server zur Authentifizierung verwendet wird. Die Shared Secrets, die durch die IWFs zum Kommunizieren mit den Accounting-Servern verwendet werden, sind in der in der MSC angeordneten Heimat-/Fremd-Domänen-Directory gespeichert. Die Shared Secrets für Accounting-Sicherheit werden durch ihre Registrierungsserver während des Registrierungsablaufs des Endsystems an die IWFs kommuniziert.

[0176] Die Accounting-Server-Software wird in einem Computer ausgeführt, der in der MSC angeordnet ist. Die Rolle des Accounting-Servers im System ist das Sammeln von Roh-Accounting-Daten von den Netzelementen (in den Heimat- und Fremd-IWFs), das Verarbeiten der Daten und deren Speicherung für den Transfer zum Abrechnungssystem des Wireless Service Providers. Der Accounting-Server enthält kein Verrechnungssystem. Stattdessen enthält er Unterstützung für einen automatischen oder manuellen Accounting-Datentransfermechanismus. Durch die Verwendung des automatischen Accounting-Datentransfermechanismus übermittelt der Accounting-Server Accounting-Einträge im AMA-Abrechnungsformat über einen TCP/IP-Transport an das Abrechnungssystem des Kunden. Zu diesem Zweck definiert das System AMA-Abrechnungseintragsformate für Paketdaten. Durch die Verwendung des manuellen Transfermechanismus, sind Kunden imstande, ein Band zum Übertragen von Accounting-Einträgen an ihr Abrechnungssystem zu bilden. Um das Band für ihre Spezifizierungen aufzubauen, werden den Kunden Informationen zum Zugreifen auf Accounting-Einträge bereitgestellt, derart, dass sie sie verarbeiten können, bevor sie auf Band geschrieben werden.

[0177] In Fig. 22 werden die Roh-Accountingdaten, die durch den Accounting-Server von der Heimat- oder der dienenden IWF empfangen werden, durch den Accounting-Server verarbeitet und gespeichert. Die Verarbeitung, die durch den Accounting-Server erfolgt, enthält Filtern, Komprimieren und Zuordnen der Roh-Accounting-Daten, die von der IWF empfangen wurden. Ein Datei-Server mit hoher Verfügbarkeit, der duale Aktiv-/Standby-Prozessoren und im laufenden Betrieb austauschbare RAID-Laufwerke verwendet, wird für das Puffern der Accounting-Daten verwendet, während sie den Accounting-Server durchlaufen.

[0178] Der Accounting-Server verzögert die Verarbeitung der Roh-Accounting-Daten, bis ein Endsystem die Session beendet hat. Wenn ein Endsystem seine Session beendet, verarbeitet der Accounting-Server die Roh-Accounting-Daten, die er für die Session gesammelt hat und Speichert einen Accounting-Zusammenfassungseintrag in einer SQL-Datenbank. Der Accounting-Zusammenfassungseintrag, der in der SQL-Datenbank gespeichert ist, zeigt auf eine ASN.1 verschlüsselte Datei. Diese Datei enthält detaillierte Accounting-Informationen über die Session des Endsystems. Die im Accounting-Server gespeicherten Daten werden dann durch den Abrechnungsdaten-Übertragungsagent an das Abrechnungssystem des Kunden übertragen. Alternativ kann der Wireless Service Provider die Accounting-Daten von der SQL-Datenbank und/oder der ASN.1 verschlüsselten Datei über ein Band an das Abrechnungssystem übertragen. Das Datenbankschema und das Format der ASN.1 verschlüsselten Datei sind dokumentiert und werden den Kunden zu diesem Zweck bereitgestellt. Wenn das Volumen der verarbeiteten Accounting-Daten, die im Accounting-System gespeichert sind, eine Hochwassermarke überschreitet, erzeugt der Accounting-Server einen NMS-Alarm. Dieser Alarm wird gelöscht, wenn das im Accounting-Server gespeicherte Datenvolumen unter die Hochwassermarke sinkt. Die hohen und niedrigen Wassermarken zum Erzeugen und Löschen des Alarms sind konfigurierbar. Der Accounting-Server erzeugt ebenfalls einen NMS-Alarm, wenn das Alter der gespeicherten Accounting-Daten eine konfigurierbare Schwelle übersteigt. Umgekehrt wird der Alarm gelöscht, wenn das Alter der Accounting-Daten unter die Schwelle sinkt.

[0179] Die Abonnenten-Directory wird verwendet, um Informationen über die Abonnenten zu speichern und ist im Heimat-Netz angeordnet. Der Heimat-Registrierungsserver konsultiert diese Directory während der Registrierungsphase zum Authentifizieren und Registrieren eines Endsystems. Für jeden Abonnenten speichert die Abonnenten-Directory die folgenden Informationen.

1. Benutzername. Dieses Feld im Abonnenteneintrag ist im SMTP-Format (z.B. Benutzer@fqdn), wo das Benutzer-Unterfeld den Benutzer/die Benutzerin in seiner oder ihrer drahtlosen Heimat-Domäne identifiziert und das fqdn-Unterfeld die drahtlose Heimat-Domäne des Abonnenten identifiziert. Dieses Feld wird durch das Endsystem in seiner Registrierungsanfrage während der Registrierungsphase gesendet. Dieses Feld wird dem Abonnenten durch den Wireless Service Provider zum Zeitpunkt des Abonnierens des Netzdienstes zugewiesen. Dieses Feld unterscheidet sich vom Benutzernamensfeld, das im PPP verwendet wird.
2. Mobility-Security-Association. Dieses Feld im Abonnenteneintrag enthält die Mobility-Security-Association zwischen dem Abonnenten/der Abonnentin und seinem/ihrem Heimatnetz. Wie vorhergehend beschrieben besteht eine Mobility-Security-Association zwischen jedem Abonnenten und seinem Heimat-Registrierungsserver. Die Mobility-Security-Association definiert eine Sammlung von Sicherheitskontexten. Jeder Si-

cherheitskontext definiert einen Authentifizierungsalgorithmus, einen Authentifizierungsmodus, ein Shared Secret, einen Replay-Protection-Typ und den Verschlüsselungstyp (einschließlich ohne Verschlüsselung), die zwischen dem Endsystem und seinem Heimatserver zu verwenden sind. Während der Registrierung, ruft der Heimat-Registrierungsserver Informationen über den Sicherheitskontext des Abonnenten unter Verwendung des durch das Endsystem in seiner Registrierungsanfrage gelieferten Benutzernamens und Security Parameter Index (SPI) von der Abonnenten-Directory ab. Die Informationen im Sicherheitskontext werden verwendet, um Authentifizierung, Verschlüsselung und Replay-Protection während der Session geltend zu machen. Die Mobility-Security-Association wird durch den Wireless Service Provider zum Zeitpunkt der Abonnierung erzeugt. Es liegt am Wireless Service Provider, es dem Abonnenten zu erlauben, diese Association entweder durch Aufrufen eines Kundendienstvertreters oder dadurch, dass den Abonnenten das Zugreifen auf eine sichere Website ermöglicht wird, zu ändern. Die Website-Software exportiert Web-Seiten, die der Wireless Service Provider von einem sicheren Webserver aus zugänglich machen kann. Auf diese Weise sind die Abonnenten imstande, die Inhalte der Mobility-Security-Association zusätzlich zu anderen Abonnenteninformationen, die der Service Provider zugänglich machen möchte, anzuzeigen oder zu ändern.

3. Modem-MAC-Adresse. Dieses Feld enthält die MAC-Adresse des Modems, das sich im Besitz des Abonnenten befindet. Zusätzlich zum Shared Secret, wird dieses Feld während der Registrierung verwendet, um den Benutzer zu authentifizieren. Es ist möglich, die MAC-Adressen basierte Authentifizierung für einzelne Benutzer abzuschalten. Die MAC-Adresse wird während der Registrierung an den Heimat-Registrierungsserver kommuniziert.

4. MAC-Adressen-Authentifizierung freigeben. Dieses Feld wird verwendet, um die MAC-Adresse basierend darauf, ob die MAC-Adressen basisierte Authentifizierung freigegeben oder gesperrt ist, verwendet. Wenn sie freigegeben ist, prüft der Heimat-Registrierungsserver die MAC-Adresse des registrierenden Endsystems gegen dieses Feld, um die Identität des Endsystems zu bestätigen. Wenn es gesperrt ist, wird keine Prüfung vorgenommen.

5. Flag Roaming freigegeben. Wenn dieses Feld auf freigegeben gesetzt wird, wird es dem Endsystem erlaubt, auf Fremd-Netze zu roamen. Wenn dieses Feld gesperrt ist, wird es dem Endsystem nicht erlaubt, auf fremde Netze zu roamen.

6. Roaming-Domänenliste. Dieses Feld hat nur Bedeutung, wenn der Flag Roaming freigegeben auf freigegeben gesetzt ist. Dieses Feld enthält eine Liste von Fremd-Dömänen, auf die das System roamen darf. Wenn die Inhalte dieser Liste Null sind und der Flag Roaming freigegeben auf freigegeben gesetzt ist, wird es dem Endsystem erlaubt, frei zu roamen.

7. Flag Dienst freigeben/sperren. Dieses Feld kann durch den Systemadministrator auf gesperrt gesetzt werden, um den Dienst für einen Abonnenten zu sperren. Wenn dieses Feld gesperrt ist, wird es dem Abonnenten erlaubt, sich für diesen Dienst zu registrieren. Wenn der Abonnent registriert ist und der Wert dieses Felds auf gesperrt gesetzt wird, wird die Verbindung des Endsystems sofort durch das Netz getrennt.

8. Internet Service Provider Association. Dieses Feld enthält Informationen über den Internet Service Provider des Abonnenten. Diese Informationen werden durch die IWF während der PPP-Registrierungsphase verwendet, um die Authentifizierung mit dem Internet Service Provider für das Endsystem auszuführen und ebenfalls, um einen L2TP-Tunnel zwischen der IWF und dem PPP-Server des Internet Service Providers zu erzeugen. Dieses Feld enthält die Identität des ISP des Abonnenten. Die IWF verwendet diese Informationen, um auf die ISP-Directory zuzugreifen, um das Authentifizieren und das Einrichten des L2TP-Tunnels für das Endsystem.

9. Name & Adressinformationen des Abonnenten. Dieses Feld enthält den Namen, die Adresse, Telefonnummer, Faxnummer, E-Mail-Adresse usw. des Abonnenten.

[0180] Die Heimat-Domänen-Directory (HDD) wird durch den Registrierungsserver verwendet, um Parameter über das Endsystem abzurufen, um die Registrierung für das Endsystem zu vervollständigen. Durch die Verwendung dieser Informationen bestimmt der Registrierungsserver, ob das Endsystem sich in der Heimat registriert oder ob das Endsystem ein roamendes End-System ist. Im ersten Fall nimmt der Registrierungsserver die Rolle des Heimat-Registrierungsservers an und fährt mit der Registrierung des Endsystems fort. Im letzteren Fall, nimmt der Registrierungsserver die Rolle des Fremd-Registrierungsservers an und leitet die Anfrage an den tatsächlichen Heimat-Registrierungsserver, dessen Identität er von dieser Directory erhält, weiter, indem er als ein Radius-Proxy agiert. Für das roamende Endsystem enthalten die Parameter, die in der HDD gespeichert sind, die IP-Adresse des Heimat-Registrierungsservers, das Heimat-Fremd-Shared-Secret, die dienende IWF-Tunnelkonfiguration der Heimat, usw. Die HDD ist in der MSC angeordnet.

[0181] Die folgenden Informationen sind in der HDD gespeichert.

1. Name der Heimat-Domäne. Dieses Feld wird als der Schlüssel für die Suche der HDD für einen Eintrag, der zum vollständig qualifizierten Domänennamen passt, der durch das Endsystem in seiner Registrie-

rungsanfrage bereitgestellt wird, verwendet.
2. Proxy-Registrierungsanfrage. Dieses Feld wird durch den Registrierungsserver verwendet, um zu bestimmen, on er als ein Fremd-Registrierungsserver agieren soll und das Proxy der Registrierungsanfrage des Endsystems an den tatsächlichen Heimat-Registrierungsserver vornehmen soll.
3. DNS-Name des Heimat-Registrierungsservers. Wenn der Proxy-Registrierungsanfrage-Flag TRUE ist, wird dieses Feld verwendet, um auf den DNS-Namen des tatsächlichen Heimat-Registrierungsservers zuzugreifen. Andernfalls wird dieses Feld ignoriert. Der DNS-Name wird durch den Fremd-Registrierungsserver in eine IP-Adresse übersetzt. Der Fremd-Registrierungsserver verwendet die IP-Adresse, um die Registrierungsanfrage des Endsystems zu übertragen.
4. Fremd-Domänenname. Wenn der Proxy-Registrierungsanfrage-Flag TRUE ist, wird dieses Feld verwendet, um den Fremd-Domänennamen des Heimat-Registrierungsservers des Endsystems zu identifizieren. Andernfalls wird dieses Feld ignoriert. Der Fremd-Registrierungsserver verwendet diese Informationen, um die Fremdserver-Maschinen-ID im SMTP-Format zu erzeugen, zum Beispiel Maschine@fqdn. Diese Maschinen-ID wird im Radius Access-Request durch den Fremd-Registrierungsserver an den Heimat-Registrierungsserver gesendet.
5. Shared Secret. Wenn der Proxy-Registrierungsanfrage-Flag TRUE ist, wird das Shared Secret zwischen den Fremd- und Heimat-Registrierungsservern verwendet, um ihre Identität miteinander zu authentifizieren. Andernfalls wird dieses Feld ignoriert.
6. Tunneling-Protokoll-Parameter. Dieses Feld wird verwendet, um Parameter zum Konfigurieren von Tunneln zum Bereitstellen von Diensten für das Endsystem zu speichern. Für ein Endsystem in der Heimat, enthält es Informationen über Tunnelparameter zwischen der Basisstation und der Heimat-IWF und von der Heimat-IWF zum PPP-Server. Für ein roamendes Endsystem enthält es Tunnelparameter von der Basisstation zur dienenden IWF und von der dienenden IWF zur Heimat-IWF. Als Minimum enthält dieses Feld für jeden Tunnel den Typ des zu verwendenden Tunneling-Protokolls und Tunneling-Protokoll spezifische Parameter. Zum Beispiel kann dieses Feld den Identifikator für das Tunneling-Protokoll L2TP und zusätzliche Parameter, die zum Konfigurieren des L2TP-Tunnels zwischen der IWF und ihrem Peer, erforderlich sind, enthalten.
7. Accounting Server Association. Dieses Feld wird verwendet, um Informationen zu speichern, die durch die IWF benötigt werden, um Accounting-Daten für das Endsystem zu erzeugen. Es enthält den Namen des Accounting-Protokolls (z.B. RADIUS), den DNS-Namen des Accounting-Servers und zusätzliche Accounting-Protokoll spezifische Parameter, wie die UDP-Portnummer, das Shared Secret, das die IWF im Radius Accounting-Protokoll verwenden muss, die Frequenz des Checkpointings, die Ausgangszahl für das Erzeugen der Sessions-/Multi-Sessions-ID, usw. Der DNS-Name des Accounting-Servers wird in die IP-Adresse des Accounting-Servers, die an die IWF gesendet wird, übersetzt.

[0182] Für Wireless Service Provider, die Roaming-Vereinbarungen miteinander haben, wird die HDD zur Authentifizierung verwendet, und, um den Registrierungsprozess zu vervollständigen. Wenn ein Endsystem von seinem Heimatnetz zu einem Fremdnetz roamt, konsultiert der Fremd-Registrierungsserver in diesem Netz die HDD in seiner MSC, um Informationen über die Heimatregistrierung des besuchenden Endsystems zu erhalten und, um das Heimatnetz zu authentifizieren, bevor es Dienste für das besuchende Endsystem bereitstellt.

[0183] Die Software für das Heimat-Domänen-Directory-Management stellt vorzugsweise eine auf einer grafischen Benutzerschnittstelle (GUI) basierende HDD-Management-Schnittstelle für Systemadministratoren bereit. Durch die Verwendung dieser GUI sind die Systemadministratoren imstande, Einträge in der HDD anzuzeigen und zu aktualisieren. Diese GUI ist nicht zur Verwendung durch Fremd-Wireless-Service-Provider zum Ausführen von Fern-Aktualisierungen basierend auf Roaming-Vereinbarungen bestimmt. Sie ist lediglich für die Verwendung durch vertrauenswürdiges Personal des Heimat-Wireless-Service-Providers, das hinter Firewalls arbeitet, bestimmt.

[0184] Die Fremd-Domänen-Directory (FDD) stellt Funktionen bereit, die das Gegenteil der Heimat-Domain-Directory sind. Die FDD wird durch den Heimat-Registrierungsserver verwendet, um Parameter über den Fremd-Registrierungsserver und das Fremdnetz abzurufen, um das Fremdnetz zu authentifizieren und einen Tunnel zwischen einer dienenden IWF und einer Heimat-IWF zu erzeugen. Diese Parameter umfassen das Heimat-Fremd-Shared-Secret, die der Heimat-IWF dienende IWF-Tunnelkonfiguration, usw. Die FDD ist vorzugsweise in der MSC des Heimat-Registrierungsservers angeordnet. Die FDD wird durch die Heimat-Registrierungsserver zum Registrieren von roamenden Endsystemen verwendet.

[0185] Die folgenden Informationen werden in der FDD gespeichert.
1. Fremd-Domänenname. Dieses Feld wird als der Schlüssel zum Suchen der FDD für einen Eingang, der zum vollständig qualifizierten Domänennamen des Fremdregistrierungsservers passt, der die Registrie-

rungsanfrage überträgt, verwendet.

2. Shared Secret. Dies ist das Shared Secret, das zwischen den Fremd- und Heimat-Registrierungsservern verwendet wird, um gegenseitig ihre Identität miteinander zu authentifizieren.

3. Heimat-IWF dienende IWF Tunneling-Protokoll-Parameter. Dieses Feld wird verwendet, um Parameter zum Konfigurieren des Tunnels zwischen der Heimat-IWF und der dienenden IWF zu speichern. Als Minimum, enthält dieses Feld den Typ des zu verwendenden Tunneling-Protokolls und Tunneling-Protokoll spezifische Parameter. Zum Beispiel kann dieses Feld den Identifikator für das Tunneling-Protokoll L2TP und zusätzliche Parameter, die erforderlich sind, um den L2TP-Tunnel zwischen der dienenden IWF und der Heimat-IWF zu konfigurieren, enthalten.

4. Accounting Server Association. Dieses Feld wird verwendet, um Informationen, die durch die Heimat-IWF benötigt werden, um Accounting-Daten für das Endsystem zu erzeugen, zu speichern. Es enthält den Namen des Accounting-Protokolls (z.B. RADIUS), den DNS-Namen des Accounting-Servers und zusätzliche Parameter, die spezifisch für das Accounting-Protokoll sind, wie die UDP-Portnummer, das Shared Secret, dass die IWF im Radius-Accounting-Protokoll verwenden muss, die Frequenz von Checkpointings, die Ausgangszahl zum Erzeugen der Session-/Multi-Session-ID usw. Der DNS-Name des Accounting-Servers wird in die IP-Adresse des Accounting-Servers übersetzt, die an den Fremdagent gesendet wird.

[0186] Für Wireless Service Provider, die Roaming-Vereinbarungen miteinander haben, wird die FDD verwendet, um die Authentifizierung vorzunehmen und das Registrierungsverfahren zu vollenden. Wenn ein Endsystem von seinem Heimatnetz zu einem Fremdnetz roamt, konsultiert der Registrierungsserver im Heimatnetz die FDD in seiner MSC, um Informationen zu erhalten und das Fremdnetz, das Dienste für das Endsystem bereitstellt, zu authentifizieren.

[0187] Die Fremd-Domänen-Directory-Managementsoftware stellt eine auf einer grafischen Benutzerschnittstelle (GUI) basierende FDD-Managementschnittstelle für Systemadministratoren bereit. Durch die Verwendung dieser GUI, sind Systemadministratoren imstande, Einträge in der FDD anzuzeigen und zu aktualisieren. Diese GUI ist nicht für die Verwendung durch Fremd-Wireless-Service-Provider für Fern-Aktualisierungen basierend auf Roaming-Vereinbarungen bestimmt. Sie ist nur für die Verwendung durch vertrauenswürdiges Personal des Heimat-Wireless-Service-Providers, das hinter Firewalls arbeitet, bestimmt.

[0188] Die Internet-Service-Provider-Directory (ISPD) wird durch die Heimat-IWF verwendet, um die Konnektivität mit ISPs, die Servicevereinbarungen mit dem Wireless Service Provider haben, zu verwalten, derart, dass Abonnenten unter Verwendung des Netzes auf ihre ISPs zugreifen können. Für jeden Abonnenten hat die Abonnenten-Directory einen Eintrag für den ISP des Abonnenten. Dieses Feld zeigt auf einen Eintrag in der ISPD. Die Heimat-IWF verwendet diese Informationen, um die Verbindung mit dem ISP für den Abonnenten einzurichten.

[0189] Die Netzarchitektur unterstützt Roaming. Damit das Roaming zwischen Wireless Service Providern funktioniert, muss die Architektur das Einrichten von Roaming-Vereinbarungen zwischen Wireless Service Providern unterstützen. Dies setzt zwei Dinge voraus: (1) Aktualisieren der Systemdirectories über Wireless Service Provider und (2) Bereinigung von Rechnungen zwischen Service Providern.

[0190] Um den Abonnenten den Zugang zu Internet Service Providern zu ermöglichen, unterstützt die Architektur Roaming-Vereinbarungen mit Internet Service Providern. Dies setzt voraus, dass die Architektur imstande sein muss, Daten an und von PPP-Servern von ISPs zu senden und zu empfangen (d.h. Industriestandard-Protokolle wie PPP, L2TP und Radius unterstützen). Es setzt ebenfalls voraus, dass die Architektur Directory-Aktualisierungen für ISP-Zugang und Bereinigung von Rechnungen mit ISPs verarbeitet.

[0191] Wenn Roaming-Vereinbarungen zwischen zwei Wireless Service Providern eingerichtet werden, müssen beide Provider ihre Heimat- und Fremd-Domänen-Directories aktualisieren, um Authentifizierungs- und Registrierungsfunktionen für Endsysteme, die ihre Netze vom anderen Netz aus besuchen, zu unterstützen. Als Minimumm unterstützt die Architektur der vorliegenden Ausführungsform manuelle Directory-Aktualisierungen. Wenn eine Roaming-Vereinbarung zwischen zwei Wireless Service Providern eingerichtet wird, tauschen die beiden Parteien der Vereinbarung Informationen zum Bevölkern ihrer Heimat- und Fremd-Domänen-Directories aus. Die eigentliche Aktualisierung der Directories wird manuell durch das Personal der entsprechenden Service Provider vorgenommen. Wenn später die Informationen in den Heimat- und Fremd-Dömänen-Directories aktualisiert werden müssen, tauschen die beiden Parteien der Vereinbarung die aktualisierten Informationen aus und wenden dann ihre Aktualisierungen manuell auf die Directories an.

