[Anlage NK19 -- *Übersetzung*]

US 20020075844A1

(19) **USA**

(12) **Patentanmeldungsveröffentlichung**

Hagen

(10) **Veröffentlichungsnr.: US 2002/0075844 A1**

(43) **Veröffentlichungsdatum: 20. Juni 2002**

(54) **INTEGRATION ÖFFENTLICHER UND PRIVATER NETZWERKRESSOURCEN FÜR DEN OPTIMIERTEN DRAHTLOSEN BREITBANDZUGANG UND VERFAHREN**

(76) Erfinder: **W. Alexander Hagen**, Montara, Kalifornien (USA)

Korrespondenzadresse:
TOWNSEND AND TOWNSEND AND CREW,
LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (USA)

(21) Anmeldenr.: **09/832,679**
(22) Anmeldedatum: **10. April 2001**

Zugehörige US-Anmeldedokumente

(63) Nicht-vorläufige Anmeldung der vorläufigen Anmeldung Nr. 60/256,158, eingereicht am 15. Dezember 2000.

Klassifikation der Veröffentlichung

(51) **Int. Kl.**[7] **H04L 12/28**
(52) **U.S. Kl.** **370/351**; 370/328

(57) **ZUSAMMENFASSUNG**

Es wird ein System und Verfahren offengelegt für die Bereitstellung eines allgegenwärtigen öffentlichen Netzwerkzugangs zu drahtlosen, mobilen Terminals unter Inanspruchnahme privater Netzwerke mit privaten Netzwerkzugangspunkten und Verbindungen mit dem öffentlichen Netzwerk. Die drahtlosen, mobilen Terminals können drahtlose Funkfrequenz-Kommunikationsgeräte verwenden, die private Netzwerkzugangspunkte umfassen. Ein Netzwerk-Zugangs-Server („Network Access Server", NAS) ist jedem drahtlosen Funkfrequenz-Kommunikationsgerät zugeordnet und stellt eine Schnittstelle zwischen den drahtlosen, mobilen Terminals und dem privaten Netzwerk bereit. Der NAS steuert die Registrierung der drahtlosen, mobilen Terminals als Teilnehmer und stellt einen öffentlichen Netzwerkzugang zu den mobilen Terminals über den Zugangspunkt des privaten Netzwerks und die öffentliche Netzwerkverbindung bereit. Der NAS beschränkt außerdem den Zugang durch die mobilen Terminals zum privaten Netzwerk, misst die Nutzung des Netzwerks durch die mobilen Terminals und steuert die Nutzung der Bandbreite durch die mobilen Terminals. Der NAS hat außerdem eine Schnittstelle mit verteilten Diensten des Integrationsbetreibers über das öffentliche Netzwerk. Die Dienste des Integrationsbetreibers beinhalten Datenbanken und Server zum Speichern und Bereitstellen von Teilnehmer- und Netzwerkanbieter-informationen für die Registrierung der Teilnehmer, für Netzwerkzugangs- und Netzwerknutzungskontrolle sowie zu Abrechnungszwecken. Der NAS kann als eigen-ständiges Element bereitgestellt werden, das in einem Rechner eingebaut ist, oder er kann in dem drahtlosen Funkfrequenzgerät und/oder einem Netzwerkadaptergerät für das private Netzwerk integriert sein.

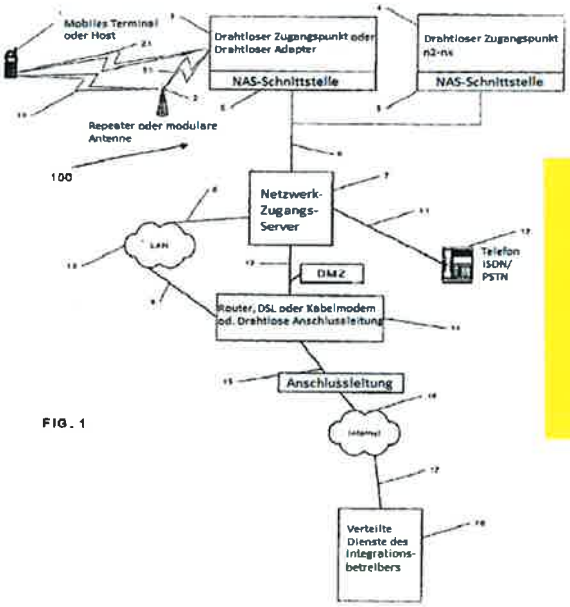

FIG. 1

Anlage NK19a

Zoltán Pál ./. Apple GmbH

Aktenzeichen: X ZR 100/13

BARDEHLE PAGENBERG
Unser Zeichen: A123365NI

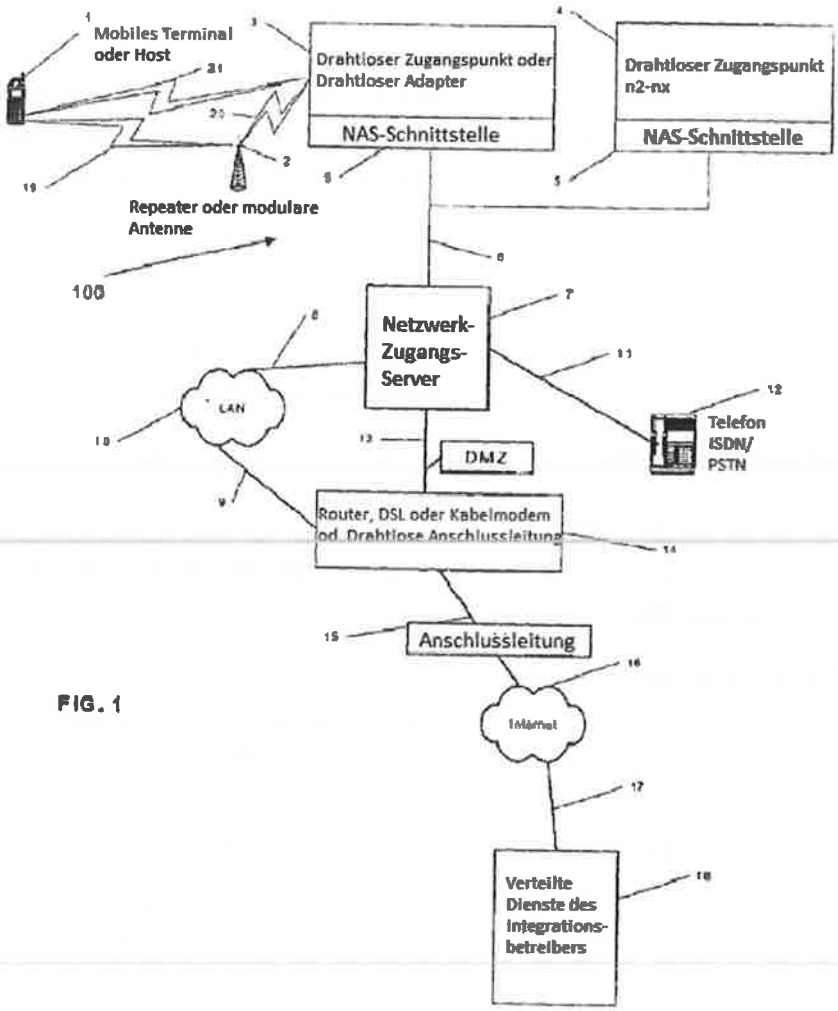
Mobiles Terminal oder Host
Drahtloser Zugangspunkt oder Drahtloser Adapter
NAS-Schnittstelle
Drahtloser Zugangspunkt n2-nx
NAS-Schnittstelle
Repeater oder modulare Antenne
100
Netzwerk-Zugangs-Server
LAN
DMZ
Telefon ISDN/ PSTN
Router, DSL oder Kabelmodem od. Drahtlose Anschlussleitung
Anschlussleitung
Verteilte Dienste des Integrations-betreibers

FIG. 1

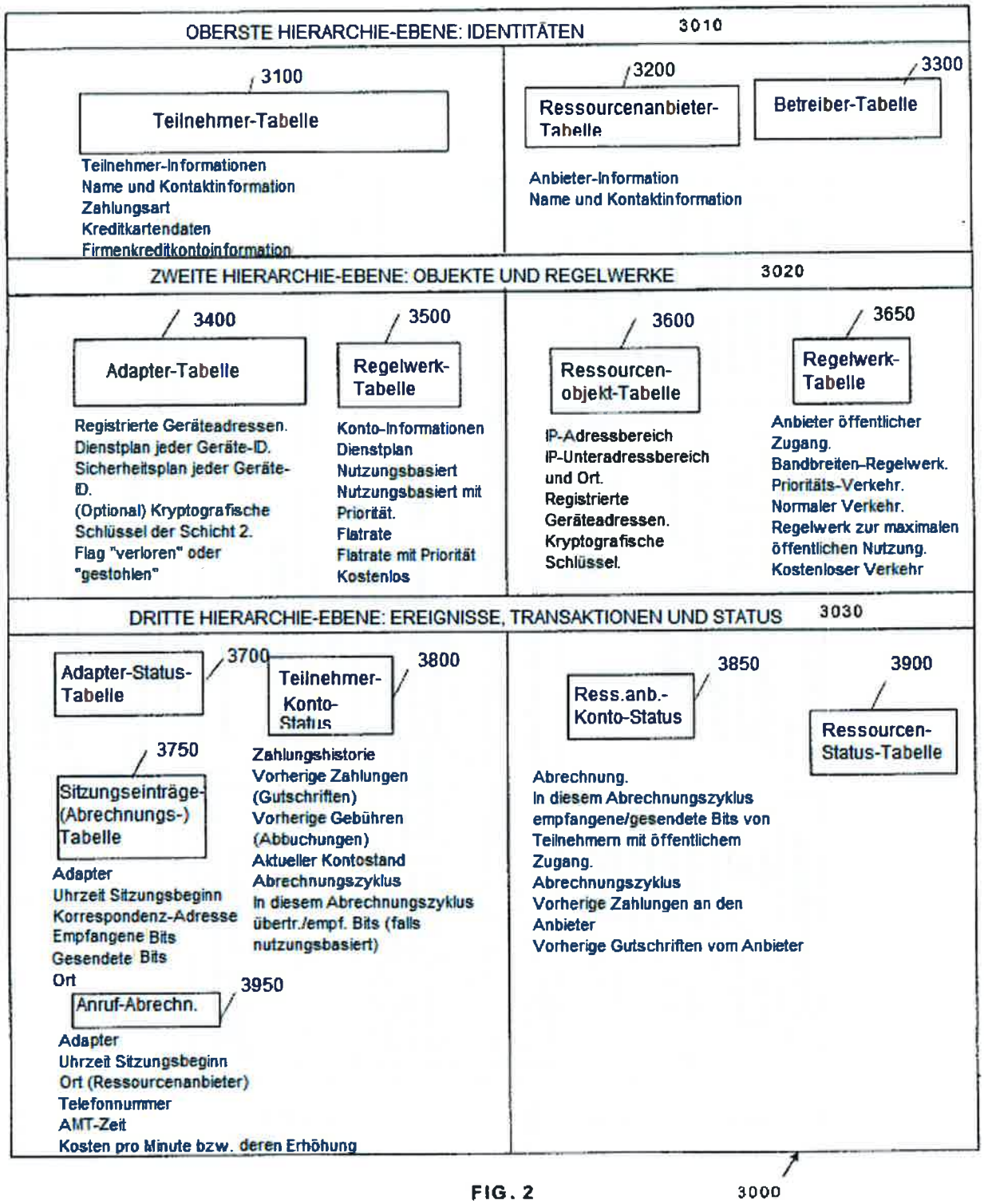
OBERSTE HIERARCHIE-EBENE: IDENTITÄTEN
3010
3100
Teilnehmer-Tabelle
Teilnehmer-Informationen
Name und Kontaktinformation
Zahlungsart
Kreditkartendaten
Firmenkreditkontoinformation
3200
Ressourcenanbieter-Tabelle
Anbieter-Information
Name und Kontaktinformation
3300
Betreiber-Tabelle
ZWEITE HIERARCHIE-EBENE: OBJEKTE UND REGELWERKE
3020
3400
Adapter-Tabelle
Registrierte Geräteadressen.
Dienstplan jeder Geräte-ID.
Sicherheitsplan jeder Geräte-ID.
(Optional) Kryptografische Schlüssel der Schicht 2.
Flag "verloren" oder "gestohlen"
3500
Regelwerk-Tabelle
Konto-Informationen
Dienstplan
Nutzungsbasiert
Nutzungsbasiert mit Priorität.
Flatrate
Flatrate mit Priorität
Kostenlos
3600
Ressourcen-objekt-Tabelle
IP-Adressbereich
IP-Unteradressbereich und Ort.
Registrierte Geräteadressen.
Kryptografische Schlüssel.
3650
Regelwerk-Tabelle
Anbieter öffentlicher Zugang.
Bandbreiten-Regelwerk.
Prioritäts-Verkehr.
Normaler Verkehr.
Regelwerk zur maximalen öffentlichen Nutzung.
Kostenloser Verkehr
DRITTE HIERARCHIE-EBENE: EREIGNISSE, TRANSAKTIONEN UND STATUS
3030
Adapter-Status-Tabelle
3700
Teilnehmer-Konto-Status
3800
Zahlungshistorie
Vorherige Zahlungen (Gutschriften)
Vorherige Gebühren (Abbuchungen)
Aktueller Kontostand
Abrechnungszyklus
In diesem Abrechnungszyklus übertr./empf. Bits (falls nutzungsbasiert)
3750
Sitzungseinträge-(Abrechnungs-) Tabelle
Adapter
Uhrzeit Sitzungsbeginn
Korrespondenz-Adresse
Empfangene Bits
Gesendete Bits
Ort
Anruf-Abrechn.
3950
Adapter
Uhrzeit Sitzungsbeginn
Ort (Ressourcenanbieter)
Telefonnummer
AMT-Zeit
Kosten pro Minute bzw. deren Erhöhung
3850
Ress.anb.-Konto-Status
Abrechnung.
In diesem Abrechnungszyklus empfangene/gesendete Bits von Teilnehmern mit öffentlichem Zugang.
Abrechnungszyklus
Vorherige Zahlungen an den Anbieter
Vorherige Gutschriften vom Anbieter
3900
Ressourcen-Status-Tabelle
3000

FIG. 2

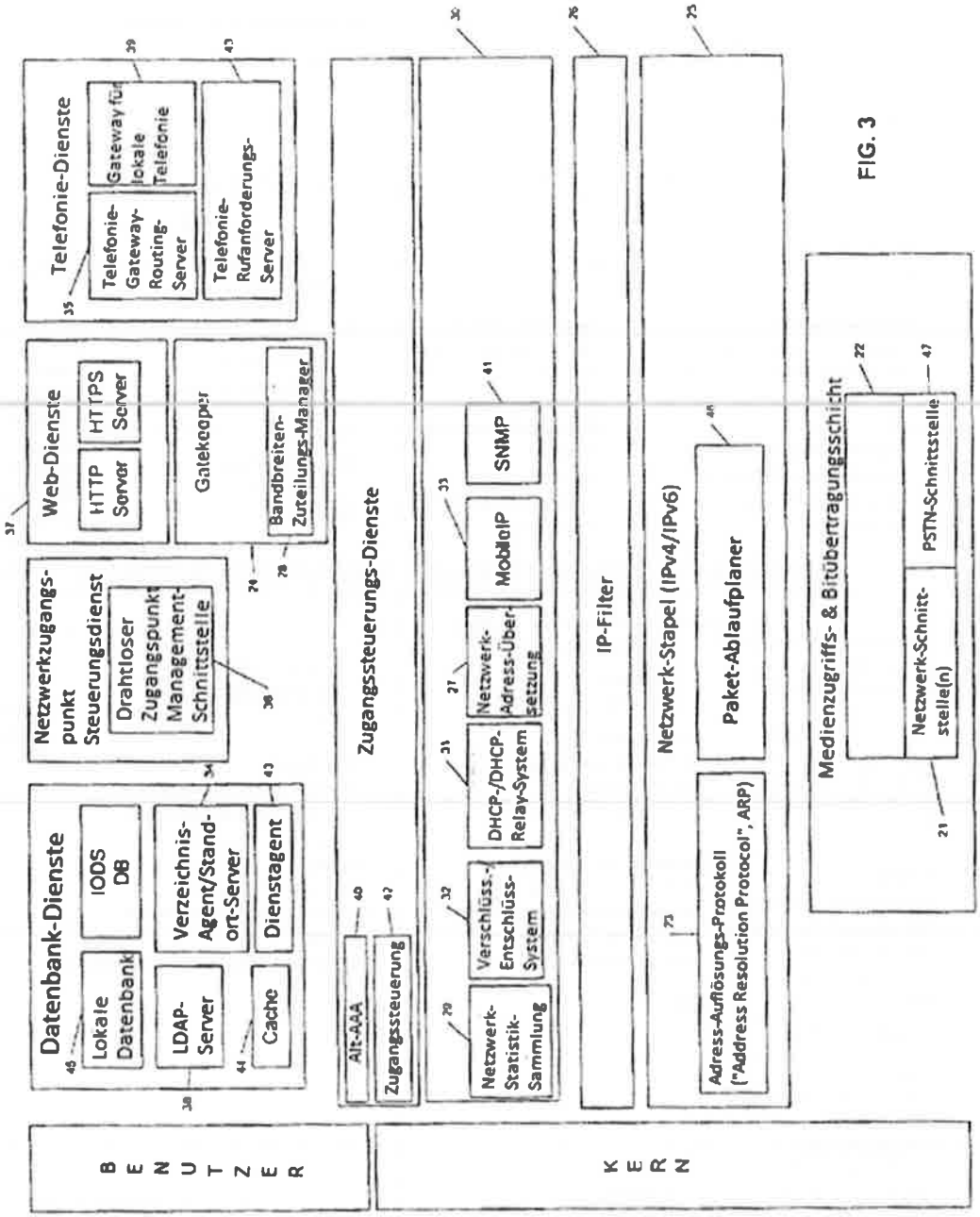
BENUTZER
KERN
Datenbank-Dienste
Lokale Datenbank
IODS DB
LDAP-Server
Verzeichnis-Agent/Standort-Server
Cache
Dienstagent
Netzwerkzugangspunkt Steuerungsdienst
Drahtloser Zugangspunkt Management-Schnittstelle
Web-Dienste
HTTP Server
HTTPS Server
Gatekeeper
Bandbreiten-Zuteilungs-Manager
Telefonie-Dienste
Telefonie-Gateway-Routing-Server
Gateway für lokale Telefonie
Telefonie-Rufanforderungs-Server
Zugangssteuerungs-Dienste
Alt-AAA
Zugangssteuerung
Netzwerk-Statistik-Sammlung
Verschlüss.-Entschlüss.-System
DHCP-/DHCP-Relay-System
Netzwerk-Adress-Übersetzung
MobileIP
SNMP
IP-Filter
Netzwerk-Stapel (IPv4/IPv6)
Adress-Auflösungs-Protokoll ("Address Resolution Protocol", ARP)
Paket-Ablaufplaner
Medienzugriffs- & Bitübertragungsschicht
Netzwerk-Schnittstelle(n)
PSTN-Schnittstelle