[0192] In einer alternativen Ausführungsform gliedert die Directory-Management-Software Entwicklungsstandards in die IETF ein, um Roaming zwischen Internet Service Providern zu ermöglichen und es den ISPs zu ermöglichen, Roaming-Verhältnisse automatisch zu verwalten und zu entdecken. Hierdurch ist manuelles Directory-Management nicht länger notwendig. Das Netzsystem propagiert Roaming-Verhältnisse automatisch und entdeckt sie, um besuchende Endsysteme zu authentifizieren und zu registrieren.

[0193] Als Minimum verarbeitet die Netzarchitektur einfach die Accounting-Daten und speichert sie und macht die Daten für das Abrechnungssystem des Wireless Service Providers verfügbar. Es liegt am Abrechnungssystem, die Bereinigung von Rechnungen für Roaming zu verwalten.

[0194] In einer alternativen Ausführungsform, werden Entwicklungsstandards in der IETF zur Handhabung der Verteilung von Accounting-Einträgen zwischen Internet Service Providern in die Netzarchitektur eingegliedert, um es den ISPs zu ermöglichen, Abrechnungsbereinigung für roamende Endsysteme vorzunehmen.

[0195] Die Systemsoftware unterstützt den Zugang zu ISPs und privaten Intranets durch Unterstützen des L2TP zwischen der Heimat-IWF und den ISPs oder dem PPP-Server des Intranets. Die Directory des Internet Service Providers enthält Informationen, die für die IWF nützlich für das Erzeugen dieser Tunnel sind. Wenn Zugangsvereinbarungen zwischen dem Wireless Service Provider und Internet Service Providern eingeführt werden, wird diese Directory manuell durch das Personal des Wireless Service Providers aktualisiert. Automatische Aktualisierungen und das Entdecken von Zugangsverhältnissen zwischen dem Wireless Service Provider und Internet Service Providern werden gegenwärtig ins Auge gefasst und in dem Maße ausgeführt, in dem sich die Internet-Standards entwickeln. Beim Zugang zu einem Internet Service Provider, enthält der Abonnent zwei Rechnungen – eine vom Wireless Service Provider für die Verwendung des drahtlosen Netzes und die zweite vom Internet Service Provider. Obwohl gemeinsames Abrechnen, das beide Gebührentypen kombiniert, nicht durch die Software der Minimum-Ausführungsform gehandhabt wird, wird ins Auge gefasst, das die Software sich die Internet-Standards für Abrechnungsbereinigung in dem Maße zunutze macht, in dem sich diese entwickeln, derart, dass Abonnenten eine gemeinsame Rechnung erhalten können, die auf Roaming-Vereinbarungen zwischen dem ISP und den Wireless Service Providern basieren.

[0196] Das System enthält ein Elementmanagementsystem für das Management der Netzelemente. Vom Elementmanager aus, führen Systemadministratoren die Konfigurations-, Leistungs- und Fehler/Alarmmanagementfunktionen aus. Die Elementmanagementapplikationen werden zuoberst auf einem Webbrowser ausgeführt. Durch die Verwendung eines Webbrowsers verwalten Systemadministratoren das Netz, von überall dort, wo sie TCP/IP-Zugang haben. Der Elementmanager führt zudem eine Agentenrolle für einen Manager einer höheren Ebene aus. In dieser Rolle exportiert er ein SNMP MIB für Alarm- und Fehlerüberwachung.

[0197] Ein SNMP-Manager einer höheren Ebene wird über SNMP-Traps von Alarmbedingungen benachrichtigt. Der SNMP-Manager einer höheren Ebene fragt die MIB des Elementmanagers periodisch nach der Gesundheit und dem Status des Netzes ab. Systemmanagementpersonal beim Manager der höheren Ebene ist imstande, eine Icondarstellung des Netzes und seines gegenwärtigen Alarmzustands anzuzeigen. Durch Hinweisen und Klicken auf das Netzelement-Icon, führt das Systemmanagementpersonal Elementmanagementanwendungen unter Verwendung eines Webbrowsers aus und führt detailliertere Managementfunktionen aus.

[0198] Innerhalb des Netzes wird die Verwaltung der physischen und logischen Netzelemente unter Verwendung einer Kombination des SNMP-Protokolls und von internen Managementapplikations-Programmierschnittstellen ausgeführt. Die Applikationen im Elementmanager verwenden SNMP oder andere Management-APIs zum Ausführen von Netzmanagementfunktionen.

[0199] Die Architektur des Elementmanagementsystems enthält zwei getrennte Sätze von funktionellen Elementen. Der erste Satz von funktionellen Elementen, der den Konfigurationsdatenserver, den Leistungsdatenmonitor und den Gesundheits-/Statusmonitor und die Netzelementwiederherstellungssoftware enthält, wird auf einem HA-Server, der mit RAID-Laufwerken ausgestattet ist, ausgeführt. Der zweite Satz von funktionellen Elementen, der die Managementapplikationen enthält, wird auf einem dedizierten nicht HA-Managementsystem ausgeführt. Sogar wenn das Elementmanagersystem nicht mehr betriebsbereit ist, behalten die Netzelemente die Fähigkeit, ausgeführt zu werden und Alarme zu berichten und sogar die Fähigkeit, von Fehlerzuständen wiederhergestellt zu werden. Da alle Managementapplikationen im nicht HA-Elementmanager ausgeführt werden, sind, wenn der Elementmanager abstürzt, Wiederherstellungstätigkeiten, die menschliche Eingriffe erfordern, indes nicht möglich, bis der Elementmanager betriebsbereit wird.

[0200] Die drahtlosen Hubs (WHs) in den Basisstationen sind typischerweise das Eigentum eines Wireless

Service Providers (WSP) und sie sind entweder über Punkt-zu-Punkt-Verbindungen, Intranets oder das Internet mit dem Registrierungsserver (RS) des WSP verbunden. Der Registrierungsserver des WSP ist typischerweise ein Softwaremodul, das auf einem Prozessor ausgeführt wird, um bestimmte Registrierungsfunktionen auszuführen. Interworking-Funktions-Einheiten (IWF-Einheiten) sind typischerweise Softwaremodule, die auf einem Prozessor ausgeführt werden, um bestimmte Schnittstellenfunktionen durchzuführen. IWF-Einheiten sind typischerweise über Intranets/WAN mit den Registrierungsservern verbunden und die IWF-Einheiten sind typischerweise im Besitz des WSP. Die IWF-Einheiten müssen indes nicht innerhalb des gleichen LAN angeordnet sein wie die Registrierungsserver. Typischerweise sind die Accounting- und Directory-Server (ebenfalls Softwaremodule, die auf einem Prozessor ausgeführt werden) über ein LAN mit den Registrierungsservern im Datenzentrum des Service Providers (d.h. ein Datenzentrum, das einen oder mehrere Prozessoren enthält, der/die verschiedenen Server und anderen Software-Module beherbergt/beherbergen) verbunden. Der Verkehr vom Endsystem wird dann über einen (mit dem LAN verbundenen) Router zum öffentlichen Internet oder dem Intranet des ISP geroutet. Auf den Registrierungsserver, der im Netz eines Fremd-WSP angeordnet ist, wird mit Fremd-Registrierungsserver (FRS) Bezug genommen und auf den Registrierungsserver, der im Heimatnetz des Endsystems angeordnet ist (wo das mobile System seinen Dienst kauft), wird als Heimat-Registrierungsserver (HRS) Bezug genommen. Auf die Interworking-Funktions-Einheit im Heimatnetz wird mit Heimat-IWF Bezug genommen, während auf die Interworking-Funktions-Einheit im Fremdnetz (d.h. das Netz, das das Endsystem besucht) als die dienende IWF Bezug genommen wird.

[0201] Für feste drahtlose Dienste (z.B. ein sich nicht bewegendes Endsystem), kann ein Endsystem sich vom Heimatnetz (z.B. beim Heimat-Dienst) oder von einem Fremdnetz (z.B. Roaming-Dienst) auf dem Heimatnetz für den Dienst registrieren. Das Endsystem empfängt eine durch einen Agenten gesendete Ankündigung (z.B. eine in Software ausgeführte Agentenfunktion) im drahtlosen Hub über den Zugangspunkt. Sowohl die MAC-Schicht-Registrierung als auch die Netzschichtregistrierung sind auszuführen. Diese können aus Gründen der Effizienz kombiniert werden.

[0202] Für Endsysteme in der Heimat (**Fig. 23**) gibt die Netzschichtregistrierung (wie die lokale Registrierung) dem Heimatregistrierungsserver den drahtlosen Hub bekannt, an den das Endsystem gegenwärtig angebunden ist. Eine IWF im Heimatnetz des Endsystems wird zum Anker oder zur Heimat-IWF. Somit reisen PPP-Rahmen zu und vom Endsystem über den drahtlosen Hub zur Heimat-IWF im Heimatnetz. Wenn das Endsystem zu Hause ist, wird die Heimat-IWF über ein XTunnel-Protokoll mit dem drahtlosen Hub verbunden.

[0203] Für roamende drahtlose Dienste (**Fig. 24**) bestimmt der Fremdregistrierungsserver die Identität des Heimatnetzes des roamenden Endsystems während der Registrierungsphase. Unter Verwendung dieser Informationen kommuniziert der Fremd-Registrierungsserver mit dem Heimat-Registrierungsserver, um das Endsystem zu authentifizieren und zu registrieren. Der Fremdregistrierungsserver teilt dann eine dienende IWF zu und eine I-XTunnel-Protokoll-Verbindung wird zwischen der Heimat-IWF und der dienenden IWF für das roamende Endsystem eingerichtet. Die dienende IWF überträgt Rahmen zwischen dem drahtlosen Hub und der Heimat-IWF. Von der Heimat-IWF werden Daten zu einem PPP-Server (d.h. ein Punkt-zu-Punkt-Protokollserver) gesendet, der in der gleichen IWF residieren kann. Wenn die Daten indes an ein Unternehmensintranet oder ein Intranet eines ISP, das seinen eigenen PPP-Server hat, gehen, werden die Daten über das L2TP-Protokoll zum separaten PPP-Server gesendet. Der separate Server ist typischerweise im Besitz eines Internet Service Providers, der ihn betreibt und der sich vom Wireless Service Provider unterscheidet. Für die Dauer der Sessionen bleiben die Standorte der Heimat-IWF und des PPP-Servers fest. Die MAC-Schicht-Registrierung kann mit der Netzregistrierung kombiniert werden, um Ersparnisse auf dem Overhead von separaten Kommunikationen für MAC-Schicht- und Netzschichtregistrierung zu realisieren; es kann indes von Vorteil sein, diese Registrierungsverfahren nicht zu kombinieren, derart, dass die Ausrüstung des WSP mit anderen drahtlosen Netzen, die reine IETF Mobile IP unterstützen, zusammenwirken kann.

[0204] Die Registrierung richtet drei Tabellen ein. Tabelle 1 ist mit jedem Zugangspunkt verbunden und Tabelle 1 identifiziert jede Verbindung (z.B. jedes Endsystem) durch eine Verbindungs-ID (CID) und verbindet die Verbindungs-ID mit einer bestimmten Adresse (d.h. die Adresse des Endsystems oder Endsystem) eines drahtlosen Modems (WM). Tabelle 2 ist mit jedem drahtlosen Hub (WH) verbunden und Tabelle 2 verbindet jede Verbindungs-ID mit einer/einem entsprechenden drahtlosen Modem-Adresse, Zugangspunkt und XTunnel-ID (XID). Tabelle 3 ist mit jeder Interworking-Funktion (IWF) verbunden und Tabelle 3 verbindet jede Verbindungs-ID mit einer entsprechenden drahtlosen Modem-Adresse, drahtlosen Hub-Adresse, XTunnel-ID und IP-Port (IP/Port). Die Einträge, die für diese Tabellen beschrieben werden, werden beschrieben, um lediglich relevante Einträge einzubeziehen, die die Erläuterung des Mobilitätsmanagements unterstützen. In der Realität bestehen andere wichtige Felder, die ebenfalls einbezogen werden müssen.

Tabelle 1: Verbindungstabelle bei AP

CID	WM
C1	WM1
C2	WM1
C1	WM2

Tabelle 2: Verbindungstabelle bei WH

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

Tabelle 3: Verbindungstabelle bei 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

[0205] Die Protokollstapel für Einwahlbenutzer in der Heimat in einem Netz sowie roamende Benutzer sind in Fig. 25-Fig. 28 veranschaulicht. Fig. 25 veranschaulicht Protokollstapel, die für direkten Internetzugang durch ein festes (d.h. ein sich nicht bewegendes) Endsystem in der Heimat verwendet wird, wo eine PPP-Protokoll-Nachricht in der Heimat-IWF endet (typischerweise gemeinsam mit dem drahtlosen Hub untergebracht), die Nachrichten zu und von einem IP-Router und von dort zum öffentlichen Internet überträgt. Fig. 26 veranschaulicht Protokollstapel, die für Fern-Internetzugang (d.h. entweder private Unternehmensnetze oder ein ISP) durch ein festes (d.h. sich nicht bewegendes) Endsystem in der Heimat verwendet werden, wo eine PPP-Protokoll-Nachricht durch die Heimat-IWF (typischerweise gemeinsam mit dem drahtlosen Hub untergebracht) an einen PPP-Server des privaten Unternehmensintranets oder ISP übermittelt wird. Fig. 27 veranschaulicht Protokollstapel, die für direkten Internetzugang durch ein roamendes aber festes (d.h. sich nicht bewegendes) oder ein sich bewegendes Endsystem verwendet wird, wo das PPP-Protokoll in der Heimat-IWF (typischerweise in einer Mobilvermittlungsstelle des Heimatnetzes) endet, das Nachrichten an und von einem IP-Router übermittelt. In Fig. 27 ist anzumerken, wie der Nachrichtenverkehr durch eine dienende IWF (typischerweise gemeinsam mit dem drahtlosen Hub untergebracht) zusätzlich zur Heimat IWF läuft. Fig. 28 veranschaulicht Protokollstapel, die für Fern-Internetzugang (d.h. entweder private Unternehmensnetze oder ein ISP) durch ein roamendes aber festes (d.h. ein sich nicht bewegendes) oder ein sich bewegendes Endsystem verwendet werden, wo eine PPP-Protokollnachricht durch die Heimat-IWF (typischerweise in einer Mobilvermittlungsstelle des Heimatnetzes angeordnet) an einen PPP-Server des privaten Unternehmensintranets oder ISP übermittelt wird. In Fig. 28 ist zu bemerken, wie der Nachrichtenverkehr durch eine dienende IWF (typischerweise gemeinsam mit dem drahtlosen Hub untergebracht) zusätzlich zur Heimat-IWF läuft. Wenn die dienende IWF und der drahtlose Hub gemeinsam im Nest von Computern untergebracht sind oder sogar im gleichen Computer programmiert sind, ist es nicht notwendig, einen Tunnel unter Verwendung eines XTunnel-Protokolls zwischen der dienenden IWF und dem drahtlosen Hub einzurichten.

[0206] Gleichwertige Abwandlungen dieser Protokollstapel (z.B. kann das RLP am drahtlosen Hub anstatt an der dienenden IWF oder Heimat-IWF für mobile Systeme in der Heimat enden) sind ebenfalls vorgesehen. Wenn die IWF in großer Entfernung vom drahtlosen Hub angeordnet ist und die Pakete potentiell über ein ver-

lustreiches IP-Netz zwischen der IWF und dem drahtlosen Hub getragen werden können, würde es bevorzugt werden, das RLP-Protokoll am drahtlosen Hub zu beenden. Eine andere Abwandlung ist, dass der XTunnel zwischen dem drahtlosen Hub und der IWF nicht zuoberst auf dem UPD/IP gebildet werden muss. Xtunnel können unter Verwendung der Frame-Relay/ATM Verbindungsschicht gebildet werden. Die Verwendung von UDP/IP macht es indes einfacher, den drahtlosen Hub und die IWF-Software von einem Netz zum anderen zu bewegen.

[0207] Des Weiteren kann das PPP-Protokoll in einem drahtlosen Modem enden und über eine Ethernet-Verbindung an ein oder mehrere Endsysteme gesendet werden. Wie in **Fig. 29** veranschaulicht, empfängt das drahtlose Modem **300** die PPP-Protokollinformationen und verkapselt die PPP-Nutzlast in einen Ethernet-Rahmen, der über die Internet-Verbindung **302** an mindestens eines der Endsysteme **304** und **306** zu transportieren ist.

[0208] DIX-Ethernet kann für das Einkapseln der XWD MAC-Grundelemente verwendet werden, aber das System ist nicht darauf beschränkt. Das Ethernet-Rahmenformat für XWD-Steuerrahmen wird in **Fig. 30** veranschaulicht. Der Ethernet-Kopf enthält eine Zieladresse, eine Quelladresse und ein Ethernet-Typenfeld. Das Zieladressenfeld enthält die Ethernet-Adresse der MAC-Einheit, an die das Grundelement gesendet wird. Für MAC-Grundelemente, die durch den MAC-Benutzer aufgerufen werden, enthält dieses Feld die Ethernet-Adresse des MAC-Benutzers. Für gesendete Grundelemente, ist dieses Feld die Ethernet-Sendeadresse. Das Quelladressfeld enthält die Ethernet-Adresse der MAC-Einheit, die das Grundelement aufruft. Das Ethernettypenfeld umfasst den Ethernet-Typ für XWD. Mögliche Werte sind XWD_Control für Steuerrahmen und XWD-Data für Datenrahmen. Diese Werte müssen sich von allen Ethernet-Typenwerten unterscheiden, die standardisiert wurden und müssen bei der Aufsichtsbehörde registriert werden.

[0209] Der Ethernet-Rahmen hat ein XWD-Kopffeld. Der XWD-Kopf kann 16 Bit lang sein und wird nur für XWD-Steuerrahmen vorhanden sein. Die Felder sind in **Fig. 31** veranschaulicht. Der Ethernet-Rahmen enthält ebenfalls einen Protokollkopf, ein PPP-Nutzlastfeld und ein XWD MAC-Feld. Die Kopfwerte für die Grundelemente, die Ethernet-Verkapselung verwenden, sind in Tabelle 4 untenstehend veranschaulicht.

Name Grund-Element	Ziel-Adresse	Quell-Adresse	Ethernet-Typ	XWD MAC Grund-Element
M_Discover.Req	Sende- oder Unicast-MAC-Provider	MAC Benutzer	XWD_Control	0
M_Discover.Cnf	MAC Benutzer	MAC Provider	XWD_Control	1
M_OpenSap.Req	MAC Provider	MAC Benutzer	XWD_Control	2
M_OpenSap.Cnf	MAC Benutzer	MAC Provider	XWD_Control	3
M_CloseSap.Req	MAC Provider	MAC Benutzer	XWD_Control	4
M_CloseSap.Cnf	MAC Benutzer	MAC Provider	XWD_Control	5
M_EchoSap.Req	MAC Benutzer	MAC Provider	XWD_Control	6
M_EchoSap.Cnf	MAC Provider	MAC Benutzer	XWD_Control	7
M_Connect.Req	MAC Provider (nur Modem)	MAC Benutzer (nur Endsystem)	XWD_Control	8
M_Connect.Ind	MAC Benutzer (nur drahtloser Hub)	MAC Provider (nur AP)	XWD_Control	9
M_Connect.Rsp	MAC Provider (nur AP)	MAC Benutzer (nur drahtloser Hub)	XWD_Control	10
M_Connect.Cnf	MAC Benutzer (nur Endsystem)	MAC Provider (nur Modem)	XWD_Control	11
M_Disconnect.Req	MAC Provider	MAC Benutzer	XWD_Control	12

[0210] Bei einer anderen Alternative kann das PPP-Protokoll in einem drahtlosen Router enden und dann an mindestens ein Endsystem, das mit einem lokalen Netz (LAN) verbunden ist, gesendet werden. Wie in Fig. 32 veranschaulicht, empfängt der drahtlose Router **350** die PPP-Protokollinformationen über das drahtlose Modem **352**. Der Router **354** empfängt die PPP-Informationen vom drahtlosen Modem **352** und sendet die PPP-Informationen über die LAN-Verbindung **362** an mindestens eines der Endsysteme **356**, **358**, **360**.

[0211] Vier Typen von Handoff-Szenarien können eintreten und sie sind wie folgt benannt: (i) lokale Mobilität, (ii) Mikromobilität, (iii) Makromobilität, und (iv) globale Mobilität. In allen vier Szenarien (in einer Ausführungsform der Erfindung) wird eine Route-Optimierungsoption nicht berücksichtigt, derart, dass die Standorte des Heimat-Registrierungsservers und der PPP-Server des ISP sich nicht ändern. In einer anderen Ausführungsform des Systems mit Route-Optimierung, können sich die PPP-Server des ISP ändern. Dieser Aspekt wird indes untenstehend erläutert. Zusätzlich ändern sich die Standorte des Fremd-Registrierungsservers und der IWF in den ersten drei Szenarien nicht.

[0212] Der vorgeschlagene IETF Mobile IP Standard erfordert, dass, immer wenn ein Endsystem das IP-Sub-Netz, an das es angebunden ist, wechselt, es eine Registrierungsanfragenachricht an einen Heimatagent in seinem Heimat-Sub-Netz sendet. Diese Nachricht trägt eine Care-of-Adresse, wo das Endsystem in neuem Sub-Netz erreicht werden kann. Wenn Verkehr, zum Beispiel von einem ISP an ein Endsystem, gesendet wird, fängt der Heimatagent den Verkehr, der für das Endsystem gebunden ist, auf, wenn er im Heimat-Sub-Netz eintrifft, und leitet den Verkehr dann an die Care-of-Adresse weiter. Die Care-of-Adresse identifiziert einen bestimmten Fremdagent im Fremd-Sub-Netz. Ein Fremdagent des Endsystems kann im Endsystem selbst oder in einem separaten Knoten, der wiederum Verkehr an das Endsystem (d.h., den Proxy-Registrierungsagent) weiterleitet, residieren. Mobile IP Handoffs enthalten einen Austausch von Steuernachrichten

zwischen einem Agent des Endsystems, dem Heimatagent des Endsystems und potentiell seinen entsprechenden Hosts (CHs) (mit Route-Optimierungsoption).

[0213] Der vorgeschlagene IETF Mobile IP Standard würde es schwierig finden, die Latenz- und Skalierbarkeitsziele für alle Bewegungen in einem großen Internetnetz zu erreichen. Das vorliegende hierarchische Mobilitätsmanagement erreicht solche Ziele indes. Für kleine Bewegungen (z.B. ein Wechsel der Zugangspunkte), werden lediglich MAC-Schicht-Neuregistrierungen benötigt. Für größere Bewegungen werden Netzschicht-Neuregistrierungen ausgeführt. Das vorliegende hierarchische Mobilitätsmanagement unterscheidet sich von der flachen Struktur, die im von IETF vorgeschlagenen Mobile IP Standard verwendet wird, sowie dem dienenden/Anker-Interworking-Funktionsmodell, das in zellularen Systemen wie CDPD (das auf einem Standard basiert, der vom Cellular Digital Packet Data Forum gestützt wird) verwendet wird.