FIG. 3

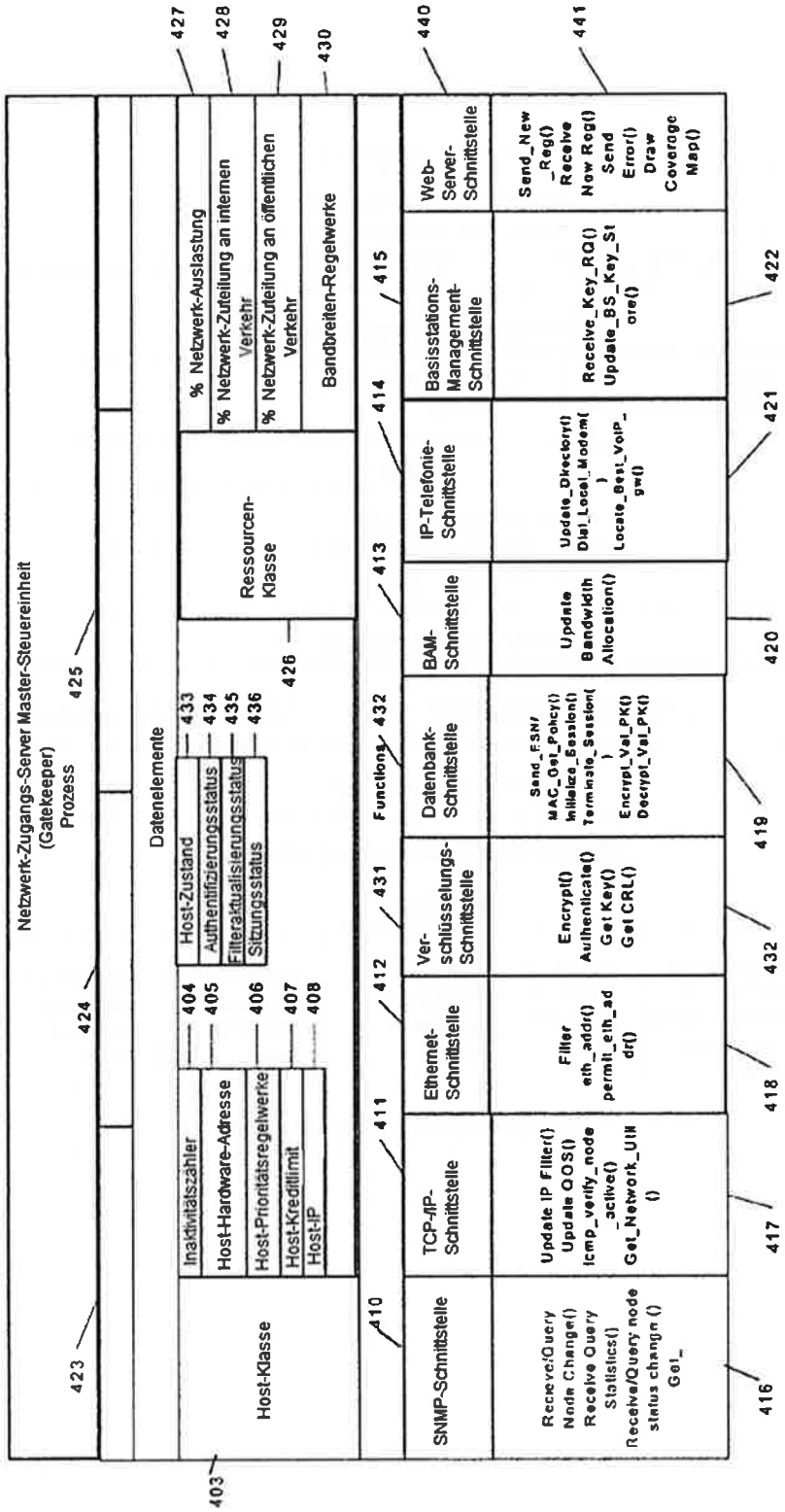
Netzwerk-Zugangs-Server Master-Steuereinheit (Gatekeeper) Prozess
423
424
425
Host-Klasse
403
Inaktivitätszähler
Host-Hardware-Adresse
Host-Prioritätsregelwerke
Host-Kreditlimit
Host-IP
404
405
406
407
408
Datenelemente
Host-Zustand
Authentifizierungsstatus
Filteraktualisierungsstatus
Sitzungsstatus
433
434
435
436
426
Ressourcen-Klasse
% Netzwerk-Auslastung
% Netzwerk-Zuteilung an internen Verkehr
% Netzwerk-Zuteilung an öffentlichen Verkehr
Bandbreiten-Regelwerke
427
428
429
430
410
411
412
431
Functions
432
413
414
415
440
441
SNMP-Schnittstelle
TCP-/IP-Schnittstelle
Ethernet-Schnittstelle
Ver-schlüsselungs-Schnittstelle
Datenbank-Schnittstelle
BAM-Schnittstelle
IP-Telefonie-Schnittstelle
Basisstations-Management-Schnittstelle
Web-Server-Schnittstelle
Receive/Query Node Change() Receive Query Statistics() Receive/Query node status change () Get_
Update IP Filter() Update QOS() Icmp_verify_node_active() Get_Network_UIM ()
Filter eth_addr() permit_eth_adr()
Encrypt() Authenticate() Get Key() Get CRL()
Send_FSN/ MAC_Get_Policy() Initialize_Session() Terminate_Session( ) Encrypt_Val_PK() Decrypt_Val_PK()
Update Bandwidth Allocation()
Update_Directory() Dial_Local_Modem( ) Locate_Best_VoIP_gw()
Receive_Key_RQ() Update_BS_Key_Store()
Send_New_Reg() Receive New Reg() Send Error() Draw Coverage Map()
416
417
418
419
420
421
422

FIG. 4

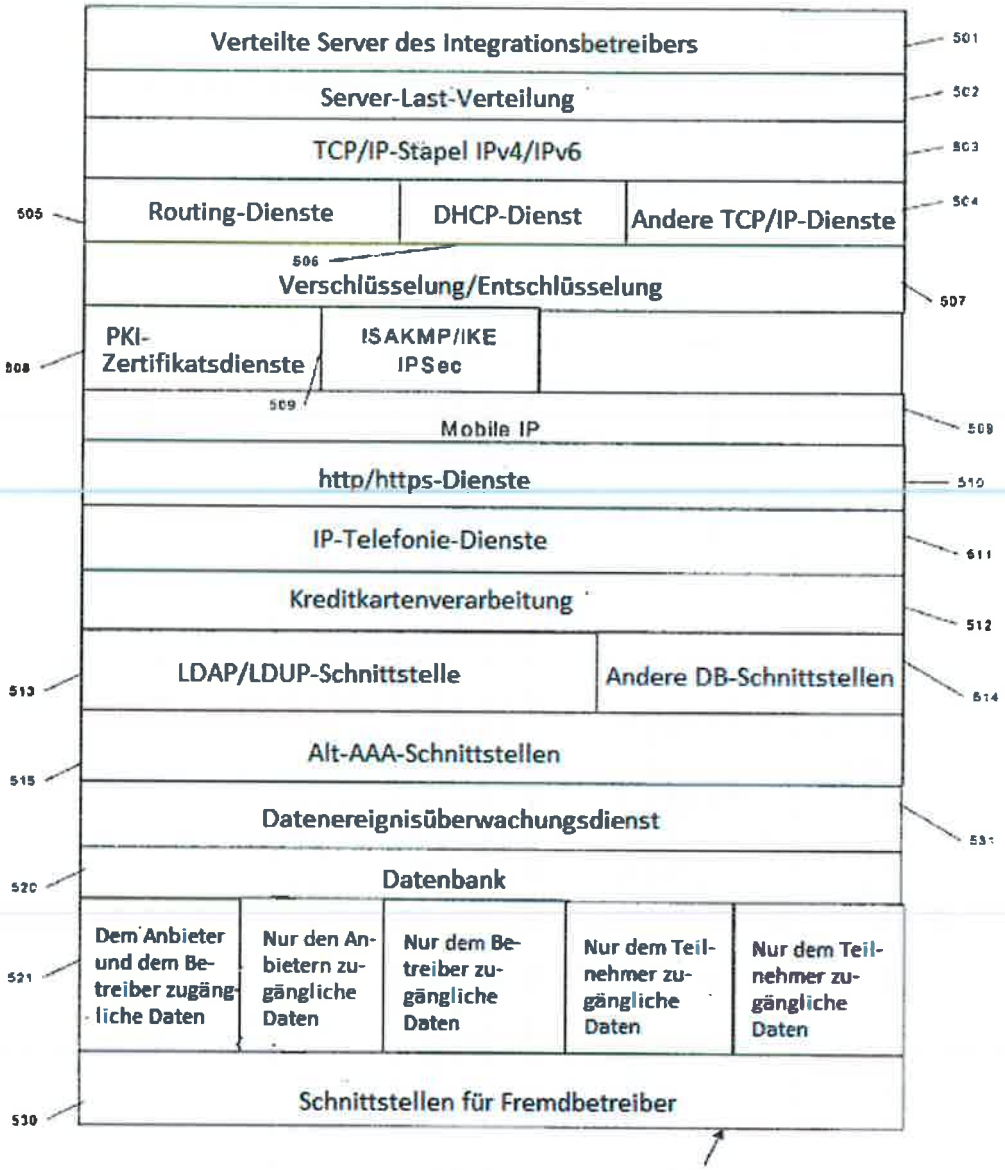
Verteilte Server des Integrationsbetreibers
501
Server-Last-Verteilung
502
TCP/IP-Stapel IPv4/IPv6
503
505
Routing-Dienste
DHCP-Dienst
Andere TCP/IP-Dienste
504
506
Verschlüsselung/Entschlüsselung
507
PKI-Zertifikatsdienste
ISAKMP/IKE IPSec
508
509
Mobile IP
509
http/https-Dienste
510
IP-Telefonie-Dienste
511
Kreditkartenverarbeitung
512
513
LDAP/LDUP-Schnittstelle
Andere DB-Schnittstellen
514
Alt-AAA-Schnittstellen
515
Datenereignisüberwachungsdienst
Datenbank
520
521
Dem Anbieter und dem Betreiber zugängliche Daten
Nur den Anbietern zugängliche Daten
Nur dem Betreiber zugängliche Daten
Nur dem Teilnehmer zugängliche Daten
Nur dem Teilnehmer zugängliche Daten
530
Schnittstellen für Fremdbetreiber
500

FIG. 5

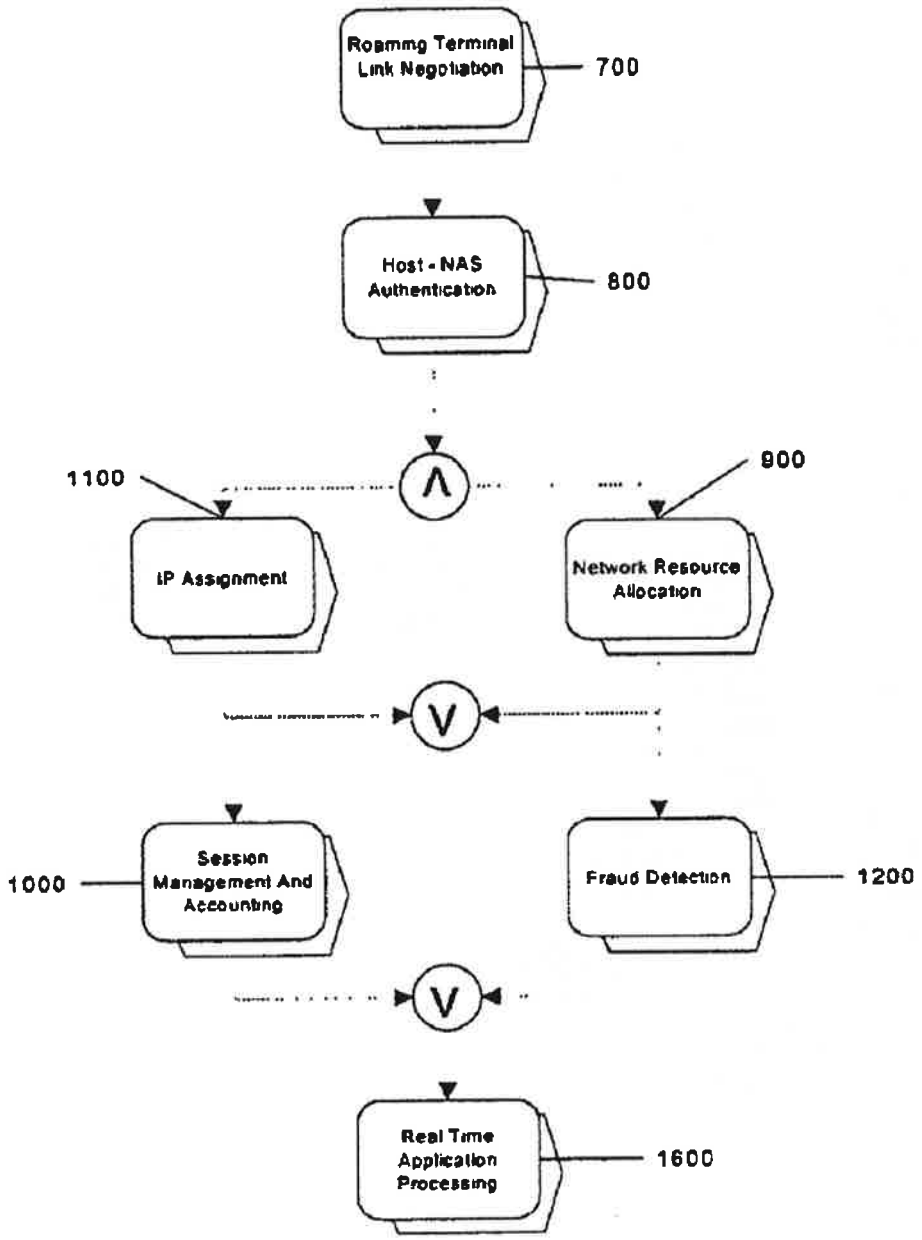

FIG. 6

Legende FIG. 6:

700: Aushandeln einer Verknüpfung für Roaming-Terminal
800: Host-NAS-Authentifizierung
900: Netzwerk-Ressourcen-Zuteilung
1000: Sitzungsmanagement und Abrechnung
1100: IP-Zuweisung
1200: Betrugserkennung
1600: Anwendungsverarbeitung in Echtzeit

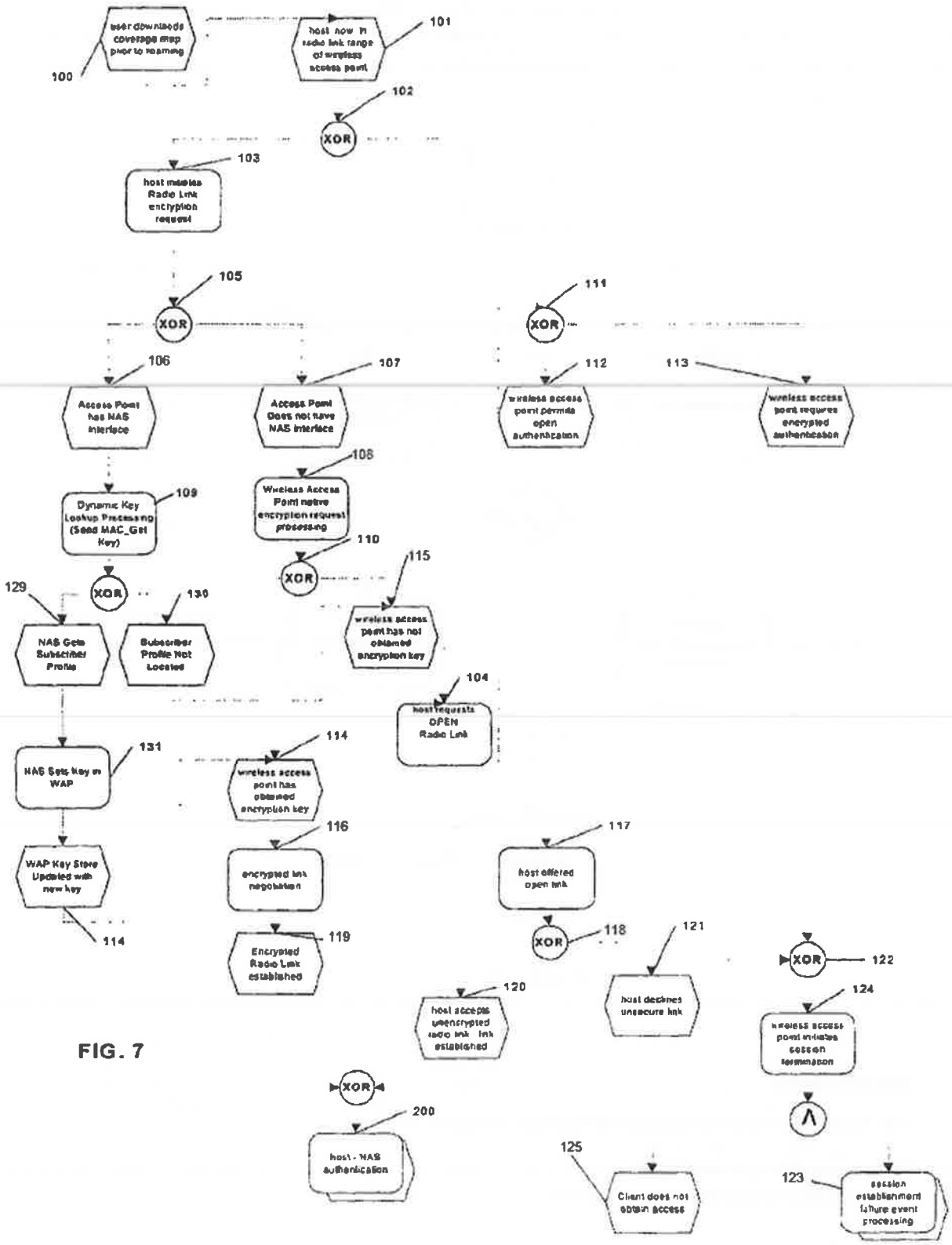
user downloads coverage map prior to roaming
100
host now in radio link range of wireless access point
101
XOR
102
host initiates Radio Link encryption request
103
XOR
105
Access Point has NAS interface
106
Access Point Does not have NAS interface
107
Dynamic Key Lookup Processing (Send MAC_Get Key)
109
Wireless Access Point native encryption request processing
108
XOR
110
XOR
129
130
NAS Gets Subscriber Profile
Subscriber Profile Not Located
NAS Sets Key in WAP
131
WAP Key Store Updated with new key
114
wireless access point has obtained encryption key
114
encrypted link negotiation
116
Encrypted Radio Link established
119
host requests OPEN Radio Link
104
XOR
111
wireless access point permits open authentication
112
wireless access point requires encrypted authentication
113
host offered open link
117
XOR
118
host accepts unencrypted radio link link established
120
host declines unsecure link
121
XOR
122
wireless access point initiates session termination
124
session establishment failure event processing
123
Client does not obtain access
125
host - NAS authentication
200

FIG. 7

Legende FIG. 7:

100: Benutzer lädt Abdeckungskarte vor Roaming herunter
101: Host nun in Funkreichweite des drahtlosen Zugangspunktes
102: XOR
103: Host initiiert Verschlüsselungsanfrage für Funkverbindung
104: Host fragt OFFENE Funkverbindung an
105: XOR
106: Zugangspunkt hat NAS-Schnittstelle
107: Zugangspunkt hat keine NAS-Schnittstelle
108: Verarbeitung einer nativen Verschlüsselungsanfrage am drahtlosen Zugangspunkt
109: Dynamische Verarbeitung der Schlüsselsuche (MAC senden_Schlüssel erhalten)
110: XOR
111: XOR
112: Drahtloser Zugangspunkt erlaubt offene Authentifizierung
113: Drahtloser Zugangspunkt verlangt verschlüsselte Authentifizierung
114 (oben): Drahtloser Zugangspunkt hat Verschlüsselungsschlüssel erhalten
114 (unten): WAP-Schlüsselspeicher wird mit neuem Schlüssel aktualisiert
115: Drahtloser Zugangspunkt hat keinen Verschlüsselungsschlüssel erhalten
116: Aushandeln einer verschlüsselten Verbindung
117: Host hat offene Verbindung angeboten
118: XOR
119: Verschlüsselte Verbindung wurde hergestellt
120: Host akzeptiert unverschlüsselte Funkverbindung_Verbindung hergestellt
121: Host lehnt unsichere Verbindung ab
122: XOR
123: Verarbeitung des Fehlerereignisses beim Herstellen der Verbindung
124: Drahtloser Zugangspunkt initiiert Beenden der Sitzung
125: Client erhält keinen Zugang
129: NAS erhält das Teilnehmerprofil
130: Teilnehmerprofil nicht lokalisiert
131: NAS setzt Schlüssel in den WAP
200: Host-NAS-Authentifizierung