[0214] Wie in Fig. 33 veranschaulicht, verwaltet das lokale Mobilitätshandoff die Bewegung des Endsystems (mit MN für Mobile Node bezeichnet) zwischen APs, die zum gleichen drahtlosen Hub gehören. Somit ist nur MAC-Schicht-Neuregistrierung erforderlich. Das Endsystem erhält eine Ankündigung vom drahtlosen Hub von einem neuen AP und antwortet mit einer an den neuen AP gerichteten Registrierungsanfrage.

[0215] Der neue AP (d.h. derjenige, der die Registrierungsanfrage vom Endsystem empfängt) erzeugt neue Einträge in seiner Verbindungstabelle und überträgt die Registrierungsmeldung an seinen drahtlosen Hub. In lokalen Mobilitätshandoffs, ändert sich der drahtlose Hub nicht. Der drahtlose Hub erkennt die Registrierungsanfrage des Endsystems als eine MAC-Schicht-Registrierungsanfrage und er aktualisiert seine Verbindungstabelle, damit sie die Verbindung mit dem neuen AP widerspiegelt. Dann löscht der alte AP den Verbindungseintrag von seiner Verbindungstabelle. Es bestehen mindestens drei Arten, auf die der alte AP die alten Einträge löschen kann, nämlich (i) bei einem Timeout, (ii) beim Empfangen von einer Kopie der übertragenen MAC-Schicht-Verbindungsnachricht vom neuen AP an den drahtlosen Hub (wenn diese Übertragungsnachricht eine gesendete Nachricht ist) und (iii) beim Erhalt der Information vom drahtlosen Hub, dass das Löschen des Eintrags erforderlich ist.

[0216] Wie in Fig. 34 veranschaulicht, verwaltet das Mikromobilitätshandoff die Bewegung des Endsystems (mit MN für Mobile Node bezeichnet) zwischen drahtlosen Hubs, die zum gleichen Registrierungsserver gehören und wo das Endsystem immer noch durch die bestehende dienende IWF bedient werden kann. Wenn eine Ankündigung vom neuen drahtlosen Hub (durch einen neuen AP) empfangen wird, sendet das Endsystem eine Nachricht zum Anfragen der Registrierung an den Registrierungsserver. Die Registrierungsanfrage wird vom neuen AP an den neuen drahtlosen Hub an den Registrierungsserver übertragen.

[0217] Wenn der Registrierungsserver bestimmt, dass die bestehende IWF immer noch verwendet werden kann, sendet der Registrierungsserver eine XTunnel-Bildungs-Anfragenachricht, um die bestehende IWF anzufragen, einen XTunnel zum neuen drahtlosen Hub zu bilden. Später sendet der Registrierungsserver eine XTunnel-Abbruchs-Anfragenachricht, um die bestehende IWF anzufragen, den bestehenden Xtunnel mit dem alten drahtlosen Hub abzubrechen. Die Xtunnel-Bildungs- und Abbruchs-Anfragenachrichten können in einer Nachricht kombiniert werden. Ein Fremdregistrierungsserver leitet die Registrierungsnachricht nicht an den Heimat-Registrierungsserver weiter, da keine Änderung der IWF, und zwar weder der dienenden IWF noch der Heimat-IWF, vorliegt.

[0218] Beim Empfangen einer positiven XTunnel-Bildungs-Antwort und einer positiven XTunnel-Abbruchs-Antwort von der IWF, sendet der Registrierungsserver eine Registrierungsantwort an das Endsystem. Wenn die Registrierungsantwort den neuen drahtlosen Hub erreicht, wird die Verbindungstabelle beim neuen drahtlosen Hub aktualisiert, um die Verbindung mit dem neuen AP widerzuspiegeln. Der neue AP aktualisiert seine MAC-Filter-Adressentabelle und Verbindungstabelle nach dem Empfangen einer Nachricht vom neuen drahtlosen Hub und die Registrierungsantwort wird an das Endsystem weitergeleitet.

[0219] 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 Verbindungstabelle des alten AP.

[0220] Wie in Fig. 35 dargestellt, verwaltet der Makromobilitäts-Handofffall Bewegung zwischen drahtlosen Hubs, die eine Änderung der dienenden IWF im Fremdnetz beinhaltet, aber sie beinhaltet keine Änderung im Registrierungsserver. Wenn eine Ankündigung von einem neuen drahtlosen Hub empfangen wird (durch einen neuen AP), sendet das Endsystem eine Nachricht, um die Netzschichtregistrierung anzufragen, an den Registrierungsserver. Die Registrierungsanfrage wird von der neuen AP an den neuen drahtlosen Hub an den Re-

gistrierungsserver übertragen.

[0221] Der Registrierungsserver erkennt, dass es ein Fremd-Registrierungsserver ist, wenn das Endsystem nicht zum Netz des vorliegenden Registrierungsservers gehört. Dieser Fremd-Registrierungsserver bestimmt die Identität des Heimat-Registrierungsservers unter Verwendung einer Anfrage, vorzugsweise einer Radius-Access-Anfrage (RA-Anfrage), an den Fremd-Directory-Server (wie große Gelbe Seiten) und weist eine geeignete IWF an, die dienende IWF zu sein, und er leitet eine Registrierungsanfrage an den Heimat-Registrierungsserver weiter, vorzugsweise durch eine Radius-Access-Anfrage (RA-Anfrage), die den Heimat-Registrierungsserver über die neu gewählte IWF informiert.

[0222] Der Heimat-Registrierungsserver authentifiziert die Registrierungsanfrage unter Verwendung einer Anfrage, vorzugsweise einer Radius-Access-Anfrage (RA-Anfrage) an den Heimat-Directory-Server. Beim Authentifizieren der Anfrage und beim Bestimmen, dass die bestehende Heimat-IWF immer noch verwendet werden kann, weist der Heimat-Registrierungsserver die Heimat-IWF an, einen neuen I-XTunnel zur neu zugewiesenen dienenden IWF zu bilden und den bestehenden I-XTunnel zur alten dienenden IWF abzubrechen. Beim Empfangen einer positiven I-XTunnel-Bildungs-Antwort und einer positiven I-XTunnel-Abbruchs-Antwort von der Heimat-IWF sendet der Heimat-Registrierungsserver eine Registrierungsantwort an den Fremd-Registrierungsserver.

[0223] Der Fremd-Registrierungsserver weist dann die neu zugewiesene IWF an, einen XTunnel zum neuen drahtlosen Hub zu bilden. Beim Empfangen einer positiven XTunnel-Bildungs-Antwort, weist der Fremd-Registrierungsserver die alte IWF an, den XTunnel zum alten drahtlosen Hub abzubrechen. Beim Empfangen einer positiven XTunnel-Bildungs-Antwort und einer positiven XTunnel-Abbruchs-Antwort sendet der Fremd-Registrierungsserver eine Registrierungsantwort an das Endsystem.

[0224] Wenn die Registrierungsantwort den neuen drahtlosen Hub erreicht, wird die Verbindungstabelle am neuen drahtlosen Hub aktualisiert, um die Verbindung mit dem neuen AP widerzuspiegeln. Der neue AP aktualisiert seine MAC-Filter-Adressentabelle und Verbindungstabelle nach dem Empfangen einer Nachricht vom neuen drahtlosen Hub und die Registrierungsantwort wird an das Endsystem weitergeleitet.

[0225] 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 Verbindungstabelle nach dem Empfangen einer Nachricht vom alten drahtlosen Hub.

[0226] Der globale Mobilitäts-Handofffall verwaltet Bewegung zwischen drahtlosen Hubs, die eine Änderung der Registrierungsserver beinhaltet. **Fig. 36** veranschaulicht einen globalen Mobilitätshandoff, in dem die Heimat-IWF sich nicht ändert und **Fig. 37** veranschaulicht ein globales Mobilitätshandoff, in dem sich die Heimat-IWF ändert. Wenn eine Ankündigung von einem neuen drahtlosen Hub (durch einen neuen AP) in einem neuen Fremdnetz empfangen wird, sendet das Endsystem eine Nachricht, um eine neue Netzschichtregistrierung anzufordern, an den neuen Fremd-Registrierungsserver. Die Registrierungsanfrage wird vom neuen AP an den drahtlosen Hub an den neuen Fremd-Registrierungsserver übertragen.

[0227] Der Registrierungsserver erkennt, dass es ein neuer Fremd-Registrierungsserver ist, wenn das Endsystem nicht zum Netz des vorliegenden Registrierungsservers gehört. Dieser Fremd-Registrierungsserver bestimmt die Identität des Heimat-Registrierungsservers durch die Verwendung einer Anfrage, vorzugsweise einer Radius-Access-Anfrage (RA-Anfrage), an den Fremd-Directory-Server (wie große Gelbe Seiten) und weist dann eine geeignete IWF an, die dienende IWF zu sein, und er leitet die Registrierungsanfrage an den Heimat-Registrierungsserver weiter, vorzugsweise durch eine Radius-Access-Anfrage (RA-Anfrage), die den Heimat-Registrierungsserver über die neu ausgewählte IWF informiert.

[0228] Der Heimat-Registrierungsserver authentifiziert die Registrierungsanfrage unter Verwendung einer Anfrage, vorzugsweise einer Radius-Access-Anfrage (RA-Anfrage) an den Heimat-Directory-Server. Beim Authentifizieren der Anfrage und beim Bestimmen, dass die bestehende Heimat-IWF immer noch verwendet werden kann (**Fig. 36**), weist der Heimat-Registrierungsserver die Heimat-IWF an, einen neuen I-XTunnel zur dienenden IWF, die durch den Registrierungsserver neu zugewiesen wurde, zu bilden. Der Heimat-Registrierungsserver sendet ebenfalls eine Registrierungsaufhebungsnachricht an den alten Fremd-Registrierungsserver und weist die Heimat-IWF an, den bestehenden I-XTunnel zur bestehenden dienenden IWF des alten Fremdnetzes abzubrechen. Beim Empfangen einer positiven I-XTunnel-Bildungs-Antwort und einer positiven I-XTunnel-Abbruchs-Antwort von der Heimat-IWF, sendet der Heimat-Registrierungsserver eine Registrie-

rungsantwort an den neuen Fremd-Registrierungsserver.

[0229] Der neue Fremd-Registrierungsserver weist dann die neu zugewiesene IWF an, einen XTunnel zum neuen drahtlosen Hub zu bilden. Beim Empfangen einer positiven XTunnel-Bildungsantwort sendet der Fremd-Registrierungsserver eine Registrierungsantwort an das Endsystem. Wenn die Registrierungsantwort den neuen drahtlosen Hub erreicht, wird die Verbindungstabelle beim neuen drahtlosen Hub aktualisiert, um die Verbindung mit dem neuen AP widerzuspiegeln. Der neue AP aktualisiert seine MAC-Filter-Adressentabelle und Verbindungstabelle nach dem Empfangen einer Nachricht vom neuen drahtlosen Hub und die Registrierungsantwort wird an das Endsystem weitergeleitet.

[0230] Der alte Fremd-Registrierungsserver weist die alte IWF an, den XTunnel zum alten drahtlosen Hub abzubrechen. Beim Empfangen einer positiven XTunnel-Abbruchs-Antwort oder gleichzeitig mit der XTunnel-Abbruchs-Anfrage sendet der alte Fremd-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 aktualisieren seine MAC-Filter-Adresstabelle und Verbindungstabelle nach dem Empfangen einer Nachricht vom alten drahtlosen Hub.

[0231] Alternativ wählt der Heimat-Registrierungsserver, nachdem der Heimat-Registrierungsserver die Registrierungsanfrage vom neuen Fremd-Registrierungsserver authentifiziert und bestimmt, dass die bestehende IWF nicht verwendet werden kann (**Fig. 37**), eine neue Heimat-IWF und weist die neue Heimat-IWF an, ein Level2Tunnel-Protokoll (L2TP-Tunnel) zum vorliegenden PPP-Server (z.B. dem PPP-Server in einem verbundenen ISP-Intranet) zu bilden. Dann weist der Heimat-Registrierungsserver die alte Heimat-IWF an, ihren L2TP-Tunnelverkehr an die neue Heimat-IWF zu übertragen.

[0232] Dann weist der Heimat-Registrierungsserver die neue IWF an, einen neuen I-XTunnel zur dienenden IWF, die durch den neuen Fremdregistrierungsserver neu zugewiesen wurde, zu bilden. Der Heimat-Registrierungsserver sendet ebenfalls eine Nachricht zum Aufheben der Registrierung an den alten Fremd-Registrierungsserver und weist die Heimat-IWF an, den bestehenden I-XTunnel zur bestehenden dienenden IWF des alten Fremdnetzes abzubrechen. Beim Empfangen einer positiven I-XTunnel-Bildungs-Antwort und einer positiven I-XTunnel-Abbruchs-Antwort von der Heimat-IWF sendet der Heimat-Registrierungsserver eine Registrierungsantwort an den neuen Fremd-Registrierungsserver.

[0233] Der neue Fremd-Registrierungsserver weist dann die neu zugewiesene IWF an, einen XTunnel zum neuen drahtlosen Hub zu bilden. Beim Empfangen einer positiven XTunnel-Bildungs-Antwort sendet der Fremd-Registrierungsserver eine Registrierungsantwort an das Endsystem. Wenn die Registrierungsantwort den neuen drahtlosen Hub erreicht, wird die Verbindungstabelle beim neuen drahtlosen Hub aktualisiert, um die Verbindung zum neuen AP widerzuspiegeln. Der neue AP aktualisiert seine MAC-Filter-Adressentabelle und Verbindungstabelle nach dem Empfangen einer Nachricht vom neuen drahtlosen Hub und die Registrierungsantwort wird an das Endsystem weitergeleitet.

[0234] Der alte Fremd-Registrierungsserver weist die alte IWF an, den XTunnel zum alten drahtlosen Hub abzubrechen. Beim Empfangen einer positiven XTunnel-Abbruchs-Antwort oder gleichzeitig mit der XTunnel-Abruchs-Anfrage, sendet der alte Fremd-Registrierungsserver eine Freigabenachricht an den alten drahtlosen Hub. Wenn der alte drahtlose Hub die Freigabenachricht empfängt, aktualisiert er seine Verbindungstabelle und die MAC-Filter-Addressentabelle und der alte AP aktualisiert seine MAC-Filter-Adressentabelle und Verbindungstabelle nach dem Empfangen einer Nachricht vom alten drahtlosen Hub.

[0235] Endsysteme, die gemäß dem vorliegenden System konstruiert sind, interoperieren mit Netzen, die gemäß den vorgeschlagenen IETF Mobile IP Standards konstruiert sind, und Endsysteme, die gemäß den vorgeschlagenen IETF Mobile IP Standards konstruiert sind, interoperieren mit Netzen, die gemäß der vorliegenden Erfindung konstruiert sind.

[0236] Die Unterschiede zwischen dem vorliegenden System und dem IETF Mobile IP (RFC2002, ein Standard-Dokument) enthalten Folgendes:

(i) Das vorliegende System ist ein hierarchisches Konzept für Mobilitätsmanagement anstatt eine flache Struktur wie im vorgeschlagenen IETF Mobile IP Standard. Geringe Mobilität innerhalb eines kleinen Bereichs ergibt keine Registrierung auf Netzebene. Mikromobilität enthält das Einrichten eines neuen XTunnels und das Abbrechen eines bestehenden XTunnels. Globale Mobilität enthält außer dem Einrichten/Abbrechen eines X-Tunnels als Minimum das Einrichten eines neuen I-XTunnels und das Abbrechen eines bestehenden I-XTunnels. Globale Mobilität enthält manchmal ebenfalls das Einrichten eines neuen

L2TP-Tunnels und den Transfer des L2TP-Zustands vom bestehenden L2TP-Tunnel zum neuen L2TP-Tunnel.
(ii) In der vorliegenden Erfindung wird, anstatt einer festen Heimat-Adresse wie im Fall des vorgeschlagenen IETF Mobile IP Standards, ein Benutzername plus ein Bereich verwendet, um einen Fern-Einwahlbenutzer zu identifizieren.
(iii) In der vorliegenden Erfindung werden die Registrierungs- und Routing-Funktionen durch separate Einheiten ausgeführt. Die zwei Funktionen werden im vorgeschlagenen IETF Mobile IP Standard durch den Heimatagent ausgeführt und beide Funktionen werden im vorgeschlagenen IETF Mobile IP Standard durch den Fremdagent ausgeführt. Im Gegensatz dazu wird die Registrierung in einer Ausführungsform der vorliegenden Erfindung im Registrierungsserver ausgeführt und die Routing-Funktionen werden sowohl durch die Heimat- und Fremd-IWF als auch durch den drahtlosen Hub (auf den auch mit Access-Hub Bezug genommen wird) ausgeführt.
(iv) Die vorliegende Erfindung verwendet drei Tunnel pro PPP-Session. Der XTunnel ist mehr ein Verbindungsschichttunnel zwischen dem drahtlosen Hub und der dienenden IWF. Der I-XTunnel zwischen der dienenden IWF und der Heimat-IWF ist mehr wie ein Tunnel zwischen Heimat- und Fremdagenten im vorgeschlagenen IETF Mobile IP Standard. Er verfügt jedoch über zusätzliche Fähigkeiten, die über diejenigen der Tunnel, die durch den Mobile IP Standard vorgeschlagen werden, hinausgehen. Der L2TP-Tunnel wird nur verwendet, wenn die Heimat IWF kein PPP-Server ist. Die Anzahl dieser Tunnel kann durch Kombinieren einiger Funktionen in den gleichen Knoten wie vorhergehend beschrieben reduziert werden.
(v) In der vorliegenden Erfindung erfolgt die drahtlose Registrierung vor dem Start der PPP-Session während die Mobile IP Registrierang im vorgeschlagenen IETF Mobile IP Standard erfolgt, nachdem die PPP-Session in den offenen Zustand eintritt.
(vi) In der vorliegenden Erfindung ist die Netzeinheit, die die Agentenankündigung ankündigt (d.h. der drahtlose Hub) nicht auf einer direkten Verbindung mit den Endsystemen während die Agentenankündigung für den vorgeschlagenen IETF Mobile IP Standard eine TTL von 1 haben muss, was bedeutet, dass die Endsysteme eine direkte Verbindung mit dem Fremdagenten haben. Zusätzlich ist die Agentenankündigung in den vorliegenden Systemen keine Erweiterung für die ICMP-Router-Ankündigungen wie im vorgeschlagenen IETF Mobile IP Standard.

[0237] Endsysteme in der vorliegenden Erfindung sollten Agent Solicitation unterstützen. Wenn ein Endsystem im vorliegenden System ein Netz besucht, das den vorgeschlagenen IETF Mobile IP Standard unterstützt, wartet es, bis es eine Agentenankündigung erhält. Wenn es innerhalb eines angemessenen Zeitraums keine Agentenankündigung empfängt, sendet es eine Agent Soliciation.

[0238] In der vorliegenden Erfindung können Netzbetreiber mit anderen Netzen verhandeln, die den vorgeschlagenen IETF Mobile IP Standard unterstützen, derart, dass den Endsystemen des vorliegenden Systems, die andere Netze verwenden möchten, Heimatadressen zugewiesen werden können. Wenn das Endsystem des vorliegenden Systems eine Agentenankündigung empfängt, kann es bestimmen, dass das Netz, das es besucht, kein Netz gemäß dem vorliegenden System ist und verwendet deshalb für die Registrierung die zugewiesene Heimatadresse.

[0239] Für Netze, die den vorgeschlagenen IETF Mobile IP Standard unterstützen, startet die PPP-Session vor der Mobile IP Registrierung und es wird vorausgesetzt, dass der PPP-Server in solchen Netzen gemeinsam mit dem Fremdagenten untergebracht ist. In einer Ausführungsform, wird ein SNAP-Kopf verwendet, um PPP-Rahmen in den MAC-Rahmen des vorliegenden Systems (auf eine Weise, die dem Ethernet-Format ähnlich ist) zu verkapseln und der Fremdagent interpretiert dieses Format als ein proprietäres PPP-Format über Ethernet-Einkapselung. Somit können das Endsystem des vorliegenden Systems und sein PPP-Peer in einen offenen Zustand eintreten, bevor der Fremdagent das Übermitteln einer Agentenankündigung startet und das Endsystem des vorliegenden Systems kann sich registrieren.

[0240] Um es den Endsystemen, die den vorgeschlagenen IETF Mobile IP Standard unterstützen, zu ermöglichen, in Netzen des Typs der vorliegenden Erfindung zu arbeiten, sind solche Mobiltelefone mindestens imstande, gleichartige MAC-Schicht-Registrierungen auszuführen. Indem das Agentenankündigungs-Nachrichtenformat dem Format der Agentenankündigungsnachricht des vorgeschlagenen Mobile IP Standards ähnlich gemacht wird, kann das besuchende Endsystem die Agentenankündigung interpretieren und sich beim drahtlosen Hub registrieren. In der vorliegenden Erfindung sind Registrierungsanfrage- und Antwortnachrichten gleichartig wie die Registrierungsanfrage- und Antwortnachrichten (ohne unnötige Erweiterungen) des vorgeschlagenen IETF Mobile IP Standards, derart, dass der Rest der Mobilitätsmanagementmerkmale des vorliegenden Systems für das besuchende Endsystem transparent ist.

[0241] Da die Endsysteme, die den vorgeschlagenen IETF Mobile IP Standard unterstützen, vor der Mobile IP Registrierung den Start einer PPP-Session erwarten, startet ein wahlfreies Merkmal in drahtlosen Hubs des vorliegenden Systems das Interpretieren von PPP LCP, NCP Paketen nach MAC-Schicht-Registrierungen.

[0242] Um während der Handoffs einen Verlust von Verkehr zu vermeiden, arbeitet das Mobilitätsmanagement des vorliegenden Systems nach einem unterbrechungslosen Konzept. Für lokale Mobilität, wird eine unterbrechungslose Verbindung erreicht, indem die MAC-Schicht-Registrierungsnachricht, die durch den neuen AP zum drahtlosen Hub übertragen wird, in eine gesendete Nachricht umgewandelt wird. Hierdurch kann der alte AP von einer neuen Registrierung erfahren und Pakete, die für das Endsystem bestimmt sind, die noch nicht an den neuen AP übermittelt wurden, weiterleiten.

[0243] Für Mikromobilität werden Informationen über den neuen drahtlosen Hub in die XTunnel-Abbruchs-Nachricht, die zwischen der dienenden IWF und dem alten WH ausgetauscht wird, eingefügt. Hierdurch kann der alte drahtlose Hub beim Empfangen einer XTunnel-Abbruchs-Nachricht von der dienenden IWF die gepufferten Pakete an den neuen drahtlosen Hub weiterleiten. Alternativ kennt die RLP-Schicht bei der IWF die Ablaufnummer, die bisher durch den alten drahtlosen Hub bestätigt wurde.