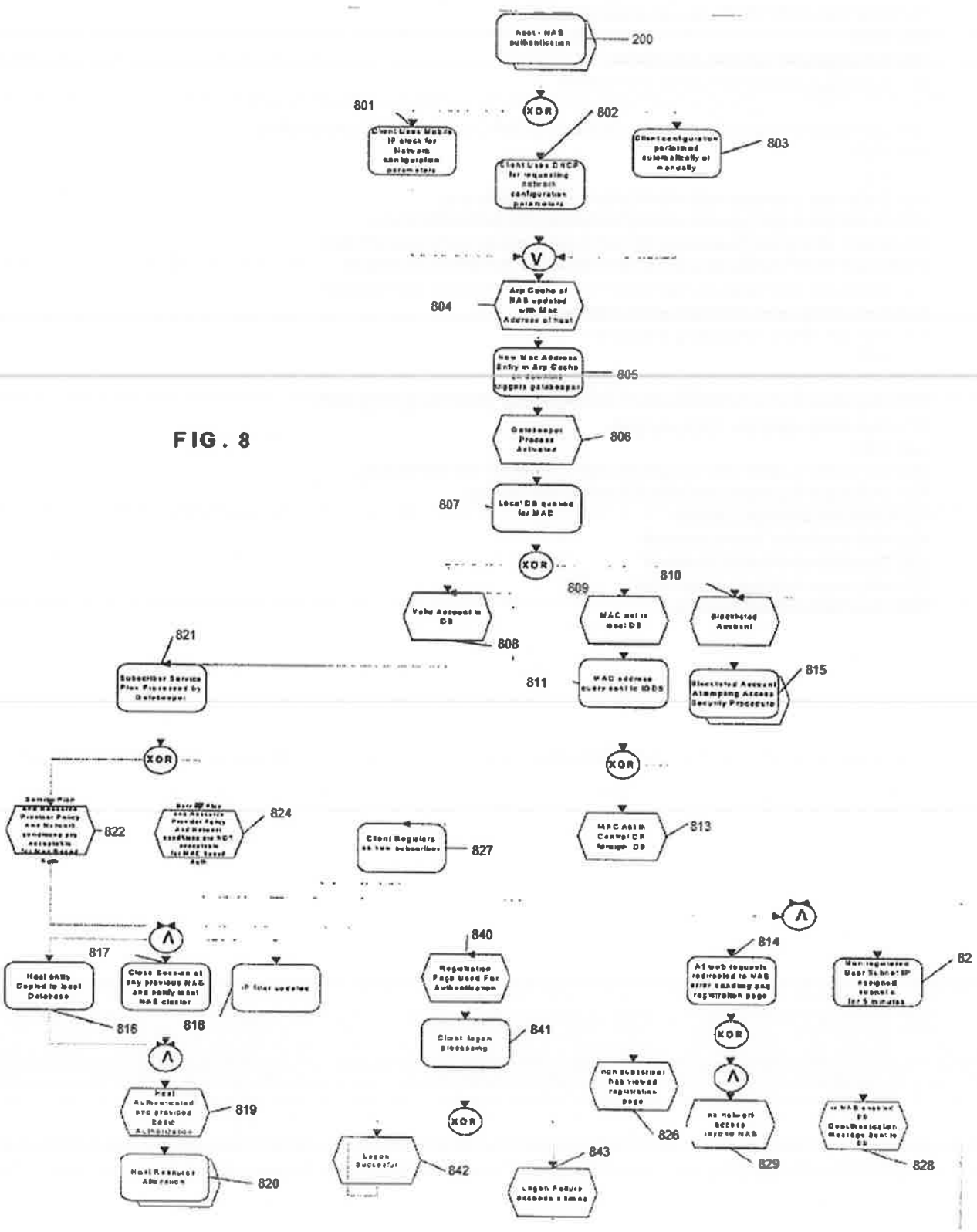
200
XOR
801
802
803
V
804
805
806
807
XOR
808
809
810
811
815
821
XOR
XOR
822
824
827
813
817
816
818
840
841
814
82
819
820
842
843
826
829
828

FIG. 8

Legende FIG. 8:

200: Host-NAS-Authentifizierung
801: Client verwendet Mobile-IP-Stapel für Netzwerkkonfigurationsparameter
802: Client verwendet DHCP für die Anfrage von Netzwerkkonfigurationsparametern
803: Client-Konfiguration wird automatisch oder manuell durchgeführt
804: ARP-Cache von NAS mit MAC-Adresse von Host aktualisiert
805: Neuer MAC-Adresseintrag im ARP-Cache für Downlink löst Gatekeeper aus
806: Gatekeeper-Prozess aktiviert
807: Lokale DB wird nach MAC durchsucht
808: Gültiges Konto in DB
809: MAC nicht in lokaler DB
810: Konto auf Blacklist
811: MAC-Adressanfrage wird an IODS gesendet
813: MAC nicht in zentraler ODER fremder DB
814: Alle Web-Anfragen werden an die Fehlerbehandlungs- und Registrierungsseite des NAS weitergeleitet
815: Zugang auf Blacklist versucht Zugangssicherheitsprozedur
816: Host-Eintrag wird in lokale Datenbank kopiert
817: Schließen der Sitzung bei einem vorherigen NAS und Benachrichtigung des lokalen NAS-Clusters
818: IP-Filter wird aktualisiert
819: Host wurde authentifiziert und erhält Basisberechtigung
820: Host-Ressourcen-Zuteilung
821: Dienstplan des Teilnehmers wird vom Gatekeeper verarbeitet
822: Dienstplan, Regelwerk des Ressourcenanbieters und Netzwerkbedingungen sind akzeptabel für MAC-basierte Authentifizierung
824: Dienstplan, Regelwerk des Ressourcenanbieters und Netzwerkbedingungen sind NICHT akzeptabel für MAC-basierte Authentifizierung
82[5]: Nicht registrierte Benutzer: Subnetz-IP wird 5 Minuten lang zugewiesen
826: Neuer Teilnehmer hat Registrierungsseite aufgerufen
827: Client registriert sich als neuer Teilnehmer
828: BS mit aktiviertem NAS: De-Authentifizierungs-Benachrichtigung wird an BS gesendet
829: Kein Netzwerkzugang außerhalb des NAS
840: Registrierungsseite wird für Authentifizierung verwendet
841: Verarbeitung der Client-Anmeldung
842: Anmeldung erfolgreich
843: Fehlgeschlagene Anmeldung überschreitet x Mal

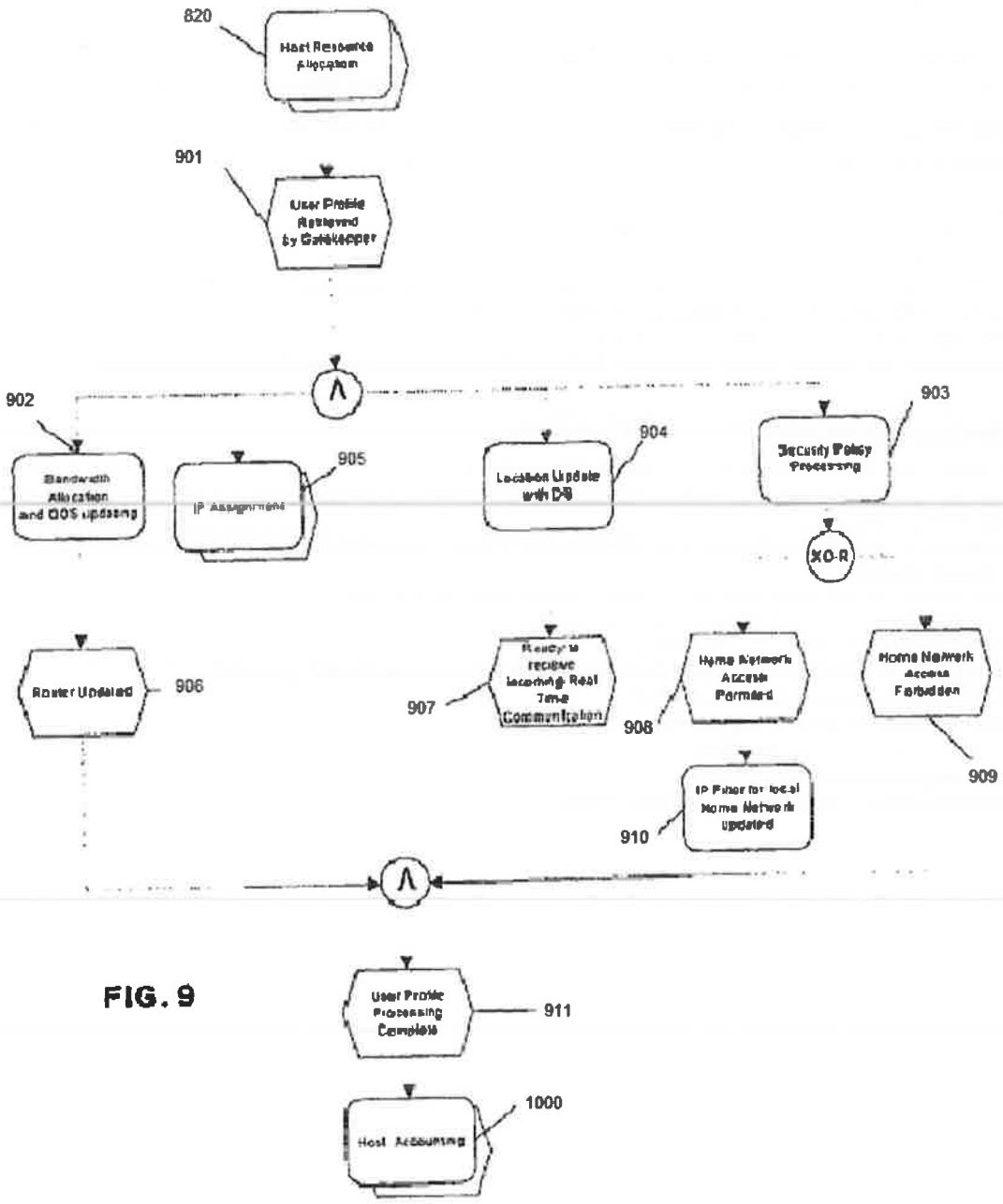

FIG. 9

Legende FIG. 9:

820: Host-Ressourcen-Zuteilung
901: Benutzerprofil von Gatekeeper abgerufen
902: Bandbreiten-Zuteilung und QoS-Aktualisierung
903: Sicherheitsregelwerk-Verarbeitung
904: Positionsaktualisierung mit DB
905: IP-Zuweisung
906: Router aktualisiert
907: Bereit für den Empfang ankommender Echtzeit-Kommunikation
908: Heim-Netzwerkzugang erlaubt
909: Heim-Netzwerkzugang untersagt
910: IP-Filter für lokales Heim-Netzwerk aktualisiert
911: Verarbeiten des Benutzerprofils abgeschlossen
1000: Host-Abrechnung

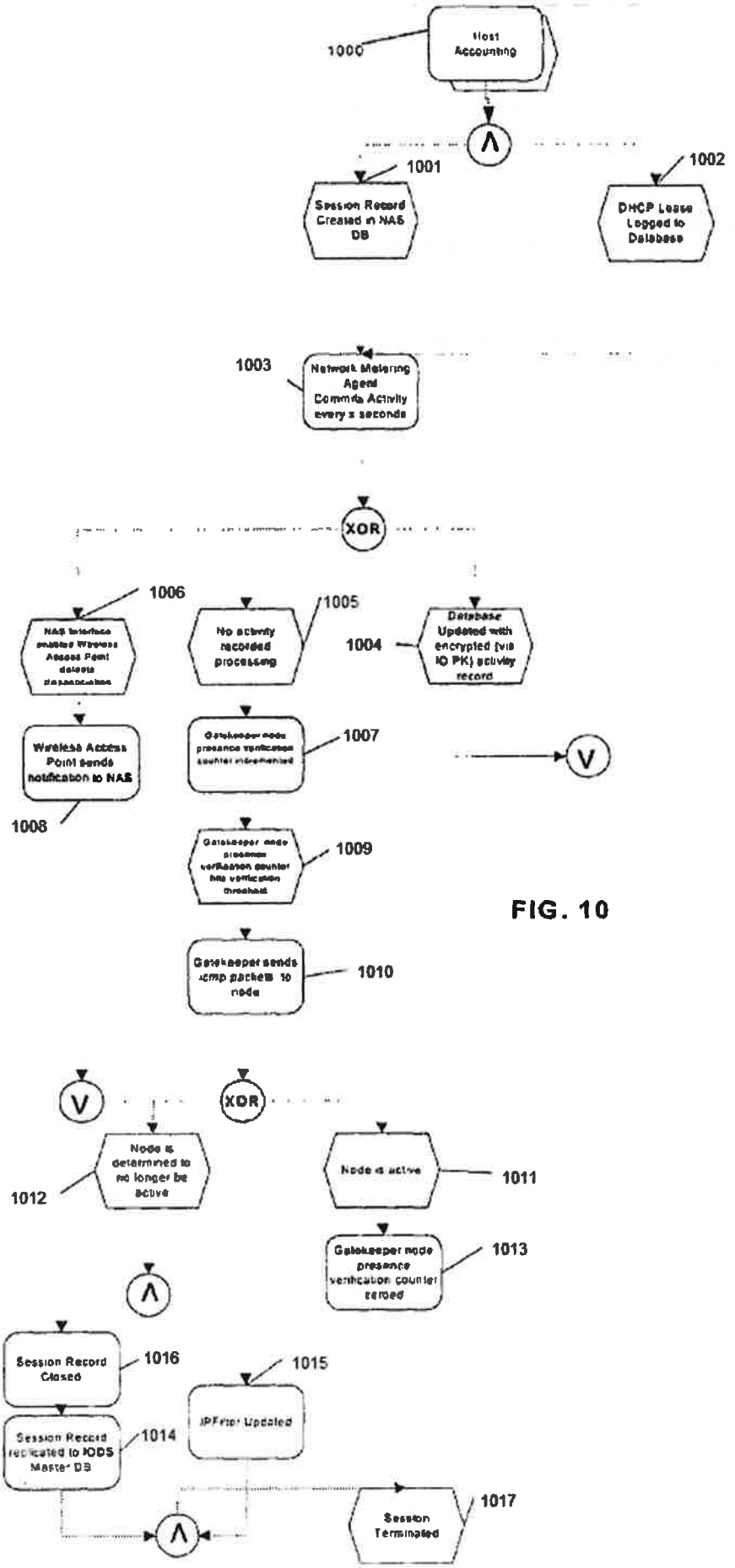
1000
Host Accounting
1001
Session Record Created in NAS DB
1002
DHCP Lease Logged to Database
1003
Network Metering Agent Commits Activity every x seconds
XOR
1006
1005
No activity recorded processing
1004
Database Updated with encrypted (via IO PK) activity record
Wireless Access Point sends notification to NAS
1008
1007
V
1009
1010
V
XOR
Node is determined to no longer be active
1012
Node is active
1011
1013
1016
1015
Session Record Closed
Session Record replicated to IODS Master DB
1014
1017
Session Terminated

FIG. 10

Legende FIG. 10:

1000: Host-Abrechnung
1001: Sitzungseintrag in NAS-DB erzeugt
1002: DHCP-Lease in Datenbank aufgezeichnet
1003: Netzwerkmessungsagent führt Aktivität alle x Sekunden aus
1004: Datenbank mit verschlüsseltem (über IO PK) Aktivitätseintrag aktualisiert
1005: Verarbeitung ohne eingetragene Aktivität
1006: Drahtloser Zugangspunkt mit aktivierter NAS-Schnittstelle erkennt Trennung
1007: Präsenzverifizierungszähler des Gatekeepers erhöht
1008: Drahtloser Zugangspunkt sendet Benachrichtigung an NAS
1009: Präsenzverifizierungszähler des Gatekeepers erreicht Schwellwert
1010: Gatekeeper sendet ICMP-Pakete an Knoten
1011: Knoten ist aktiv
1012: Knoten wird als nicht mehr aktiv bestimmt
1013: Präsenzverifizierungszähler des Gatekeepers wird auf Null gesetzt
1014: Sitzungseintrag in IODS-Master-DB repliziert
1015: IP-Filter aktualisiert
1016: Sitzungseintrag geschlossen
1017: Sitzung beendet

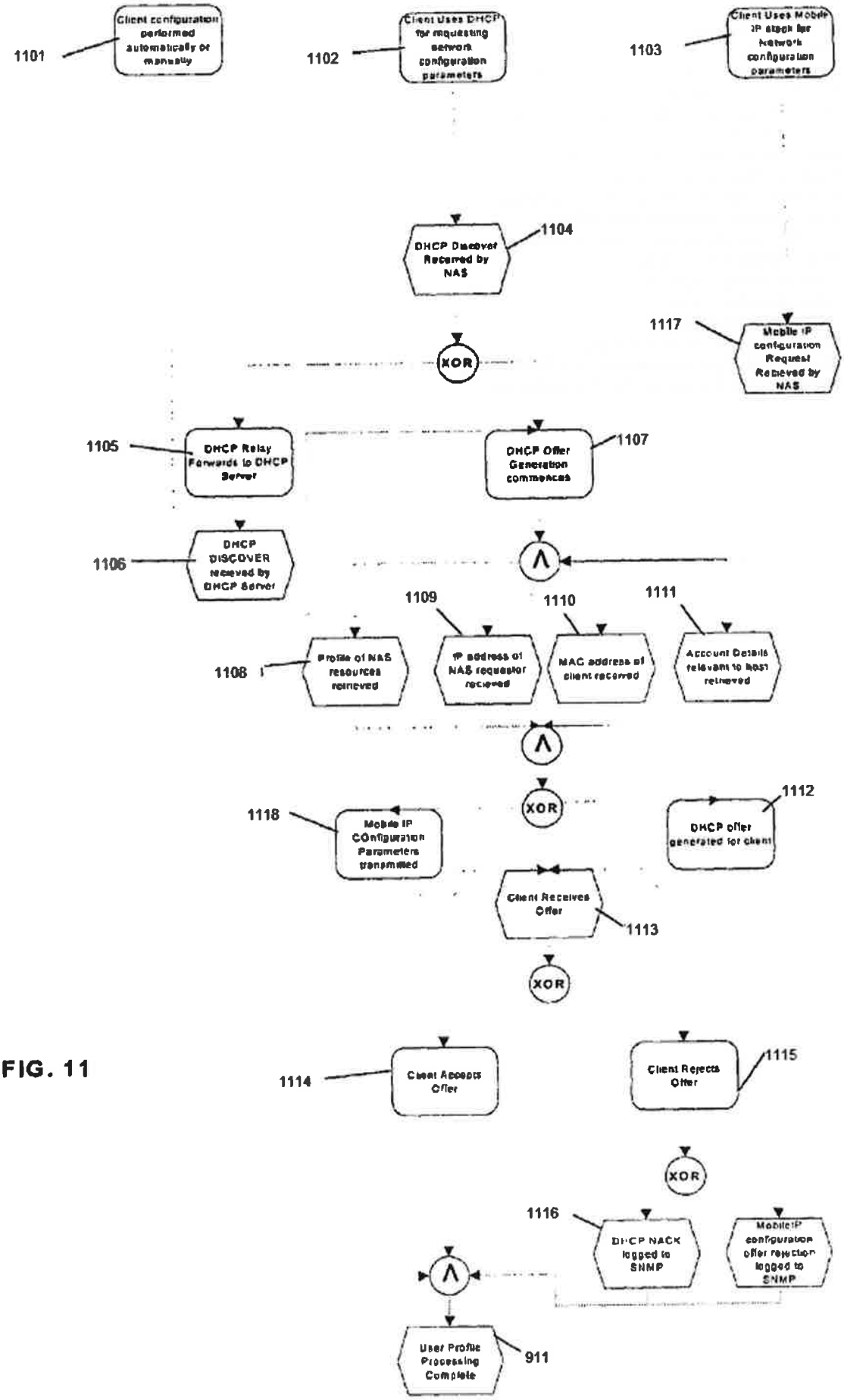
1101
Client configuration performed automatically or manually
1102
Client Uses DHCP for requesting network configuration parameters
1103
Client Uses Mobile IP stack for network configuration parameters
1104
DHCP Discover Received by NAS
1117
Mobile IP configuration Request Recieved by NAS
XOR
1105
DHCP Relay Forwards to DHCP Server
1107
DHCP Offer Generation commences
1106
DHCP DISCOVER received by DHCP Server
1109
1110
1111
1108
Profile of NAS resources retrieved
IP address of NAS requestor recieved
MAC address of client recieved
Account Details relevant to host retrieved
XOR
1118
Mobile IP COnfiguration Parameters transmitted
1112
DHCP offer generated for client
Client Receives Offer
1113
XOR
1114
Client Accepts Offer
Client Rejects Offer
1115
XOR
1116
DHCP NACK logged to SNMP
MobileIP configuration offer rejection logged to SNMP
User Profile Processing Complete
911

FIG. 11

Legende FIG. 11:

1101: Client-Konfiguration automatisch oder manuell durchgeführt
1102: Client verwendet DHCP für die Anfrage von Netzwerkkonfigurationsparametern
1103: Client verwendet Mobile-IP-Stapel für Netzwerkkonfigurationsparameter
1104: DHCP-Discover von NAS empfangen
1105: DHCP-Relay leitet weiter zu DHCP-Server
1106: DHCP-Discover von DHCP-Server empfangen
1107: DHCP-Angebotserzeugung beginnt
1108: Profil der NAS-Ressourcen abgerufen
1109: IP-Adresse des NAS-Requestors empfangen
1110: MAC-Adressen des Client empfangen
1111: Für den Host relevante Kontodaten abgerufen
1112: DHCP-Angebot für Client erzeugt
1113: Client empfängt Angebot
1114: Client akzeptiert Angebot
1115: Client lehnt Angebot ab
1116: DHCP-NACK in SNMP aufgezeichnet
1117: Mobile-IP-Konfigurationsanfrage vom NAS empfangen
911: Verarbeiten des Benutzerprofils abgeschlossen