[0244] Gleichzeitig kennt die IWF die gegenwärtige Sendeablaufnummer des letzten an den drahtlosen Hub gesendeten Pakets. Deshalb kann die IWF diese Pakete, die zwischen diesen beiden Nummern angeordnet sind, an den neuen drahtlosen Hub weiterleiten, bevor neuere Pakete gesendet werden. Der zweite Ansatz ist wahrscheinlich dem ersten Ansatz gegenüber zu bevorzugen, da der alte drahtlose Hub möglicherweise nicht direkt mit dem anderen kommunizieren kann.

[0245] Für Makromobilität kann die alte dienende IWF Pakete an die neue dienende IWF weiterleiten, zusätzlich zu den Paketweiterleitungen, die vom alten drahtlosen Hub zum neuen drahtlosen Hub ausgeführt werden. Es muss dazu lediglich die Identität der neuen dienenden IWF an die neue dienende IWF in der I-XTunnel-Abbruchs-Nachricht weitergeleitet werden. Eine andere Möglichkeit, das gleiche Ergebnis zu erreichen, ist, die Heimat-IWF die fehlenden Pakete an die neue dienende IWF weiterleiten zu lassen, anstatt von der alten dienenden IWF zu verlangen, dies zu tun, da die Heimat-IWF die I-XTunnel-Ablaufnummer, die als letztes durch die alte dienende IWF bestätigt wurde und die gegenwärtige I-XTunnel-Ablaufnummer, die durch die Heimat-IWF gesendet wurde, kennt.

[0246] Das Verfahren zum Schätzen, wie viel Puffer pro mobiber Einheit pro AP pro drahtlosen Hub pro IWF zugeteilt werden sollte, derart, dass die Verkehrsverluste zwischen Handoffs minimiert werden können, besteht darin, das Endsystem für den AP für den drahtlosen Hub für die IWF die Paketeingangsrate und die Handoffzeit schätzen zu lassen. Diese Informationen werden an den alten AP des drahtlosen Hubs der IWF weitergeleitet, um zu bestimmen, wie viel Verkehr in dieser Reihenfolge an den neuen AP des drahtlosen Hubs der IWF bei Handoffs übertragen werden sollte.

[0247] Um in der vorliegenden Erfindung Route-Optimierung zu erreichen, wählt das Endsystem den PPP-Server, der der dienenden IWF am nächsten ist. Ohne Route-Optimierung können überhöhte Transportverzögerungen und eine überhöhte Verwendung der physischen Leitungen auftreten.

[0248] Zum Beispiel kann ein Endsystem, das an ein Heimatnetz in New York City abonniert ist, nach Hongkong roamen. Zum Einrichten einer Verbindung zu einem ISP in Hongkong, hätte das Endsystem eine in einem drahtlosen Hub in Hongkong eingerichtete dienende IWF und eine im Heimatnetz in New York City eingerichtete Heimat-IWF. Eine Nachricht würde dann vom Endsystem (nach Hongkong geroamt) durch die dienende IWF (in Hongkong) und durch die Heimat-IWF (in New York City) und zurück zum ISP in Hongkong geroutet.

[0249] Ein bevorzugter Ansatz ist, die Verbindung von der dienenden IWF (in Hongkong) direkt zum ISP in Hongkong einzurichten. Die dienende IWF agiert wie die Heimat-IWF. In dieser Ausführungsform bestehen Roaming-Vereinbarungen zwischen den Heimat- und Fremd-wireless-Service-Providern. Zusätzlich kommunizieren die verschiedenen Accounting-/Abrechnungssysteme automatisch miteinander, derart, dass Abrechnungsinformationen geteilt werden. Der Austausch von Accounting-/Abrechnungsinformationen kann unter Verwendung von Standards, wie beispielsweise dem Standard, der durch die ROAMOPS-Arbeitsgruppe der IETF vorgeschlagen wird, ausgeführt werden.

[0250] Die dienende IWF muss indes immer noch den nächsten PPP-Server finden (z.B. den ISP von Hongkong). In der vorliegenden Ausführungsform erfährt der Fremd-Registrierungsserver vom Wunsch des Endsystems, sich mit einem PPP-Server zu verbinden (z.B. einem ISP von Hongkong), wenn er eine Registrierungs-

anfrage vom Endsystem empfängt. Wenn der Fremd-Registrierungsserver bestimmt, dass die dienende IWF näher am gewünschten PPP-Server (z.B. dem ISP von Hongkong) ist als die Heimat-IWF, weist der Fremdregistrierungsserver die dienende IWF an, einen L2TP-Tunnel zu seinem nächsten PPP-Server (im Gegensatz zum PPP-Server, der am nächsten an Heimat-Registrierungsserver und Heimat-IWF ist) einzurichten. Dann informiert der Fremd-Registrierungsserver den Heimat-Registrierungsserver, dass das Endsystem durch die dienende IWF und das Fremd-PPP bedient wird.

[0251] In einer alternativen Ausführungsform, bestimmt der Fremd-Registrierungsserver, dass die IWF näher am gewünschten PPP-Server (z.B. dem ISP von Hongkong) ist, als die Heimat-IWF, wenn er eine Registrierungsanfrage vom Endsystem empfängt. Der Fremd-Registrierungsserver überträgt die Registrierungsanfragenachricht an den Heimat-Registrierungsserver mit einer verbundenen Nachricht, die die Informationen der dienenden IWF und eine Benachrichtigung, dass Route-Optimierung bevorzugt wird, angibt. Gleichzeitig weist der Fremd-Registrierungsserver die dienende IWF an, einen L2TP-Tunnel zum PPP-Server einzurichten. Beim Bestätigen der Registrierungsanfrage weist der Heimat-Registrierungsserver die Heimat-IWF an, den L2TP-Zustand an die Fremd-IWF zu übertragen.

[0252] Während bevorzugte Ausführungsformen einer neuen Netzarchitektur mit drahtlosen Endbenutzern, die imstande sind, zu roamen (von denen beabsichtigt wird, dass sie veranschaulichend und nicht einschränkend sind), beschrieben wurden, wird angemerkt, dass Änderungen und Abwandlungen im Lichte der vorhergehenden Lehren durch Fachleute vorgenommen werden können. Zum Beispiel können sich die hierin beschriebenen Verbindungslinks auf bekannte Verbindungsprotokolle (z.B., IP, TCP/IP, L2TP, IEEE 802.3, usw.) beziehen; das System fasst indes andere Verbindungsprotokolle in Verbindungslinks ins Auge, die die gleichen oder gleichartige Datenlieferungsfähigkeiten haben. Agierende Agenten in den vorhergehend beschriebenen Ausführungsformen können in der Form von softwaregesteuerten Prozessoren oder andere Steuerungsformen (z.B. programmierbare Logik-Arrays, usw.) sein. Agierende Agenten können wie vorhergehend beschrieben gruppiert werden oder auf eine andere Art unter Befolgung der Verbindungslehren, die hierin beschrieben werden und die den Sicherheits- und Authentifizierungslehren, wie hierin beschrieben, unterliegen, gruppiert werden. Des Weiteren kann ein einzelner Zugangspunkt, Access Hub (z.B. drahtloser Hub) oder eine Interworking-Funktions-Einheit (IWF-Einheit) Mehrkanal-Fähigkeiten bereitstellen. Damit kann ein einzelner Access Hub oder eine einzelne IWF-Einheit auf Verkehr von mehreren Endsystemen agieren und das, was hierin als separate Zugangspunkte, Access Hubs der IWF-Einheiten beschrieben wird, fasst Gleichwertigkeit mit einem/einer einzelnen Mehrkanal-Zugangspunkt, Access Hub oder IWF-Einheit ins Auge.

Patentansprüche

1. Drahtloses Datennetz (**30**), umfassend:
ein Heimatnetz, das eine Heimat-Mobilvermittlungsstelle (**40**), ein drahtloses Modem (**36**) und mindestens ein Endsystem (**32**) enthält, wobei das drahtlose Modem und das mindestens eine Endsystem über eine Ethernet-Verbindung (**38**) miteinander verbunden sind; und
einen PPP-Server (**74**), **dadurch gekennzeichnet**, daß das drahtlose Modem dafür ausgelegt ist, von dem PPP-Server gesendete PPP-Informationen für das mindestens eine Endsystem in einem Ethernet-Rahmen zu verkapseln und die PPP-Informationen über die Ethernet-Verbindung zu dem mindestens einen Endsystem zu senden.

2. Drahtloses Datennetz nach Anspruch 1, wobei PPP-Informationen von dem mindestens einen Endsystem über die Ethernet-Verbindung zu dem drahtlosen Modem gesendet und dann von dem drahtlosen Modem zu dem PPP-Server übertragen werden.

3. Drahtloses Datennetz nach Anspruch 1, wobei die Heimatvermittlungsstelle eine Heimat-Interworking-Funktion (**72**) enthält.

4. Drahtloses Datennetz nach Anspruch 3, wobei PPP-Informationen von dem PPP-Server durch die Heimat-Interworking-Funktion zu dem drahtlosen Modem übertragen werden.

5. Drahtloses Datennetz nach Anspruch 4, wobei PPP-Informationen von dem mindestens einen Endsystem über die Ethernet-Verbindung zu dem drahtlosen Modem gesendet und dann durch die Heimat-Interworking-Funktion von dem drahtlosen Modem zu dem PPP-Server übertragen werden.

Es folgen 31 Blatt Zeichnungen

Anhängende Zeichnungen

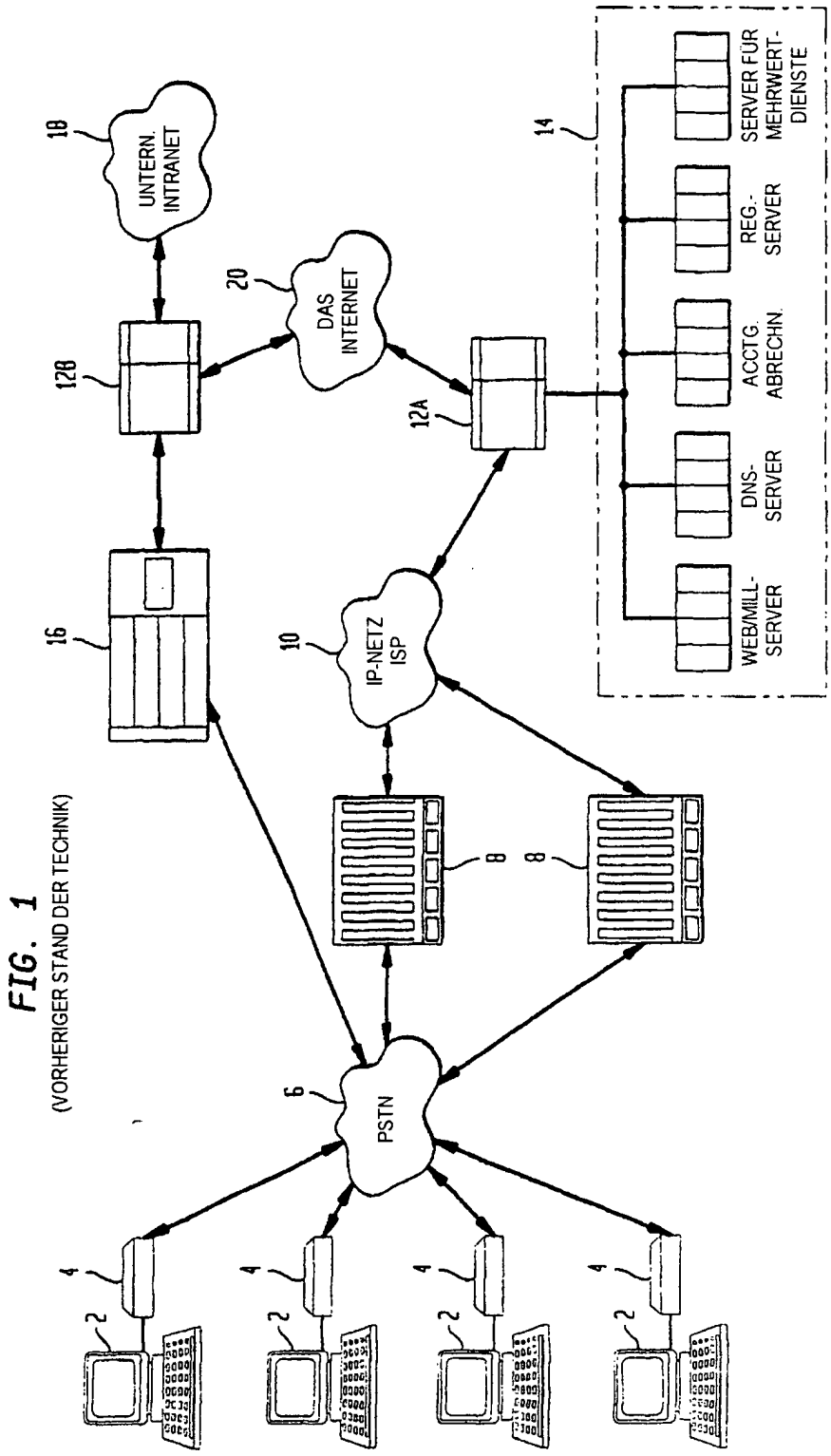


FIG. 1
(VORHERIGER STAND DER TECHNIK)

FIG. 2

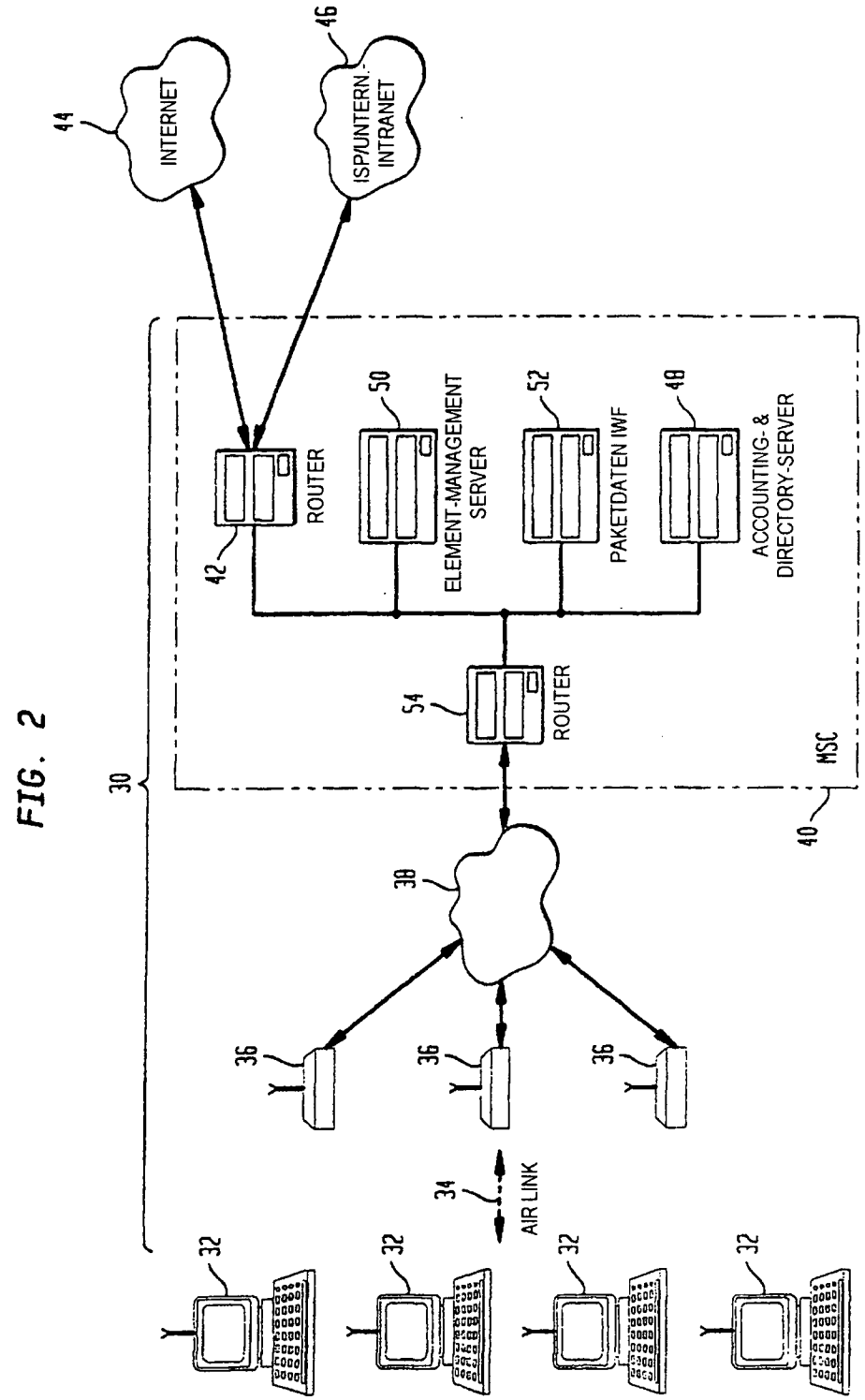

INTERNET
44
ISP/UNTERN.-INTRANET
46
ROUTER
42
50
ELEMENT-MANAGEMENT SERVER
52
PAKETDATEN IWF
48
ACCOUNTING- & DIRECTORY-SERVER
ROUTER
54
MSC
40
30
38
36
36
36
34
AIR LINK
32
32
32
32

FIG. 3

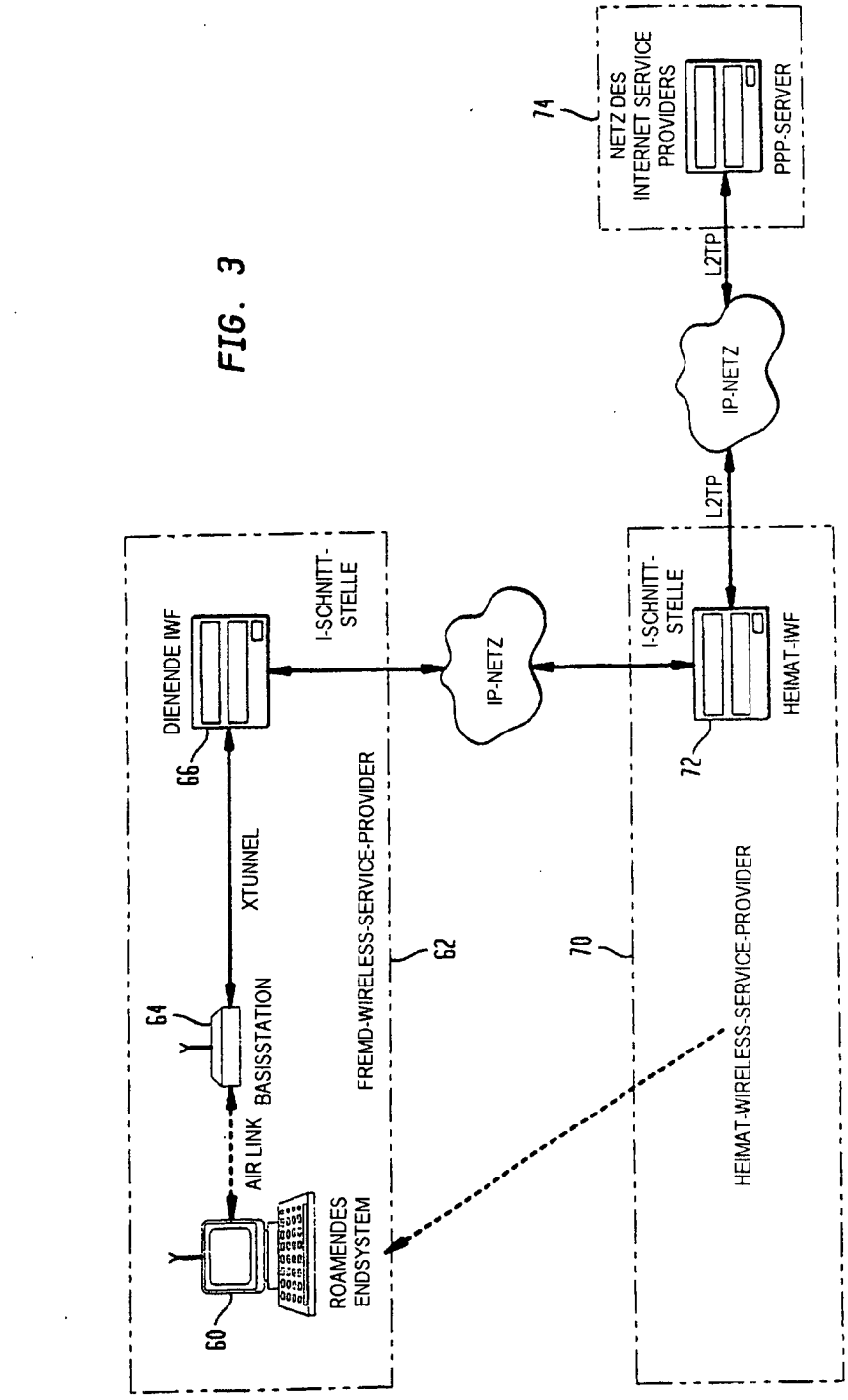

NETZ DES INTERNET SERVICE PROVIDERS
PPP-SERVER
74
L2TP
IP-NETZ
L2TP
I-SCHNITT-STELLE
HEIMAT-IWF
72
IP-NETZ
I-SCHNITT-STELLE
DIENENDE IWF
66
XTUNNEL
64
BASISSTATION
AIR LINK
ROAMENDES ENDSYSTEM
60
FREMD-WIRELESS-SERVICE-PROVIDER
62
70
HEIMAT-WIRELESS-SERVICE-PROVIDER

FIG. 4

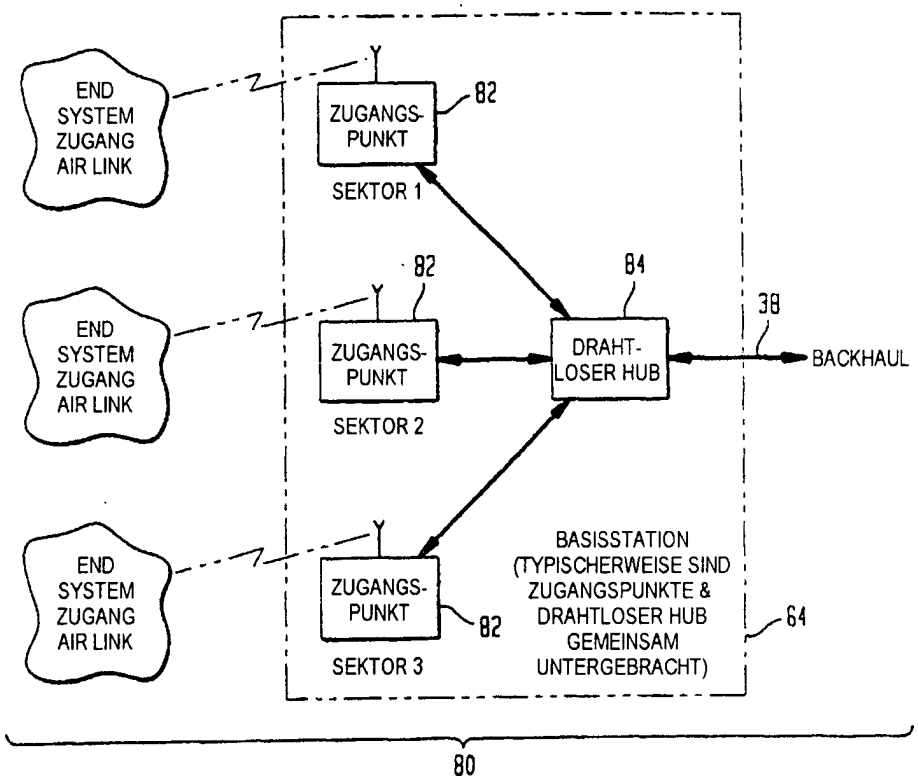

END SYSTEM ZUGANG AIR LINK
END SYSTEM ZUGANG AIR LINK
END SYSTEM ZUGANG AIR LINK
ZUGANGS-PUNKT
SEKTOR 1
ZUGANGS-PUNKT
SEKTOR 2
ZUGANGS-PUNKT
SEKTOR 3
82
82
82
84
DRAHT-LOSER HUB
88
BACKHAUL
BASISSTATION (TYPISCHERWEISE SIND ZUGANGSPUNKTE & DRAHTLOSER HUB GEMEINSAM UNTERGEBRACHT)
64
80