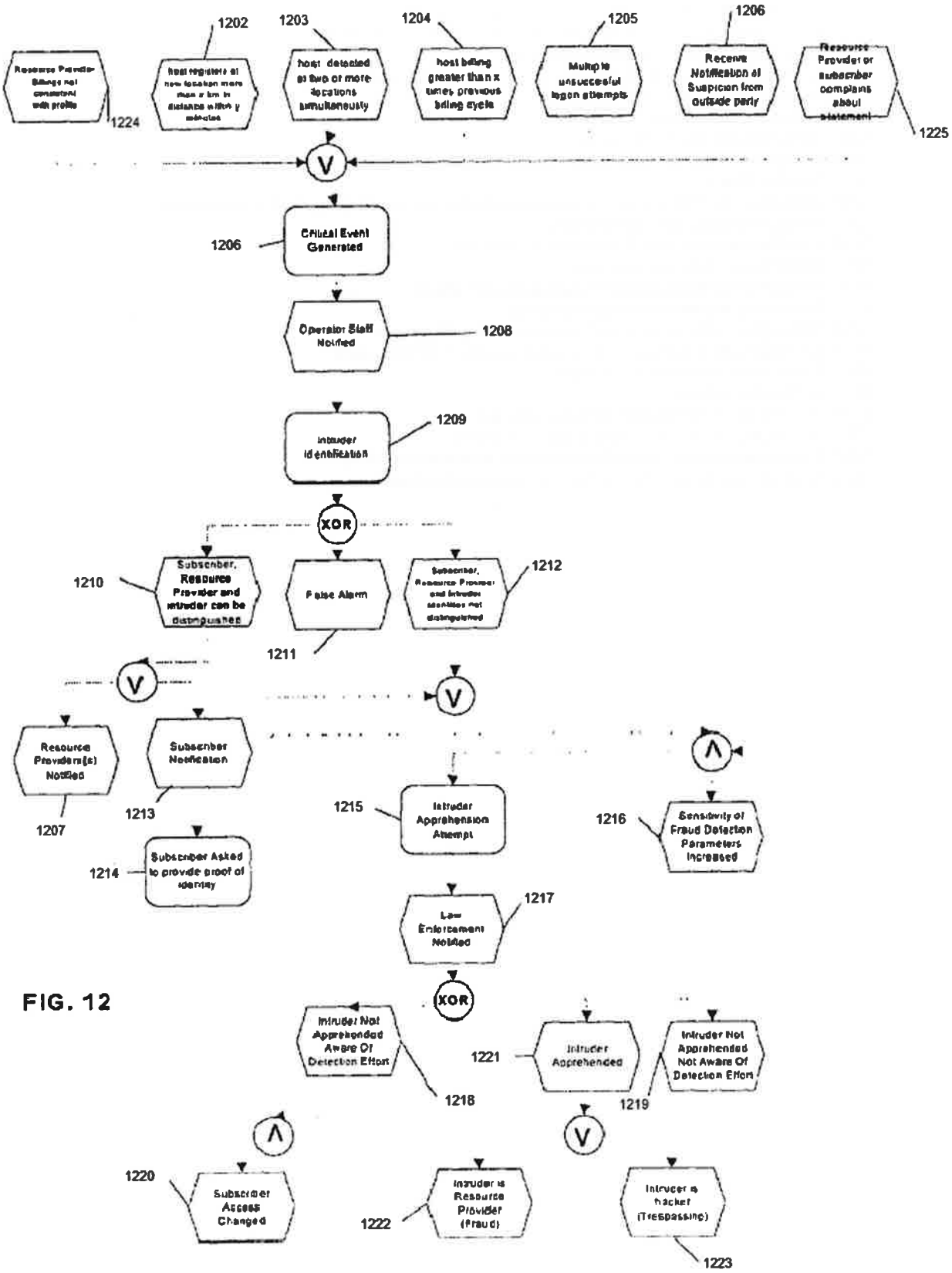
1202
1203
host detected at two or more locations simultaneously
1204
host billing greater than x times previous billing cycle
1205
Multiple unsuccessful logon attempts
1206
Receive Notification of Suspicion from outside party
1225
1224
V
1206
Critical Event Generated
Operator Staff Notified
1208
Intruder Identification
1209
XOR
1210
Subscriber, Resource Provider and intruder can be distinguished
False Alarm
1211
1212
V
V
Resource Provider(s) Notified
1207
Subscriber Notification
1213
Subscriber Asked to provide proof of identity
1214
1215
Intruder Apprehension Attempt
1216
Sensitivity of Fraud Detection Parameters Increased
Law Enforcement Notified
1217
XOR
Intruder Not Apprehended Aware Of Detection Effort
1218
1221
Intruder Apprehended
Intruder Not Apprehended Not Aware Of Detection Effort
1219
V
1220
Subscriber Access Changed
1222
Intruder is Resource Provider (Fraud)
Intruder is hacker (Trespassing)
1223

FIG. 12

Legende FIG. 12:

1202: Host registriert sich an neuem Ort in mehr als x km Entfernung innerhalb y Minuten
1203: Host an zwei oder mehr Orten gleichzeitig erkannt
1204: Host-Abrechnung größer als x-Mal vorheriger Abrechnungszyklus
1205: Mehrere gescheiterte Anmeldeversuche
1206: Empfang einer Verdachtsbenachrichtigung von außenstehender Partei
1207: Ressourcenanbieter benachrichtigt
1208: Betreiber-Personal benachrichtigt
1209: Identifizierung des Eindringlings
1210: Teilnehmer, Ressourcenanbieter und Eindringling können unterschieden werden
1211: Falscher Alarm
1212: Identitäten von Teilnehmer, Ressourcenanbieter und Eindringling nicht unterschieden
1213: Benachrichtigung des Teilnehmers
1214: Identitätsnachweis vom Teilnehmer angefordert
1215: Befürchtung Eindringlingsversuch
1216: Sensibilität der Betrugserkennungsparameter erhöht
1217: Strafverfolgungsbehörden benachrichtigt
1218: Eindringling nicht gefasst, hat Detektionsversuch bemerkt
1219: Eindringling nicht gefasst, hat Detektionsversuch nicht bemerkt
1220: Zugang des Teilnehmers verändert
1221: Eindringling gefasst
1222: Eindringling ist Ressourcenanbieter (Betrug)
1223: Eindringling ist Hacker (unerlaubtes Eindringen)
1224: Ressourcenanbieter- Abrechnungen nicht konsistent mit Profil
1225: Ressourcenanbieter oder Teilnehmer beanstandet Abrechnung

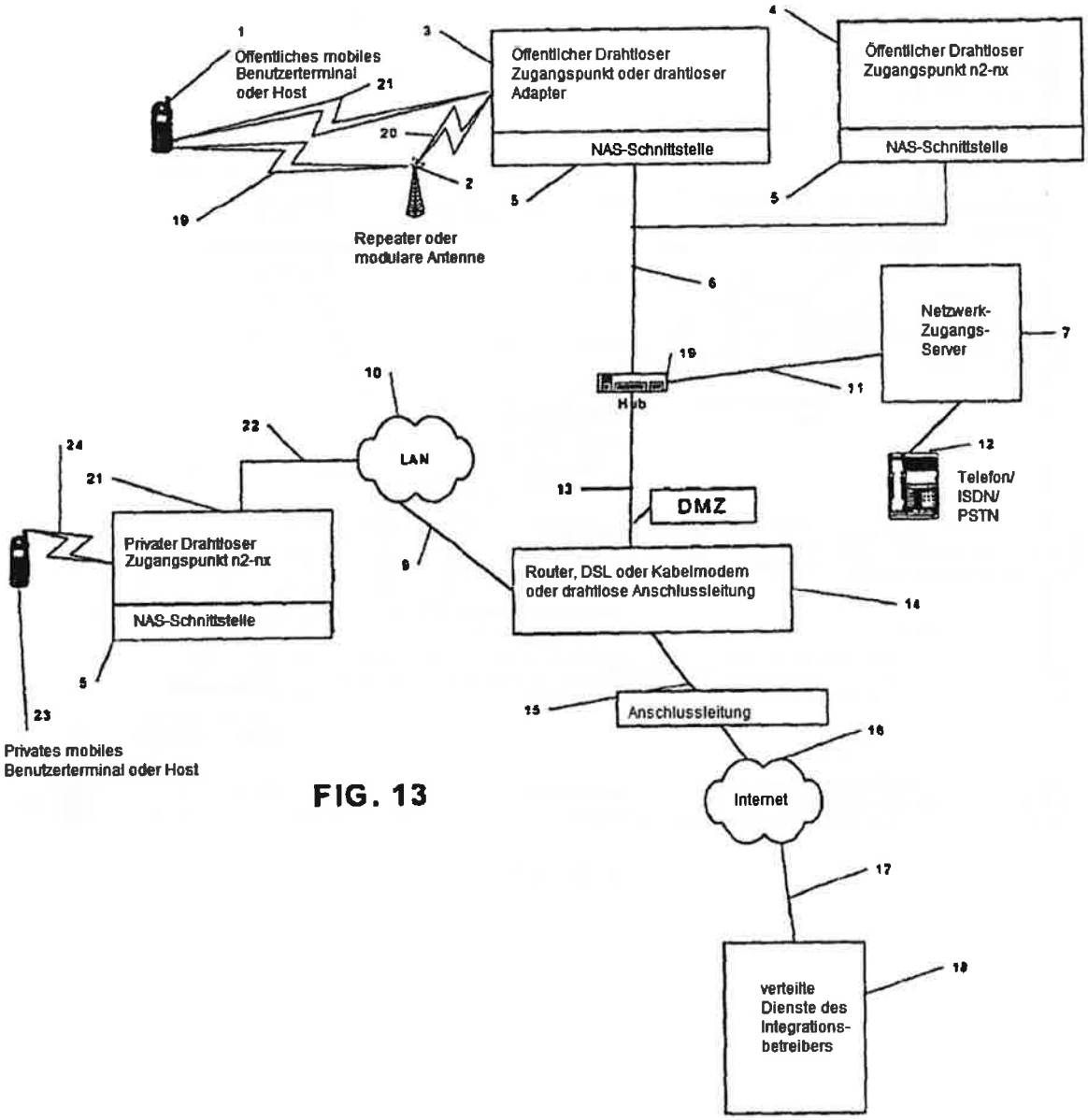
1
Öffentliches mobiles Benutzerterminal oder Host
3
Öffentlicher Drahtloser Zugangspunkt oder drahtloser Adapter
NAS-Schnittstelle
4
Öffentlicher Drahtloser Zugangspunkt n2-nx
NAS-Schnittstelle
21
20
2
19
5
5
Repeater oder modulare Antenne
6
Netzwerk-Zugangs-Server
7
19
11
Hub
10
22
LAN
24
21
12
Telefon/ ISDN/ PSTN
13
DMZ
Privater Drahtloser Zugangspunkt n2-nx
NAS-Schnittstelle
9
Router, DSL oder Kabelmodem oder drahtlose Anschlussleitung
14
5
15
Anschlussleitung
23
Privates mobiles Benutzerterminal oder Host
16
Internet
17
verteilte Dienste des Integrations-betreibers
18