FIG. 5

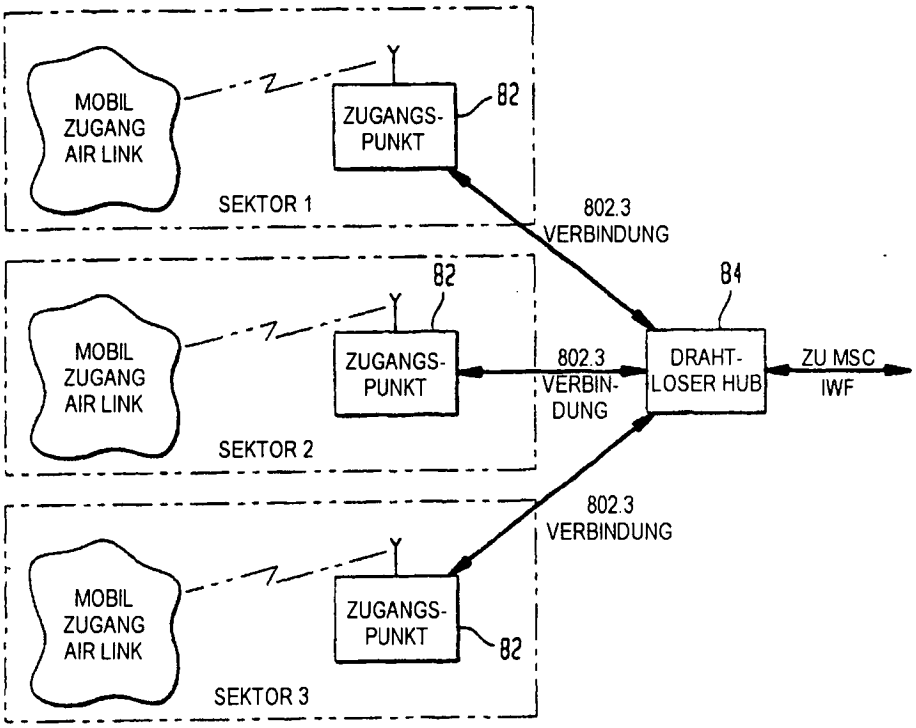

MOBIL ZUGANG AIR LINK
ZUGANGS-PUNKT
82
SEKTOR 1
802.3 VERBINDUNG
84
DRAHT-LOSER HUB
ZU MSC IWF
802.3 VERBIN-DUNG
SEKTOR 2
SEKTOR 3

FIG. 6

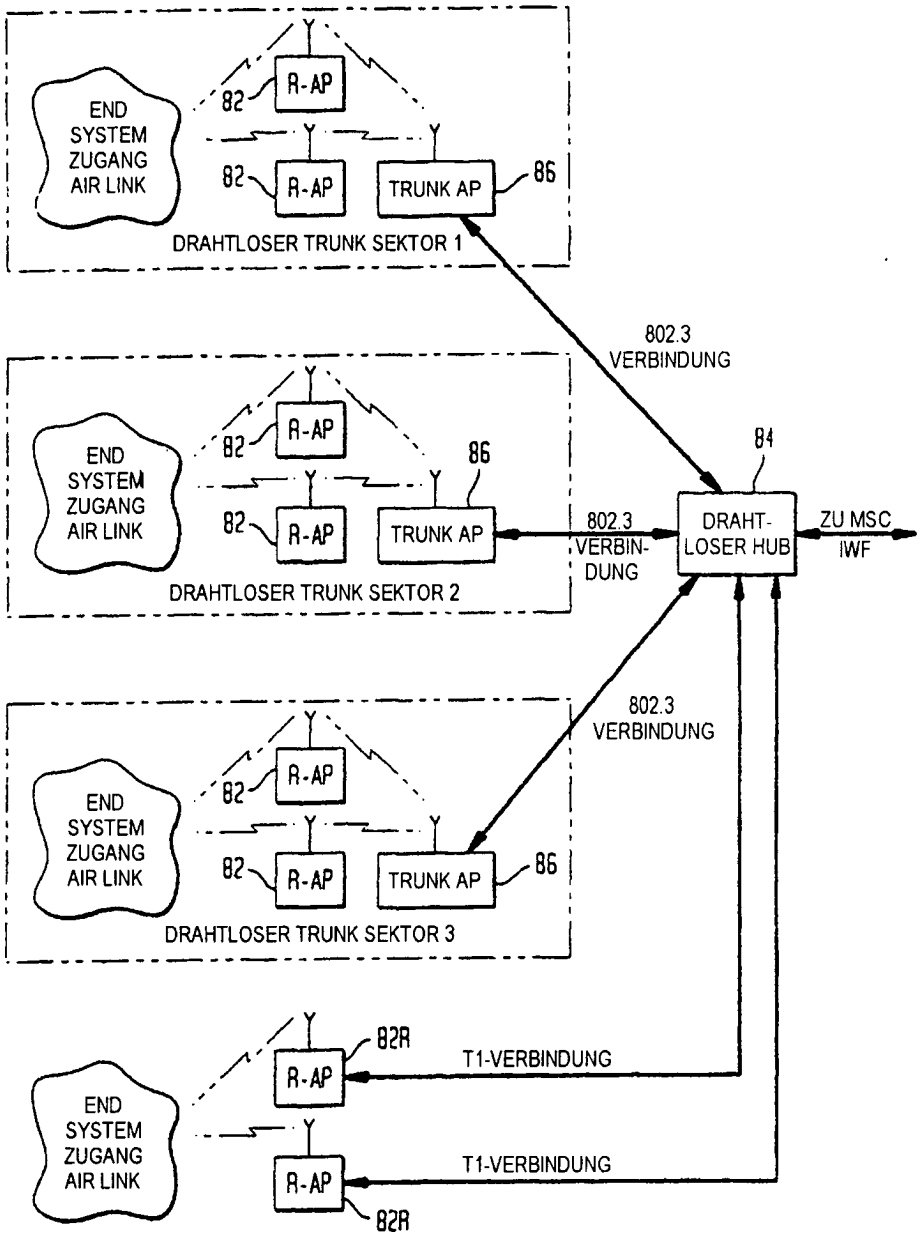

END SYSTEM ZUGANG AIR LINK
82
R-AP
82
R-AP
TRUNK AP
86
DRAHTLOSER TRUNK SEKTOR 1
802.3 VERBINDUNG
84
DRAHT-LOSER HUB
ZU MSC IWF
802.3 VERBIN-DUNG
DRAHTLOSER TRUNK SEKTOR 2
802.3 VERBINDUNG
DRAHTLOSER TRUNK SEKTOR 3
82R
T1-VERBINDUNG
T1-VERBINDUNG

FIG. 7

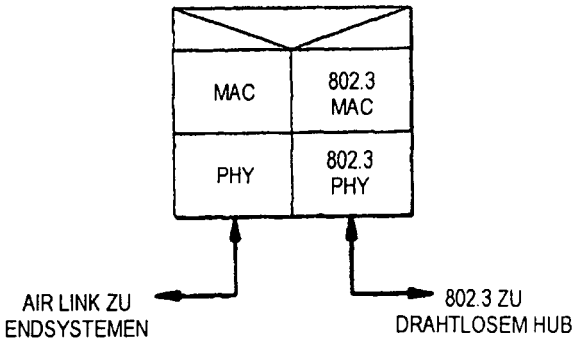


FIG. 8

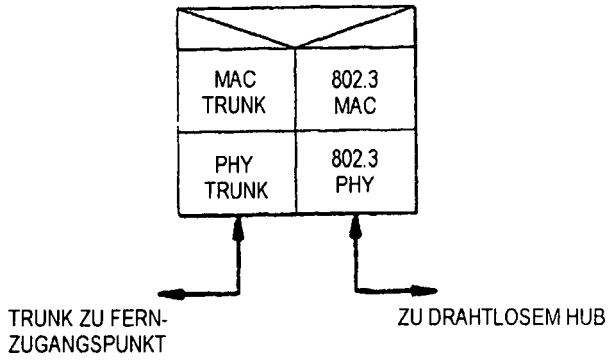


FIG. 9

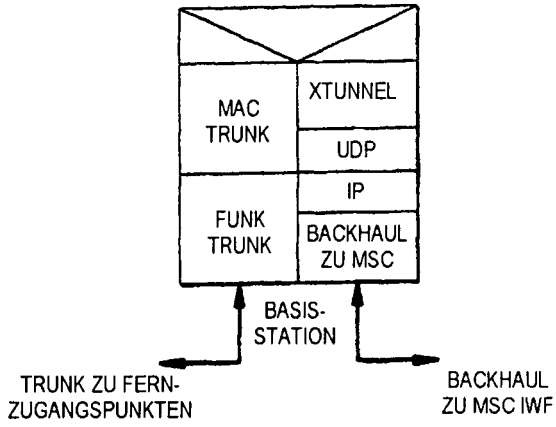


FIG. 10

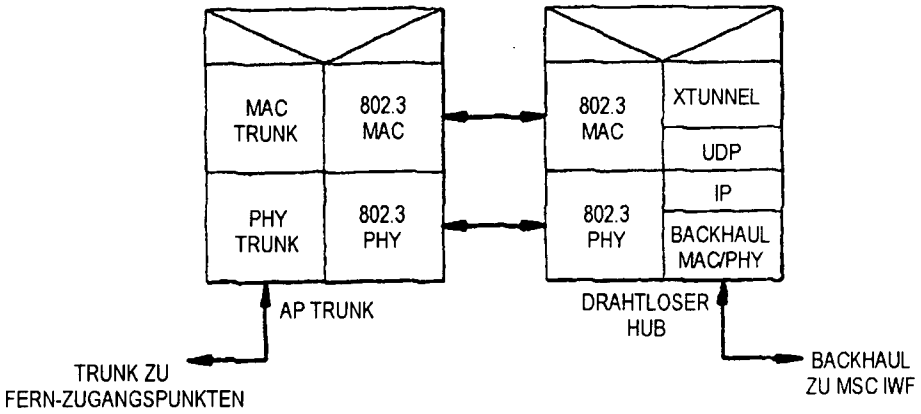

MAC TRUNK
802.3 MAC
PHY TRUNK
802.3 PHY
802.3 MAC
XTUNNEL
UDP
IP
802.3 PHY
BACKHAUL MAC/PHY
AP TRUNK
DRAHTLOSER HUB
TRUNK ZU FERN-ZUGANGSPUNKTEN
BACKHAUL ZU MSC IWF

FIG. 11

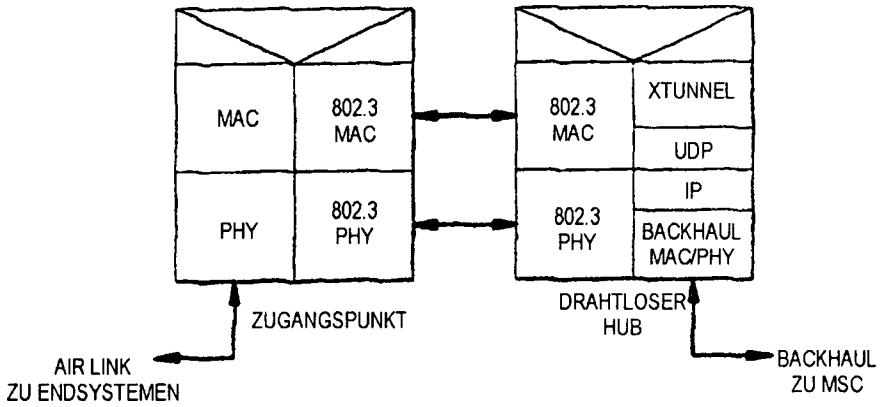

MAC
802.3 MAC
PHY
802.3 PHY
802.3 MAC
XTUNNEL
UDP
IP
802.3 PHY
BACKHAUL MAC/PHY
ZUGANGSPUNKT
DRAHTLOSER HUB
AIR LINK ZU ENDSYSTEMEN
BACKHAUL ZU MSC

FIG. 12

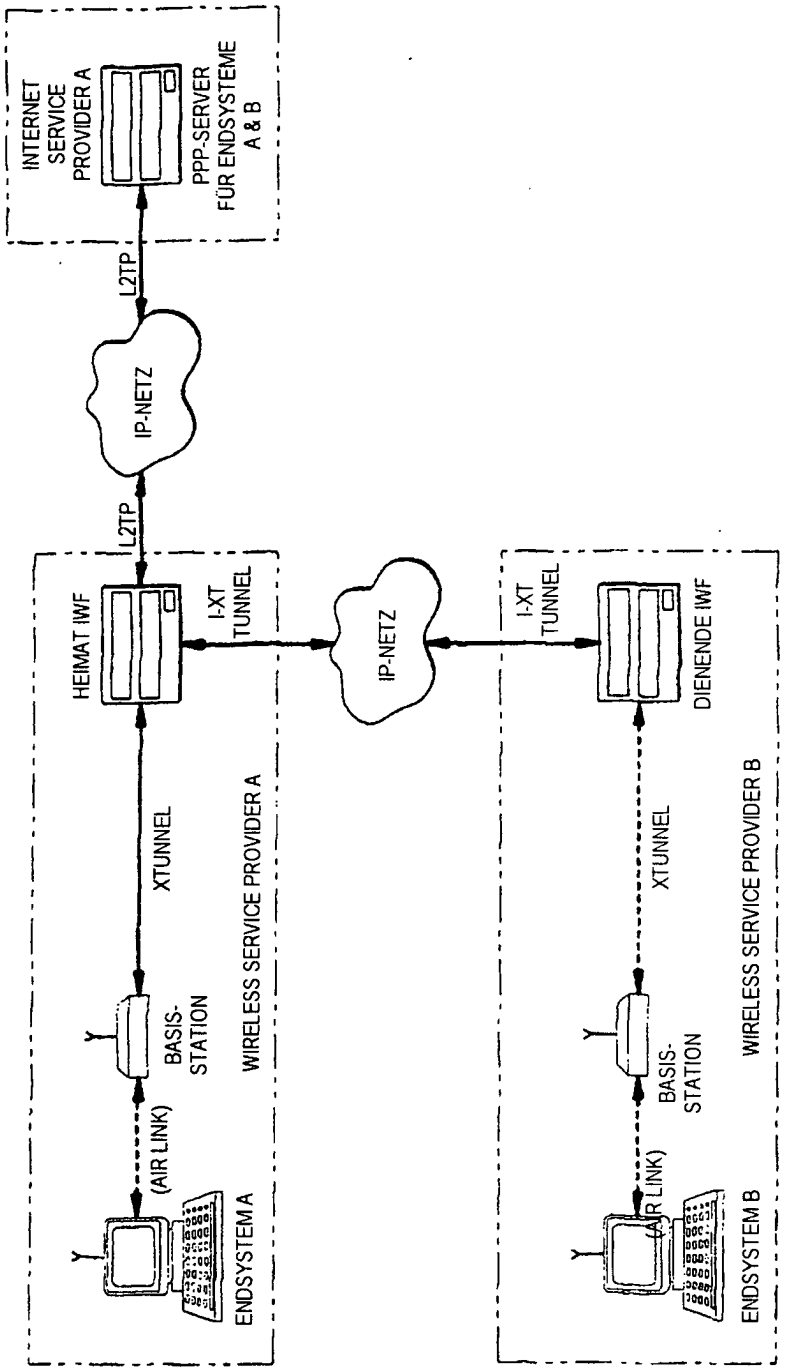

INTERNET SERVICE PROVIDER A
PPP-SERVER FÜR ENDSYSTEME A & B
L2TP
IP-NETZ
L2TP
HEIMAT IWF
I-XT TUNNEL
IP-NETZ
I-XT TUNNEL
DIENENDE IWF
XTUNNEL
XTUNNEL
BASIS-STATION
BASIS-STATION
(AIR LINK)
(AIR LINK)
WIRELESS SERVICE PROVIDER A
WIRELESS SERVICE PROVIDER B
ENDSYSTEM A
ENDSYSTEM B

FIG. 13

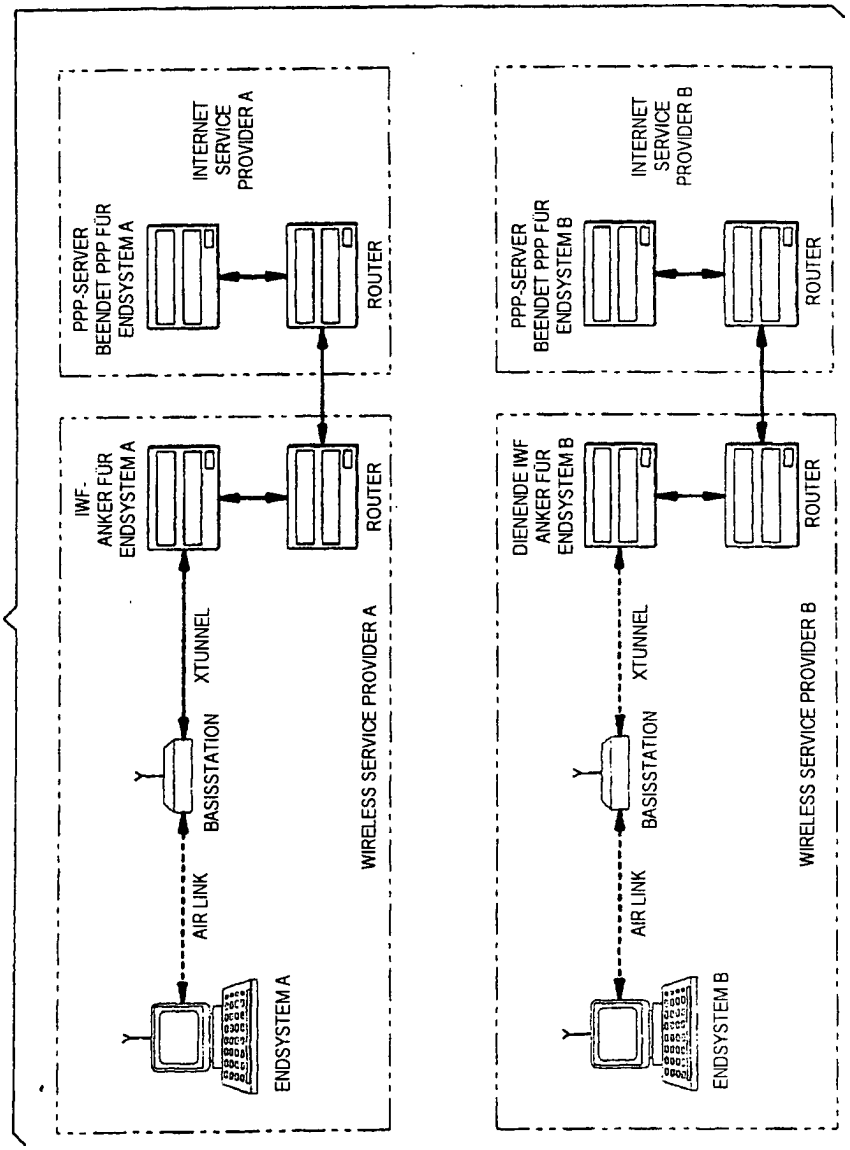

WIRELESS SERVICE PROVIDER A
WIRELESS SERVICE PROVIDER B
ENDSYSTEM A
ENDSYSTEM B
AIR LINK
BASISSTATION
XTUNNEL
IWF-ANKER FÜR ENDSYSTEM A
DIENENDE IWF ANKER FÜR ENDSYSTEM B
ROUTER
PPP-SERVER BEENDET PPP FÜR ENDSYSTEM A
PPP-SERVER BEENDET PPP FÜR ENDSYSTEM B
INTERNET SERVICE PROVIDER A
INTERNET SERVICE PROVIDER B

FIG. 14

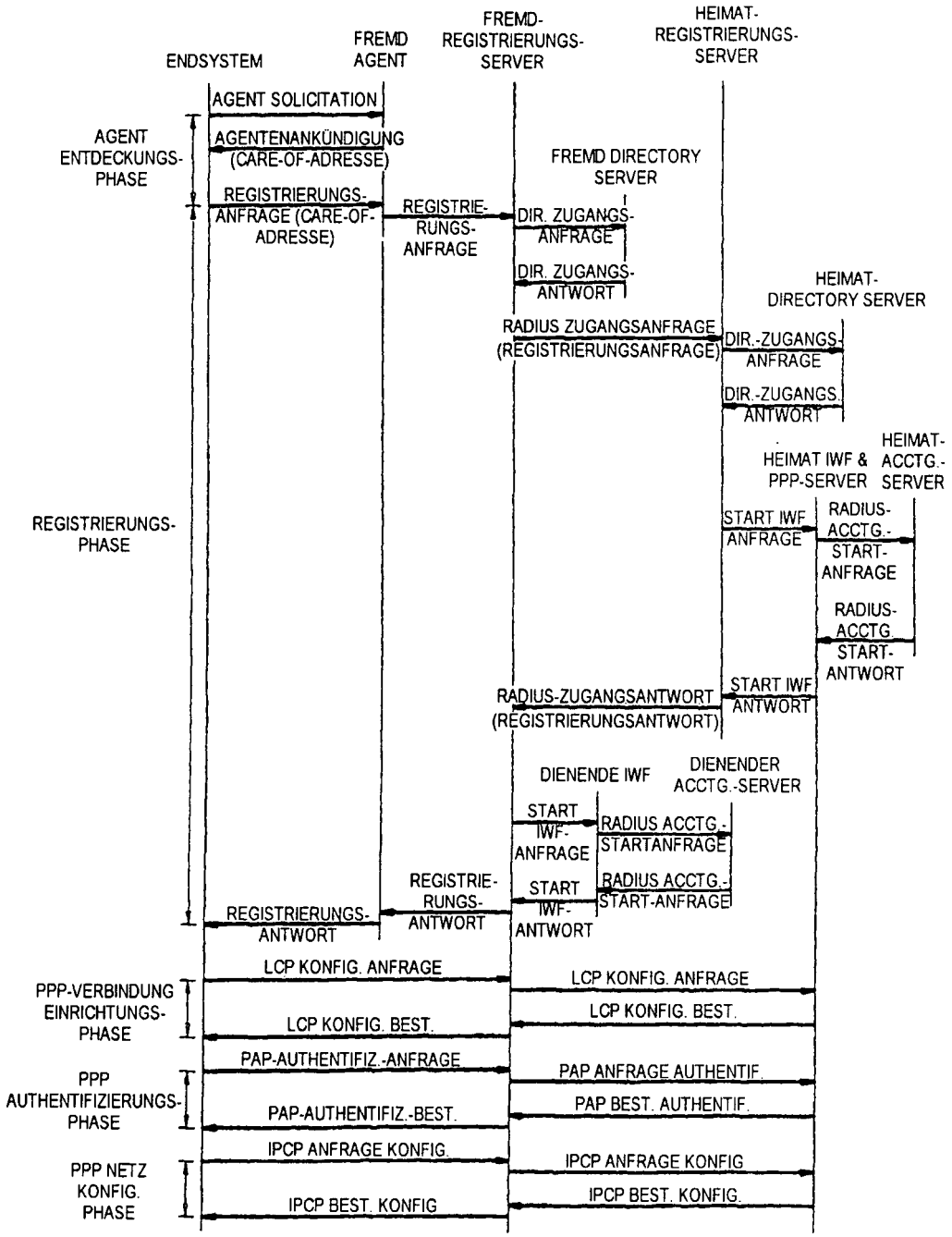

ENDSYSTEM
FREMD AGENT
FREMD-REGISTRIERUNGS-SERVER
HEIMAT-REGISTRIERUNGS-SERVER
AGENT ENTDECKUNGS-PHASE
AGENT SOLICITATION
AGENTENANKÜNDIGUNG (CARE-OF-ADRESSE)
FREMD DIRECTORY SERVER
REGISTRIERUNGS-ANFRAGE (CARE-OF-ADRESSE)
REGISTRIE-RUNGS-ANFRAGE
DIR. ZUGANGS-ANFRAGE
DIR. ZUGANGS-ANTWORT
HEIMAT-DIRECTORY SERVER
RADIUS ZUGANGSANFRAGE (REGISTRIERUNGSANFRAGE)
DIR.-ZUGANGS-ANFRAGE
DIR.-ZUGANGS-ANTWORT
HEIMAT IWF & PPP-SERVER
HEIMAT-ACCTG.-SERVER
REGISTRIERUNGS-PHASE
START IWF ANFRAGE
RADIUS-ACCTG.-START-ANFRAGE
RADIUS-ACCTG START-ANTWORT
RADIUS-ZUGANGSANTWORT (REGISTRIERUNGSANTWORT)
START IWF ANTWORT
DIENENDE IWF
DIENENDER ACCTG.-SERVER
START IWF-ANFRAGE
RADIUS ACCTG.-STARTANFRAGE
REGISTRIE-RUNGS-ANTWORT
START IWF-ANTWORT
RADIUS ACCTG.-START-ANFRAGE
REGISTRIERUNGS-ANTWORT
PPP-VERBINDUNG EINRICHTUNGS-PHASE
LCP KONFIG. ANFRAGE
LCP KONFIG. ANFRAGE
LCP KONFIG. BEST.
LCP KONFIG. BEST.
PPP AUTHENTIFIZIERUNGS-PHASE
PAP-AUTHENTIFIZ.-ANFRAGE
PAP ANFRAGE AUTHENTIF.
PAP-AUTHENTIFIZ.-BEST.
PAP BEST. AUTHENTIF.
PPP NETZ KONFIG. PHASE
IPCP ANFRAGE KONFIG.
IPCP ANFRAGE KONFIG
IPCP BEST. KONFIG
IPCP BEST. KONFIG.

FIG. 15

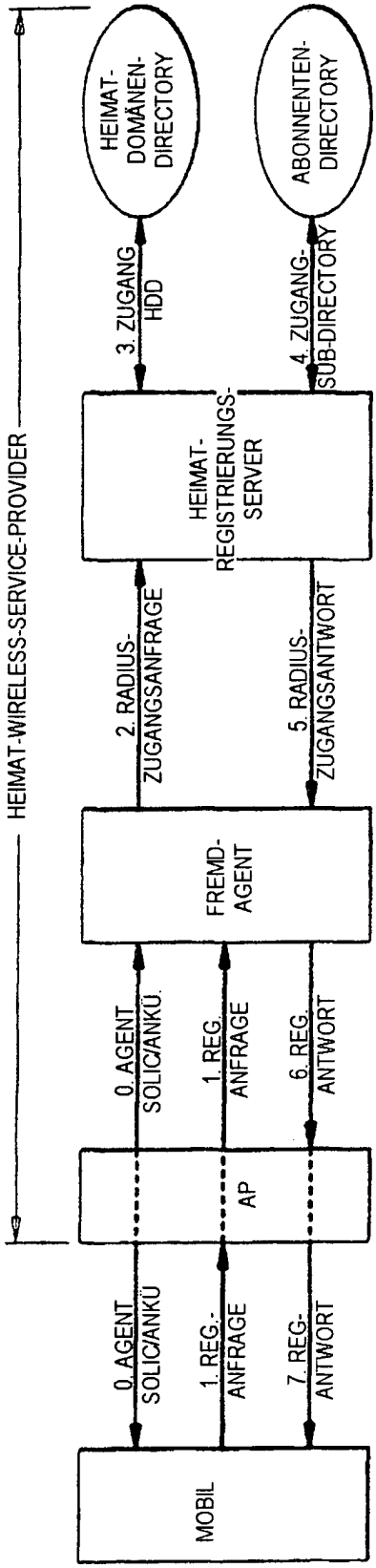
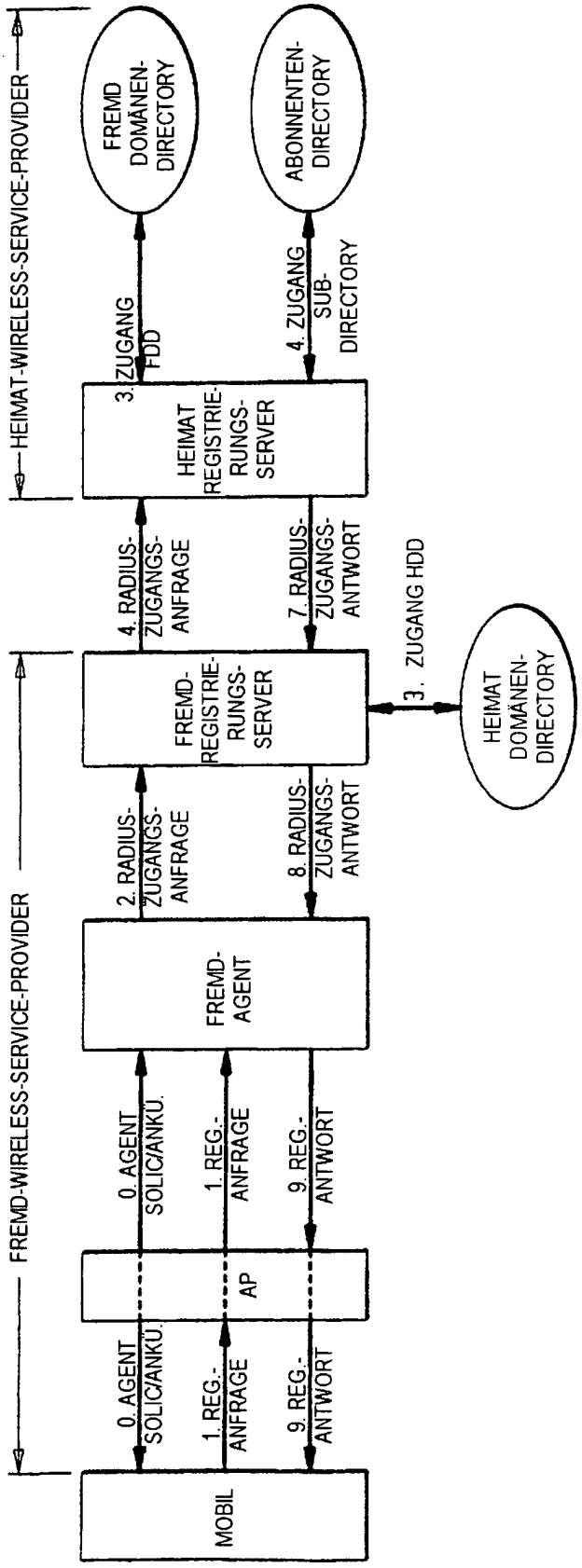

HEIMAT-WIRELESS-SERVICE-PROVIDER
HEIMAT-DOMÄNEN-DIRECTORY
ABONNENTEN-DIRECTORY
3. ZUGANG HDD
4. ZUGANG-SUB-DIRECTORY
HEIMAT-REGISTRIERUNGS-SERVER
2. RADIUS-ZUGANGSANFRAGE
5. RADIUS-ZUGANGSANTWORT
FREMD-AGENT
0. AGENT SOLIC/ANKÜ.
1. REG. ANFRAGE
6. REG. ANTWORT
AP
0. AGENT SOLIC/ANKÜ
1. REG.-ANFRAGE
7. REG.-ANTWORT
MOBIL

FIG. 16


HEIMAT-WIRELESS-SERVICE-PROVIDER
FREMD-WIRELESS-SERVICE-PROVIDER
FREMD DOMÄNEN-DIRECTORY
ABONNENTEN-DIRECTORY
HEIMAT REGISTRIE-RUNGS-SERVER
FREMD-REGISTRIE-RUNGS-SERVER
FREMD-AGENT
AP
MOBIL
3. ZUGANG HDD
4. ZUGANG SUB-DIRECTORY
4. RADIUS-ZUGANGS-ANFRAGE
7. RADIUS-ZUGANGS-ANTWORT
2. RADIUS-ZUGANGS-ANFRAGE
8. RADIUS-ZUGANGS-ANTWORT
0. AGENT SOLIC/ANKÜ.
1. REG.-ANFRAGE
9. REG.-ANTWORT
HEIMAT DOMÄNEN-DIRECTORY

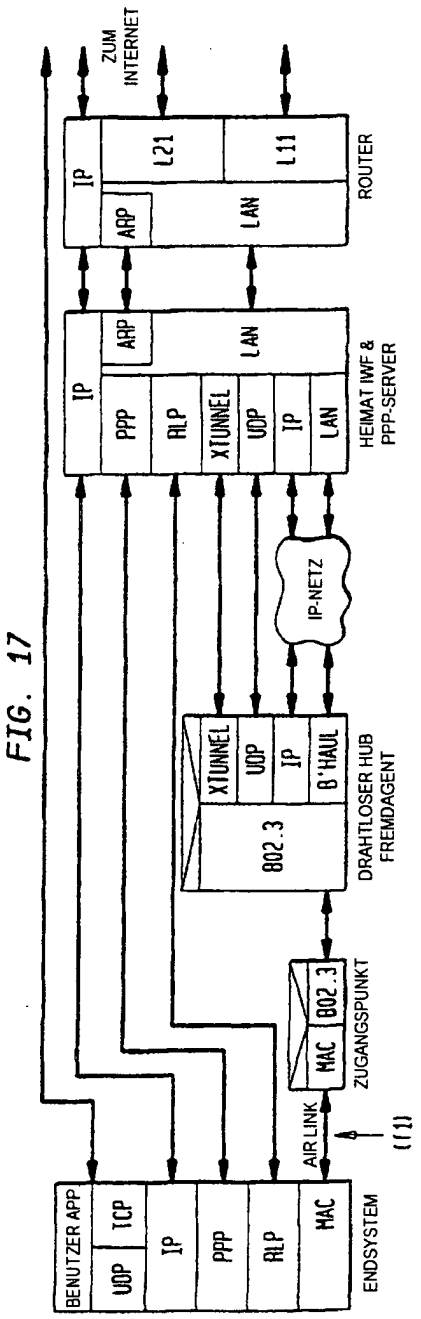

ZUM INTERNET
IP
ARP
L21
L11
LAN
ROUTER
IP
ARP
LAN
PPP
RLP
XTUNNEL
UDP
IP
LAN
HEIMAT IWF & PPP-SERVER
IP-NETZ
XTUNNEL
UDP
IP
B'HAUL
802.3
DRAHTLOSER HUB FREMDAGENT
MAC
802.3
ZUGANGSPUNKT
AIR LINK
(11)
BENUTZER APP
UDP
TCP
IP
PPP
RLP
MAC
ENDSYSTEM

FIG. 17

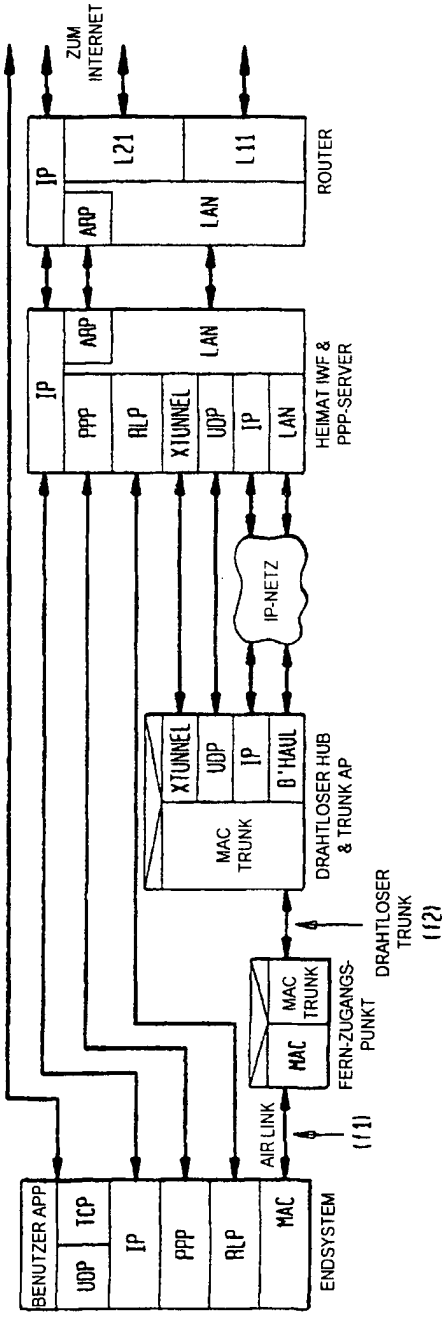

ZUM INTERNET
IP
ARP
L21
L11
LAN
ROUTER
IP
ARP
LAN
PPP
RLP
XTUNNEL
UDP
IP
LAN
HEIMAT IWF & PPP-SERVER
IP-NETZ
XTUNNEL
UDP
IP
B'HAUL
MAC TRUNK
DRAHTLOSER HUB & TRUNK AP
MAC
TRUNK
MAC
FERN-ZUGANGS-PUNKT
DRAHTLOSER TRUNK
(12)
AIR LINK
(11)
BENUTZER APP
UDP
TCP
IP
PPP
RLP
MAC
ENDSYSTEM

FIG. 18

FIG. 19

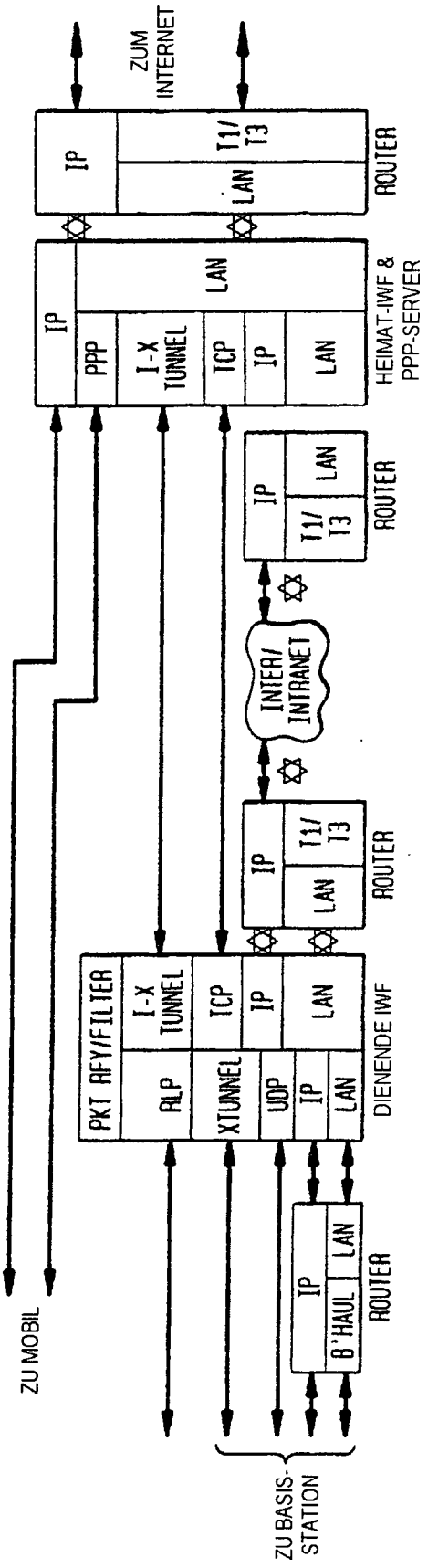

ZUM INTERNET
IP
T1/ T3
LAN
ROUTER
IP
LAN
PPP
I-X TUNNEL
TCP
IP
LAN
HEIMAT-IWF & PPP-SERVER
IP
LAN
T1/ T3
ROUTER
INTER/ INTRANET
IP
T1/ T3
LAN
ROUTER
PKT AFY/FILTER
I-X TUNNEL
TCP
IP
LAN
RLP
XTUNNEL
UDP
IP
LAN
DIENENDE IWF
IP
LAN
B'HAUL
ROUTER
ZU MOBIL
ZU BASIS-STATION

FIG. 20

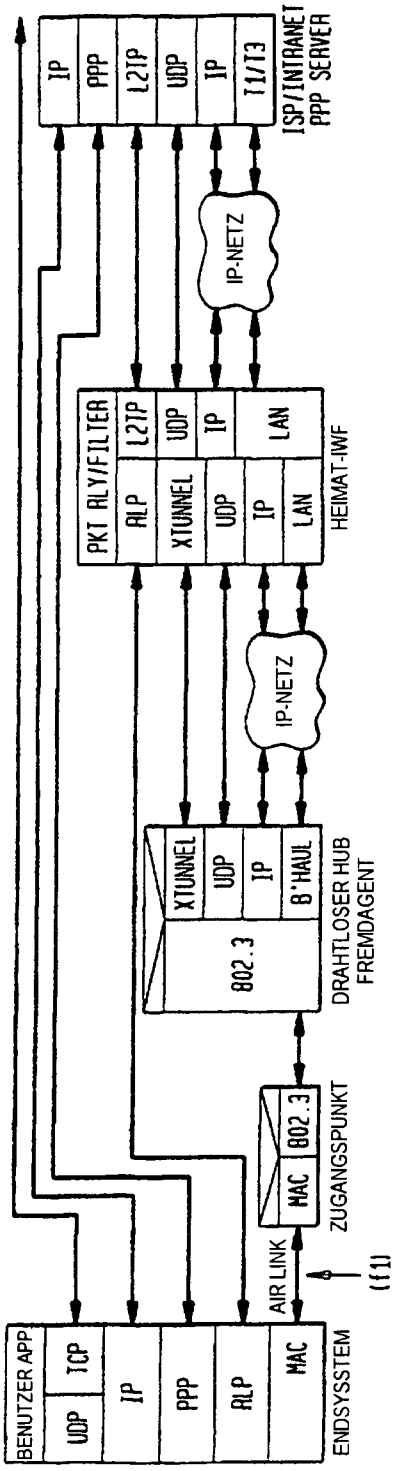
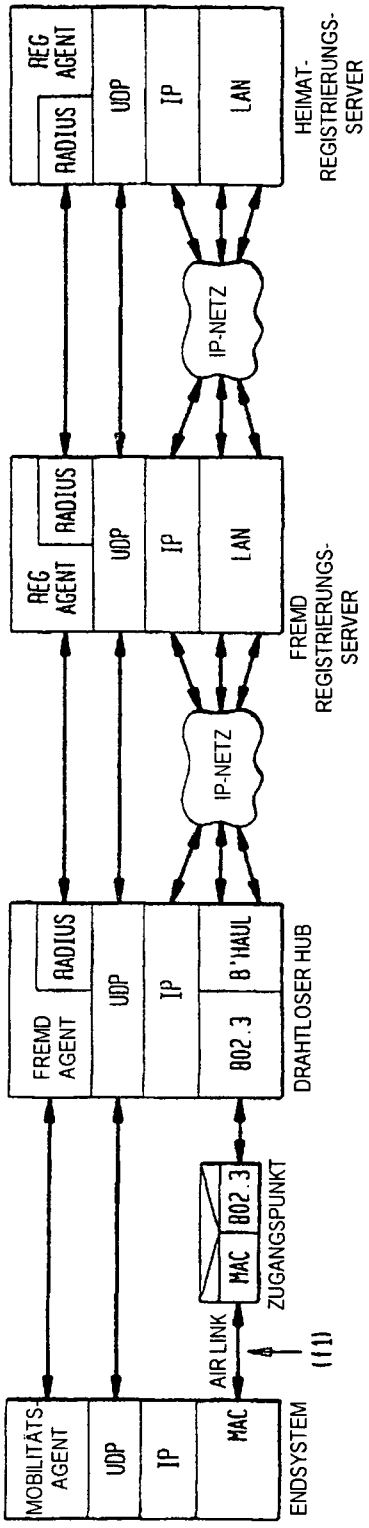

BENUTZER APP
UDP
TCP
IP
PPP
RLP
MAC
ENDSYSTEM
AIR LINK
(11)
MAC
802.3
ZUGANGSPUNKT
802.3
XTUNNEL
UDP
IP
B'HAUL
DRAHTLOSER HUB
FREMDAGENT
IP-NETZ
PKT RLY/FILTER
RLP
XTUNNEL
UDP
IP
LAN
L2TP
UDP
IP
LAN
HEIMAT-IWF
IP-NETZ
IP
PPP
L2TP
UDP
IP
T1/T3
ISP/INTRANET
PPP SERVER

FIG. 21


MOBILITÄTS-
AGENT
UDP
IP
MAC
ENDSYSTEM
AIR LINK
(11)
MAC
802.3
ZUGANGSPUNKT
FREMD
AGENT
RADIUS
UDP
IP
802.3
B'HAUL
DRAHTLOSER HUB
IP-NETZ
REG
AGENT
RADIUS
UDP
IP
LAN
FREMD
REGISTRIERUNGS-
SERVER
IP-NETZ
REG
AGENT
RADIUS
UDP
IP
LAN
HEIMAT-
REGISTRIERUNGS-
SERVER

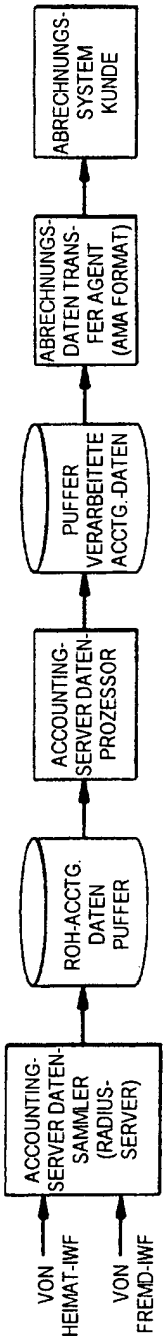
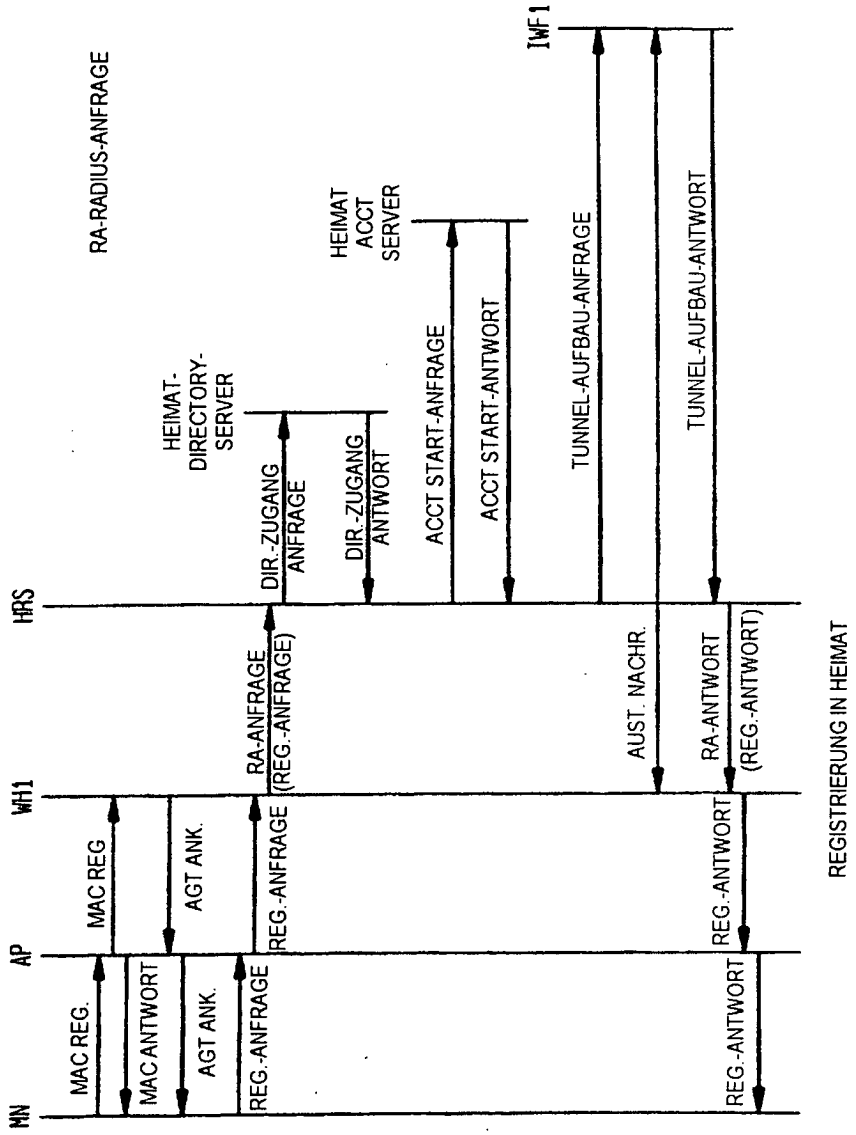

VON HEIMAT-IWF
VON FREMD-IWF
ACCOUNTING-SERVER DATEN-SAMMLER (RADIUS-SERVER)
ROH-ACCTG. DATEN PUFFER
ACCOUNTING-SERVER DATEN-PROZESSOR
PUFFER VERARBEITETE ACCTG.-DATEN
ABRECHNUNGS-DATEN TRANS-FER AGENT (AMA FORMAT)
ABRECHNUNGS-SYSTEM KUNDE

FIG. 22

FIG. 23


MN
AP
WH1
HRS
IWF1
MAC REG.
MAC ANTWORT
AGT ANK.
REG.-ANFRAGE
MAC REG
AGT ANK.
RA-ANFRAGE (REG.-ANFRAGE)
RA-RADIUS-ANFRAGE
HEIMAT-DIRECTORY-SERVER
DIR.-ZUGANG ANFRAGE
DIR.-ZUGANG ANTWORT
HEIMAT ACCT SERVER
ACCT START-ANFRAGE
ACCT START-ANTWORT
TUNNEL-AUFBAU-ANFRAGE
TUNNEL-AUFBAU-ANTWORT
AUST. NACHR.
RA-ANTWORT (REG.-ANTWORT)
REG.-ANTWORT
REG.-ANTWORT
REGISTRIERUNG IN HEIMAT

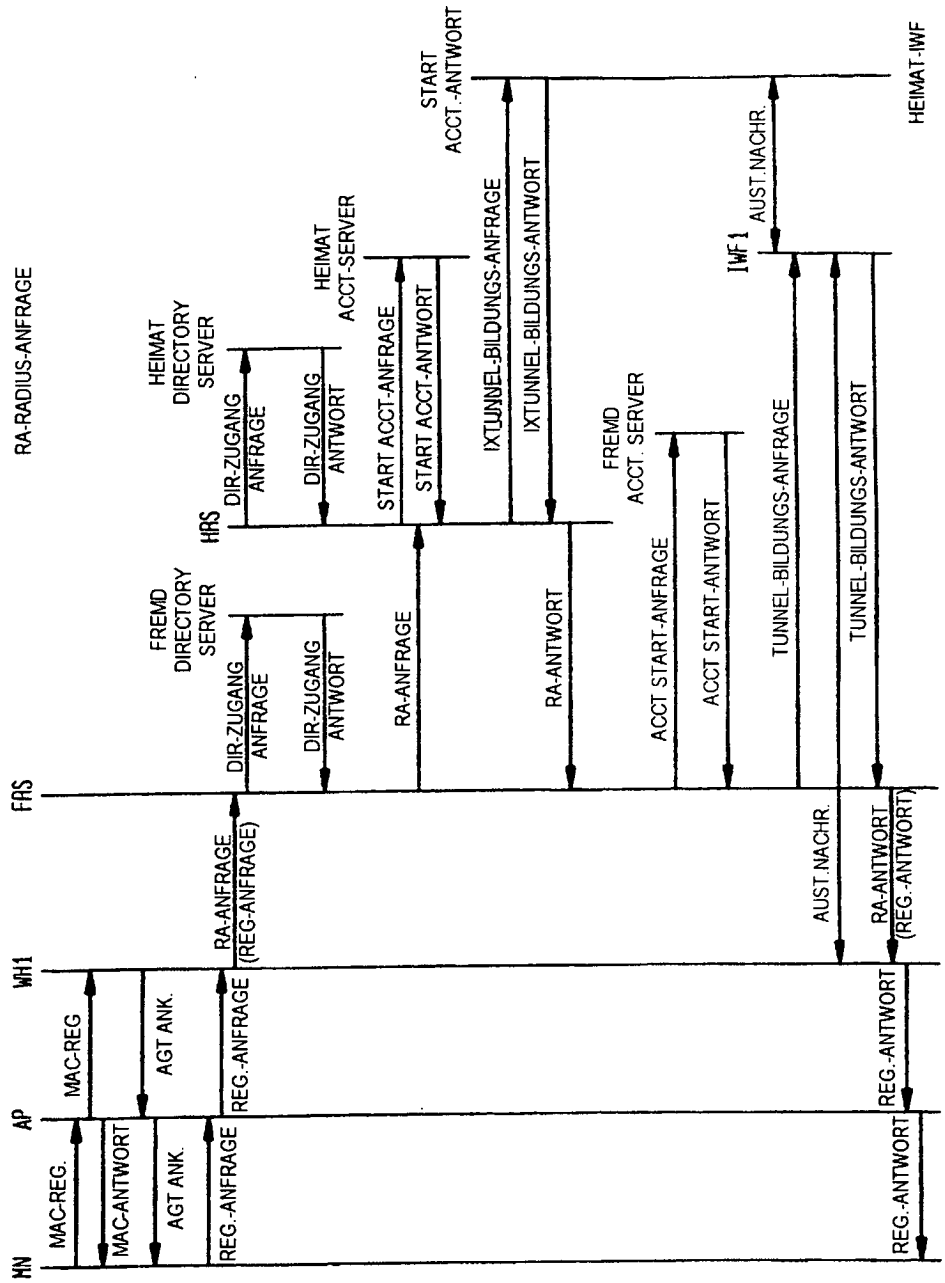

MN
AP
WH1
FRS
HRS
IWF1
HEIMAT-IWF
RA-RADIUS-ANFRAGE
MAC-REG.
MAC-ANTWORT
AGT ANK.
AGT ANK.
REG.-ANFRAGE
REG.-ANFRAGE
RA-ANFRAGE
(REG-ANFRAGE)
FREMD DIRECTORY SERVER
DIR-ZUGANG ANFRAGE
DIR-ZUGANG ANTWORT
HEIMAT DIRECTORY SERVER
DIR-ZUGANG ANFRAGE
DIR-ZUGANG ANTWORT
RA-ANFRAGE
RA-ANTWORT
HEIMAT ACCT-SERVER
START ACCT-ANFRAGE
START ACCT-ANTWORT
FREMD ACCT. SERVER
ACCT START-ANFRAGE
ACCT START-ANTWORT
START ACCT.-ANTWORT
IXTUNNEL-BILDUNGS-ANFRAGE
IXTUNNEL-BILDUNGS-ANTWORT
AUST.NACHR.
TUNNEL-BILDUNGS-ANFRAGE
AUST.NACHR.
TUNNEL-BILDUNGS-ANTWORT
AUST.NACHR.
RA-ANTWORT
(REG.-ANTWORT)
REG.-ANTWORT
REG.-ANTWORT

FIG. 24

FIG. 25

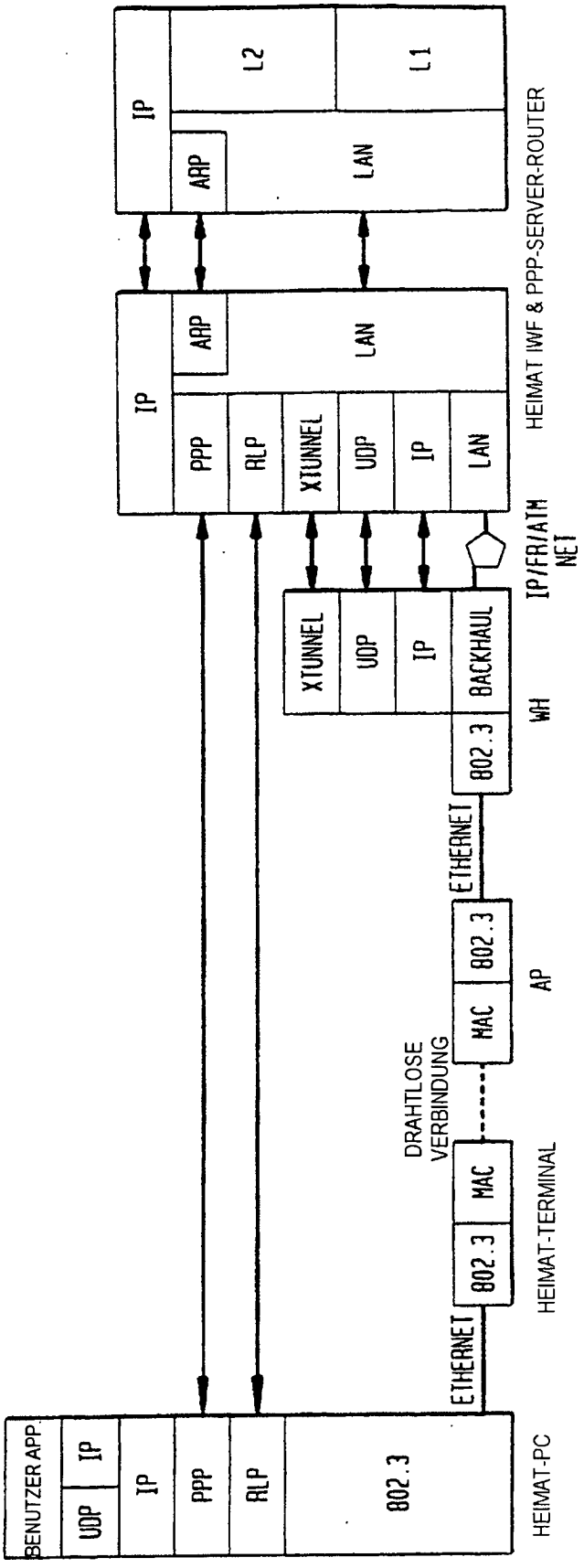

IP
L2
L1
ARP
LAN
HEIMAT IWF & PPP-SERVER-ROUTER
IP
ARP
LAN
PPP
RLP
XTUNNEL
UDP
IP
LAN
IP/FR/ATM NET
XTUNNEL
UDP
IP
BACKHAUL
802.3
WH
ETHERNET
802.3
MAC
AP
DRAHTLOSE VERBINDUNG
ETHERNET
802.3
MAC
HEIMAT-TERMINAL
BENUTZER APP
UDP
IP
IP
PPP
RLP
802.3
HEIMAT-PC

FIG. 26

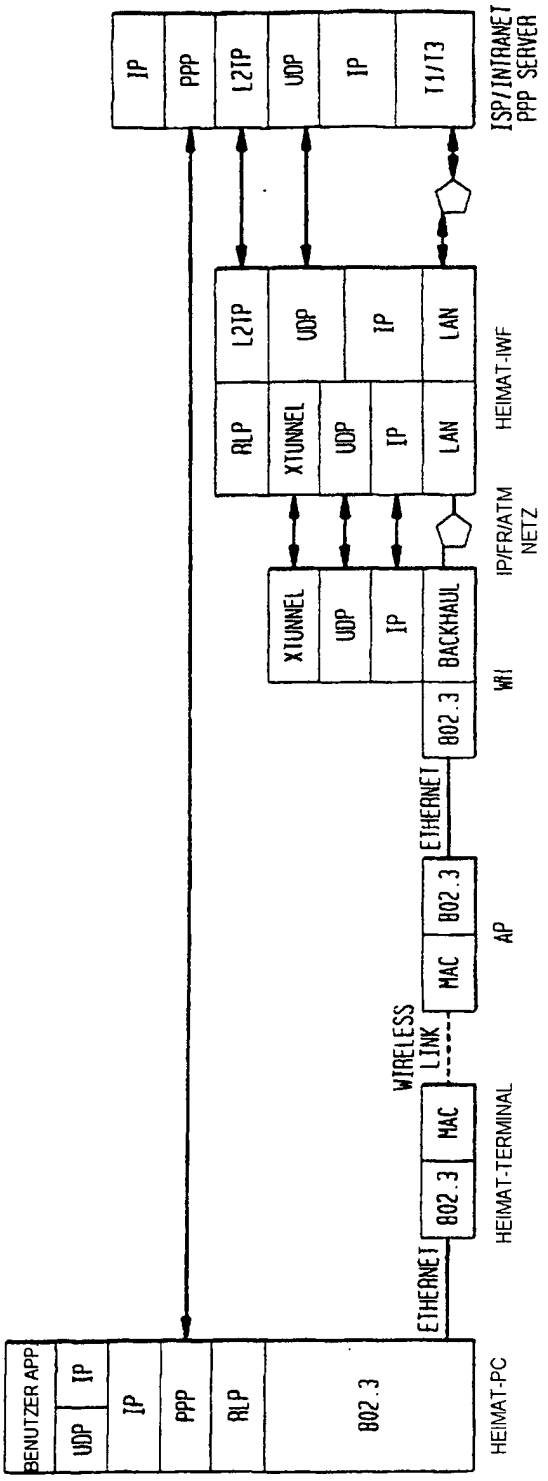

BENUTZER APP
UDP
IP
IP
PPP
RLP
802.3
HEIMAT-PC
ETHERNET
802.3
MAC
WIRELESS LINK
MAC
802.3
HEIMAT-TERMINAL
ETHERNET
802.3
BACKHAUL
AP
WLI
XTUNNEL
UDP
IP
LAN
RLP
XTUNNEL
UDP
IP
LAN
HEIMAT-IWF
L2TP
UDP
IP
LAN
IP/FR/ATM NETZ
IP
PPP
L2TP
UDP
IP
T1/T3
ISP/INTRANET PPP SERVER

FIG. 27

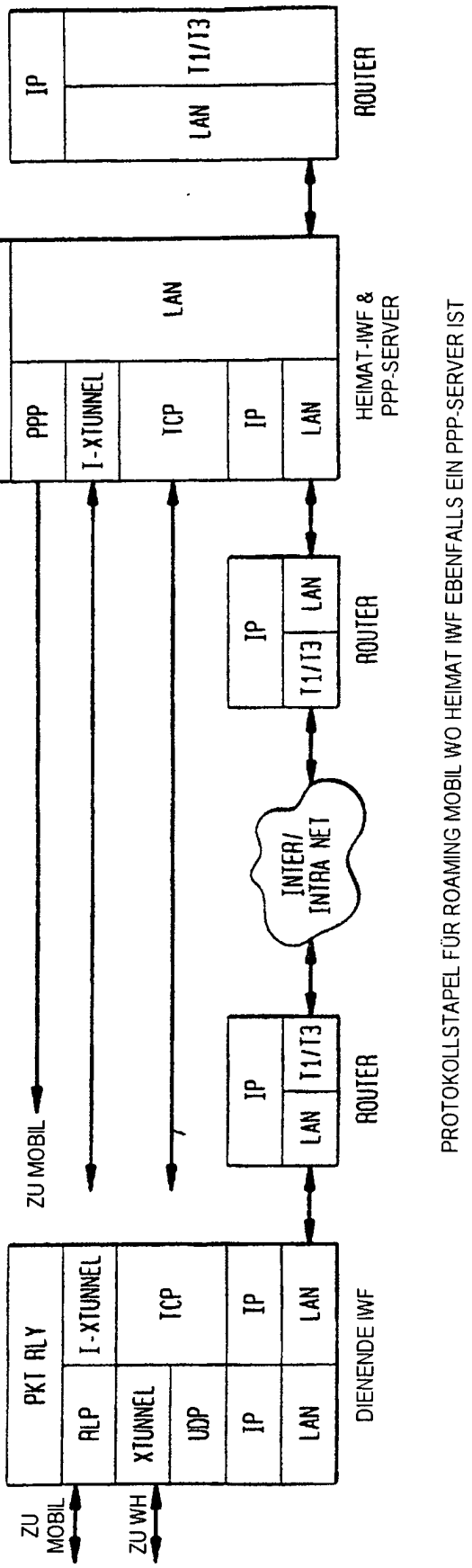
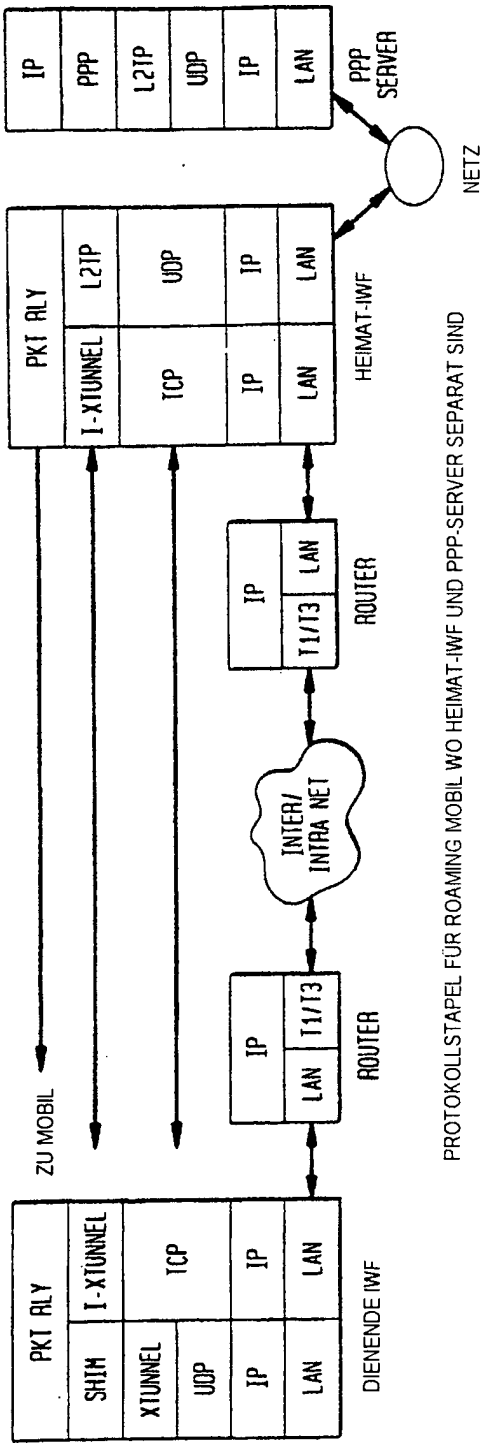

ZU MOBIL
ZU WH
PKT RLY
RLP
I-XTUNNEL
XTUNNEL
UDP
TCP
IP
LAN
DIENENDE IWF
ROUTER
INTER/
INTRA NET
ROUTER
PPP
HEIMAT-IWF &
PPP-SERVER
ROUTER
T1/T3
PROTOKOLLSTAPEL FÜR ROAMING MOBIL WO HEIMAT IWF EBENFALLS EIN PPP-SERVER IST

FIG. 28



PROTOKOLLSTAPEL FÜR ROAMING MOBIL WO HEIMAT-IWF UND PPP-SERVER SEPARAT SIND

FIG. 29

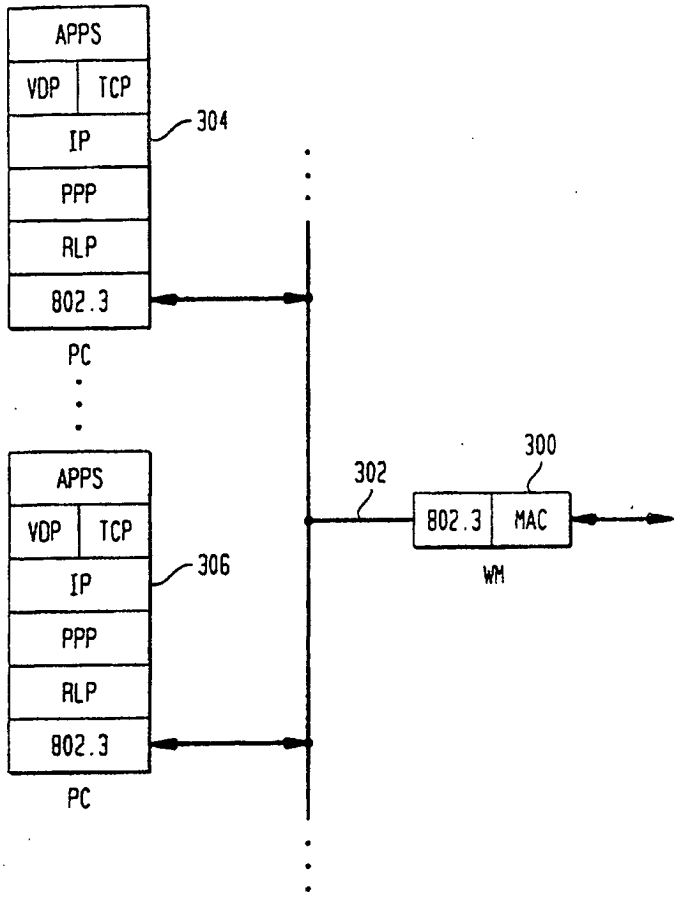

APPS
VDP
TCP
IP
PPP
RLP
802.3
304
PC
APPS
VDP
TCP
IP
PPP
RLP
802.3
306
PC
302
300
802.3
MAC
WM

FIG. 30

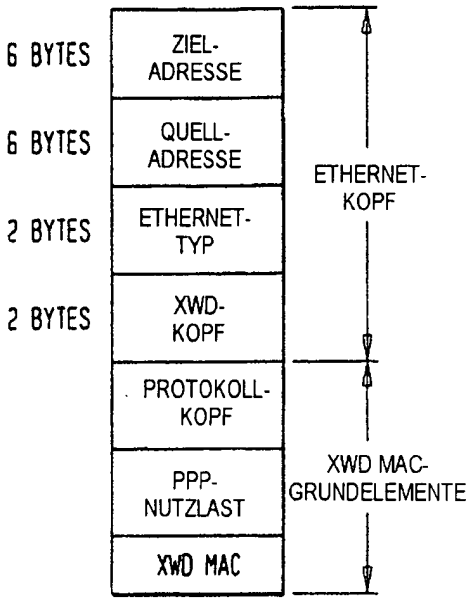

6 BYTES
ZIEL-ADRESSE
6 BYTES
QUELL-ADRESSE
2 BYTES
ETHERNET-TYP
2 BYTES
XWD-KOPF
ETHERNET-KOPF
PROTOKOLL-KOPF
PPP-NUTZLAST
XWD MAC
XWD MAC-GRUNDELEMENTE

FIG. 31

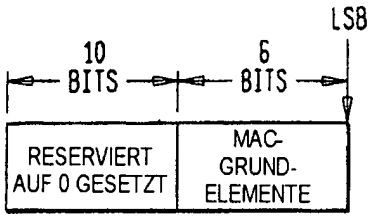

LSB
10 BITS
6 BITS
RESERVIERT AUF 0 GESETZT
MAC-GRUND-ELEMENTE

FIG. 32

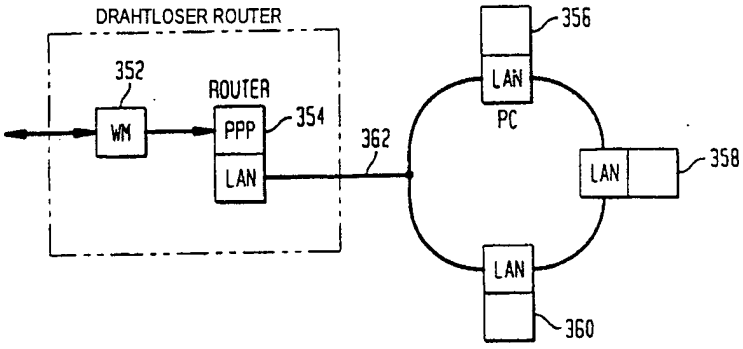
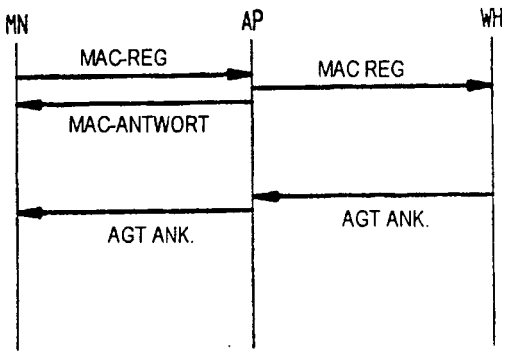

DRAHTLOSER ROUTER
352
WM
ROUTER
PPP
354
LAN
362
356
LAN
PC
LAN
358
LAN
360

FIG. 33



LOKALES HANDOFF

FIG. 34

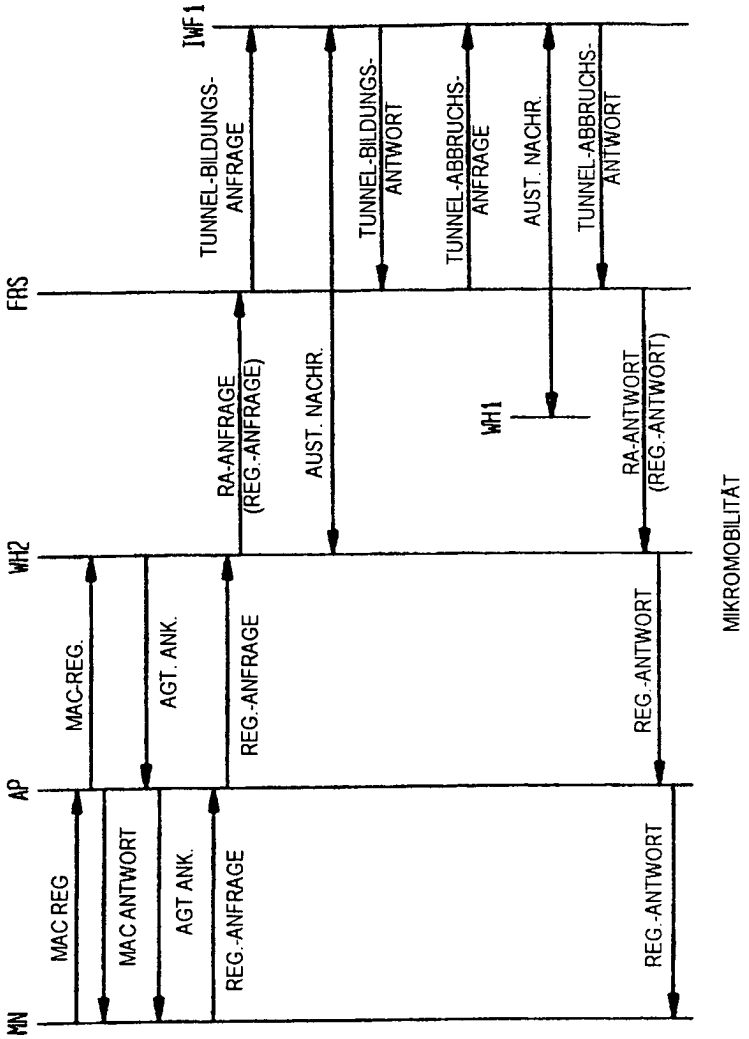

MN
AP
WH2
FRS
IWF1
MAC REG
MAC ANTWORT
AGT ANK.
REG.-ANFRAGE
MAC-REG.
AGT. ANK.
REG.-ANFRAGE
RA-ANFRAGE (REG.-ANFRAGE)
AUST. NACHR.
TUNNEL-BILDUNGS-ANFRAGE
TUNNEL-BILDUNGS-ANTWORT
TUNNEL-ABBRUCHS-ANFRAGE
AUST. NACHR.
TUNNEL-ABBRUCHS-ANTWORT
WH1
RA-ANTWORT (REG.-ANTWORT)
REG.-ANTWORT
REG.-ANTWORT
MIKROMOBILITÄT

FIG. 35

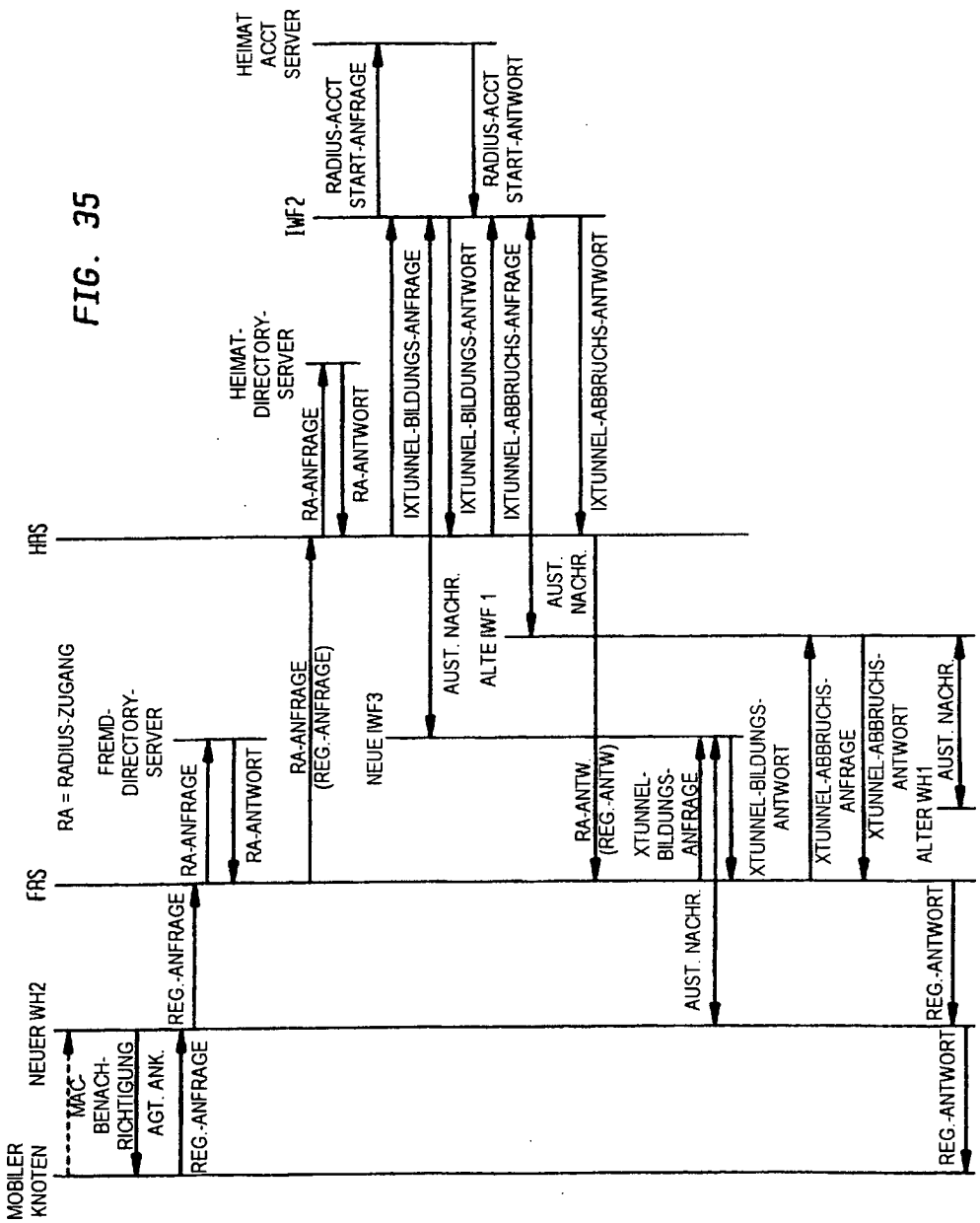

MOBILER KNOTEN
NEUER WH2
FRS
RA = RADIUS-ZUGANG
HRS
HEIMAT ACCT SERVER
HEIMAT-DIRECTORY-SERVER
IWF2
FREMD-DIRECTORY-SERVER
MAC-BENACH-RICHTIGUNG
AGT. ANK.
REG.-ANFRAGE
RA-ANFRAGE
RA-ANTWORT
RA-ANFRAGE (REG.ANFRAGE)
RA-ANTW. (REG.-ANTW)
NEUE IWF3
ALTE IWF 1
AUST. NACHR.
IXTUNNEL-BILDUNGS-ANFRAGE
IXTUNNEL-BILDUNGS-ANTWORT
IXTUNNEL-ABBRUCHS-ANFRAGE
IXTUNNEL-ABBRUCHS-ANTWORT
RADIUS-ACCT START-ANFRAGE
RADIUS-ACCT START-ANTWORT
XTUNNEL-BILDUNGS-ANFRAGE
XTUNNEL-BILDUNGS-ANTWORT
XTUNNEL-ABBRUCHS-ANFRAGE
XTUNNEL-ABBRUCHS-ANTWORT
ALTER WH1
AUST. NACHR.
REG.-ANTWORT

FIG. 36

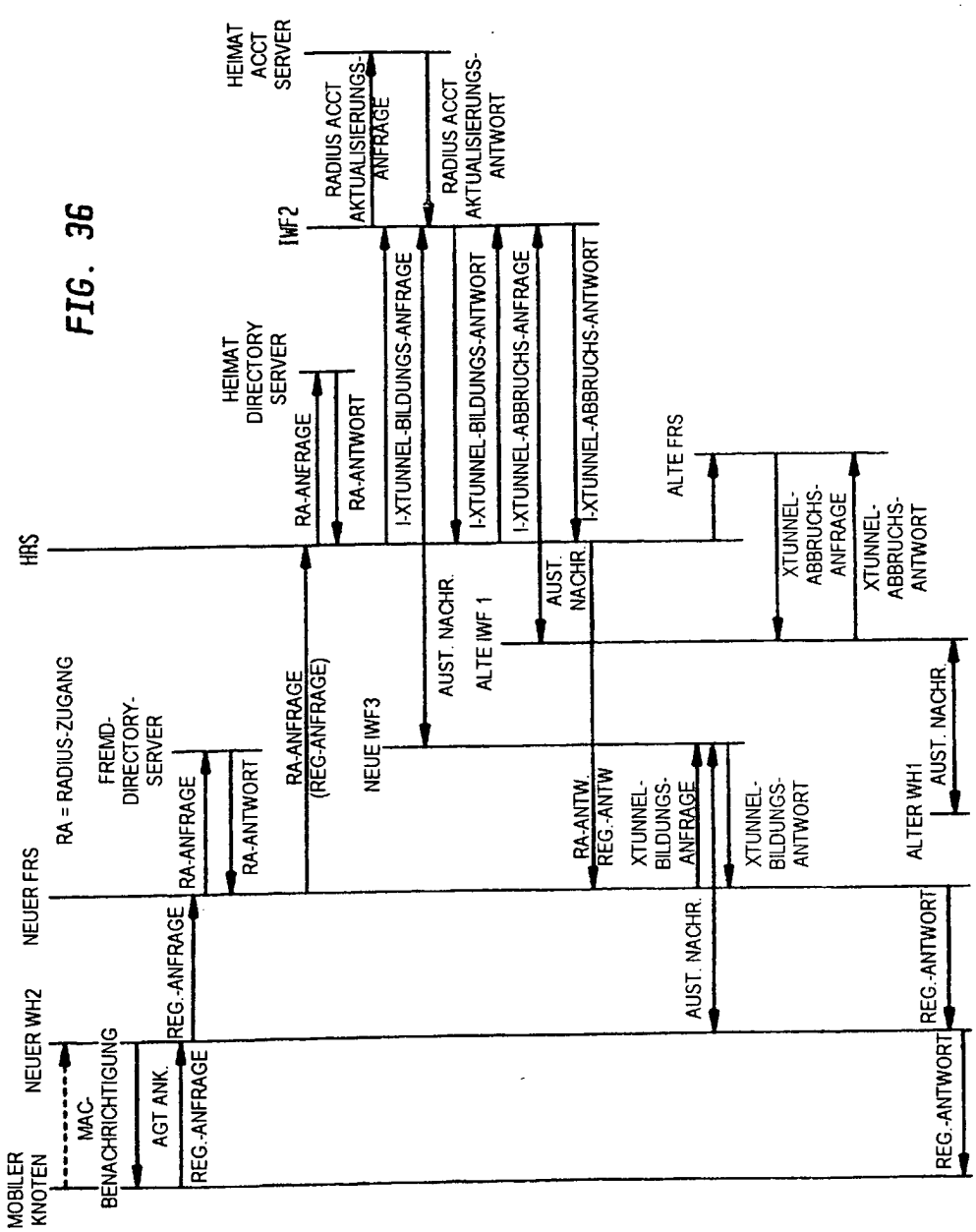
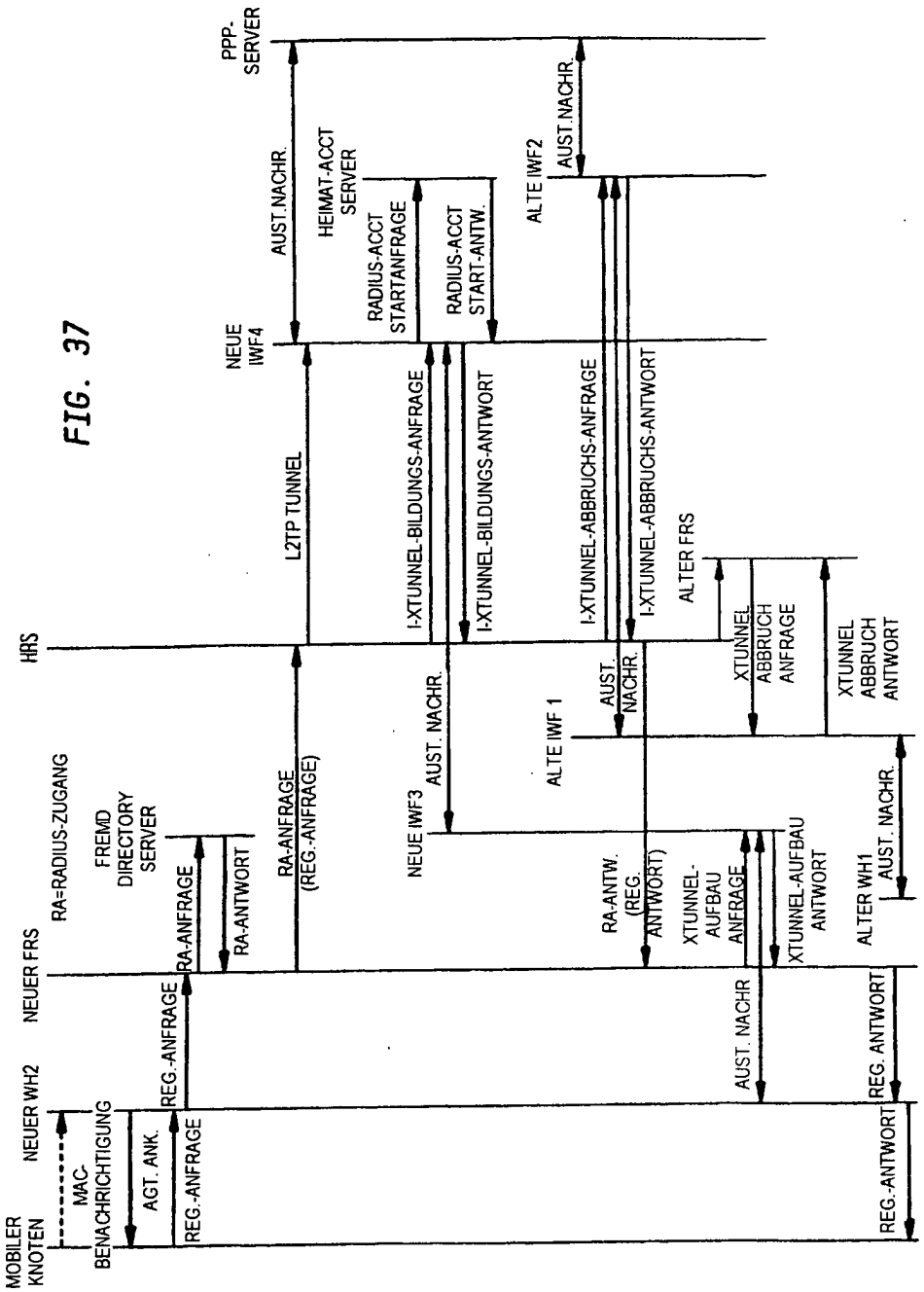

MOBILER KNOTEN
NEUER WH2
NEUER FRS
HRS
HEIMAT ACCT SERVER
IWF2
HEIMAT DIRECTORY SERVER
FREMD-DIRECTORY-SERVER
RA = RADIUS-ZUGANG
MAC-BENACHRICHTIGUNG
AGT ANK.
REG.-ANFRAGE
RA-ANFRAGE
RA-ANTWORT
RA-ANFRAGE (REG-ANFRAGE)
RADIUS ACCT AKTUALISIERUNGS-ANFRAGE
RADIUS ACCT AKTUALISIERUNGS-ANTWORT
I-XTUNNEL-BILDUNGS-ANFRAGE
I-XTUNNEL-BILDUNGS-ANTWORT
I-XTUNNEL-ABBRUCHS-ANFRAGE
I-XTUNNEL-ABBRUCHS-ANTWORT
NEUE IWF3
ALTE IWF 1
AUST. NACHR.
ALTE FRS
XTUNNEL-ABBRUCHS-ANFRAGE
XTUNNEL-ABBRUCHS-ANTWORT
RA-ANTW.
REG.-ANTW
XTUNNEL-BILDUNGS-ANFRAGE
XTUNNEL-BILDUNGS-ANTWORT
ALTER WH1
AUST. NACHR.
REG.-ANTWORT
REG.-ANTWORT

FIG. 37


MOBILER KNOTEN
NEUER WH2
NEUER FRS
HRS
RA=RADIUS-ZUGANG
FREMD DIRECTORY SERVER
NEUE IWF4
PPP-SERVER
MAC-BENACHRICHTIGUNG
AGT. ANK.
REG.-ANFRAGE
RA-ANFRAGE
RA-ANTWORT
RA-ANFRAGE (REG.-ANFRAGE)
L2TP TUNNEL
AUST.NACHR.
HEIMAT-ACCT SERVER
RADIUS-ACCT STARTANFRAGE
RADIUS-ACCT START-ANTW.
ALTE IWF2
AUST.NACHR.
I-XTUNNEL-BILDUNGS-ANFRAGE
I-XTUNNEL-BILDUNGS-ANTWORT
I-XTUNNEL-ABBRUCHS-ANFRAGE
I-XTUNNEL-ABBRUCHS-ANTWORT
ALTER FRS
NEUE IWF3
AUST. NACHR.
ALTE IWF 1
AUST. NACHR.
XTUNNEL ABBRUCH ANFRAGE
XTUNNEL ABBRUCH ANTWORT
RA-ANTW. (REG. ANTWORT)
XTUNNEL-AUFBAU ANFRAGE
XTUNNEL-AUFBAU ANTWORT
ALTER WH1
AUST. NACHR.
AUST. NACHR
REG. ANTWORT
REG.-ANTWORT