FIG. 13

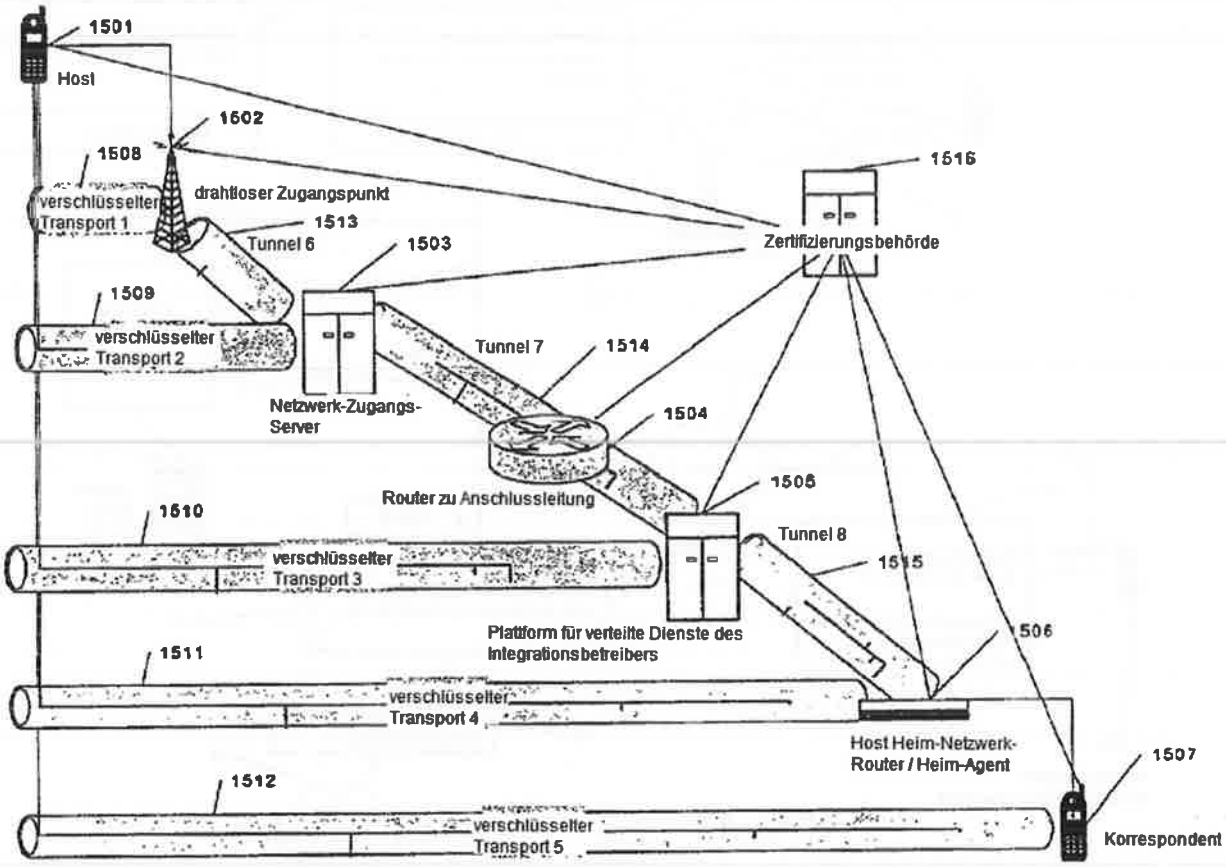
1501
Host
1502
1508
verschlüsselter Transport 1
drahtloser Zugangspunkt
1513
Tunnel 6
1503
1516
Zertifizierungsbehörde
1509
verschlüsselter Transport 2
Tunnel 7
1514
Netzwerk-Zugangs-Server
1504
Router zu Anschlussleitung
1505
1510
verschlüsselter Transport 3
Tunnel 8
1515
Plattform für verteilte Dienste des Integrationsbetreibers
1506
1511
verschlüsselter Transport 4
Host Heim-Netzwerk-Router / Heim-Agent
1507
1512
verschlüsselter Transport 5
Korrespondent

FIG. 14

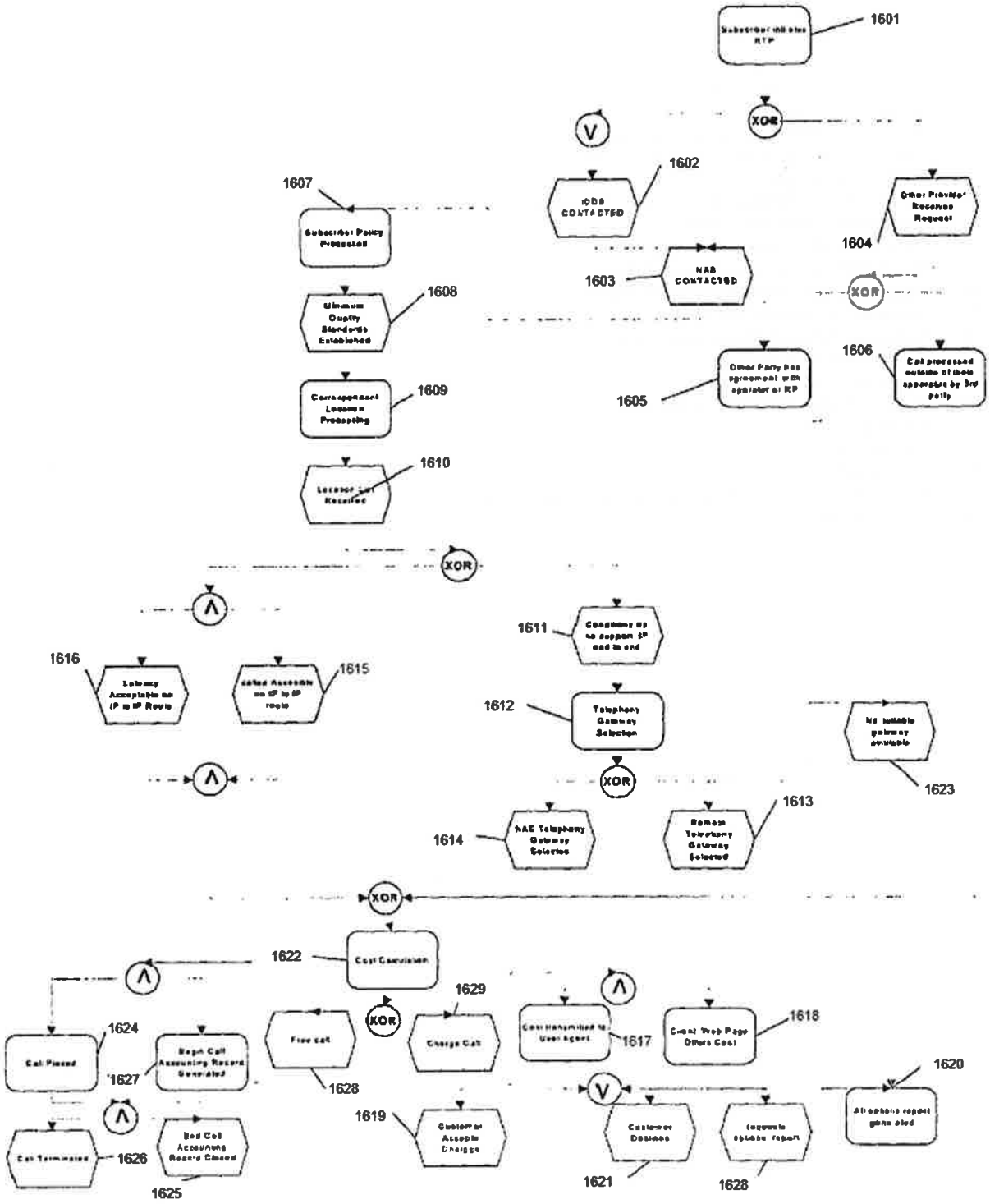
1601
XOR
V
1602
1603
1604
XOR
1605
1606
1607
1608
1609
1610
XOR
1611
1612
XOR
1613
1614
1615
1616
1623
XOR
1622
1629
XOR
1624
1627
1628
1617
1618
1620
V
1619
1626
1625
1621
1628

FIG. 15

Legende FIG. 15:

1601: Teilnehmer initiiert RTP
1602: IODS kontaktiert
1603: NAS kontaktiert
1604: Anderer Anbieter empfängt Anfrage
1605: Andere Partei hat Vereinbarung mit Betreiber oder RA
1606: Anruf wird von dritter Partei außerhalb deren Vorrichtung verarbeitet
1607: Teilnehmer-Regelwerk verarbeitet
1608: Minimale Qualitätsstandards festgelegt
1609: Verarbeitung des Korrespondenten-Ortes
1610: Ortsliste empfangen
1611: Bedingungen unterstützen kein Ende-zu-Ende-IP
1612: Auswahl des Telefonie-Gateways
1613: Remote-Telefonie-Gateway ausgewählt
1614: NAS-Telefonie-Gateway ausgewählt
1615: Angerufene erreichbar auf IP-zu-IP-Route
1616: Latenzzeit akzeptabel auf IP-zu-IP-Route
1617: Kosten an Benutzer-Agent übermittelt
1618: Client-Webseite bietet Kosten an
1619: Kunde akzeptiert Gebühren
1620: Bericht mit allen Optionen generiert
1621: Kunde lehnt ab
1622: Kostenkalkulation
1624: Anruf getätigt
1625: Abschließender Anruf-Abrechnungseintrag geschlossen
1626: Anruf beendet

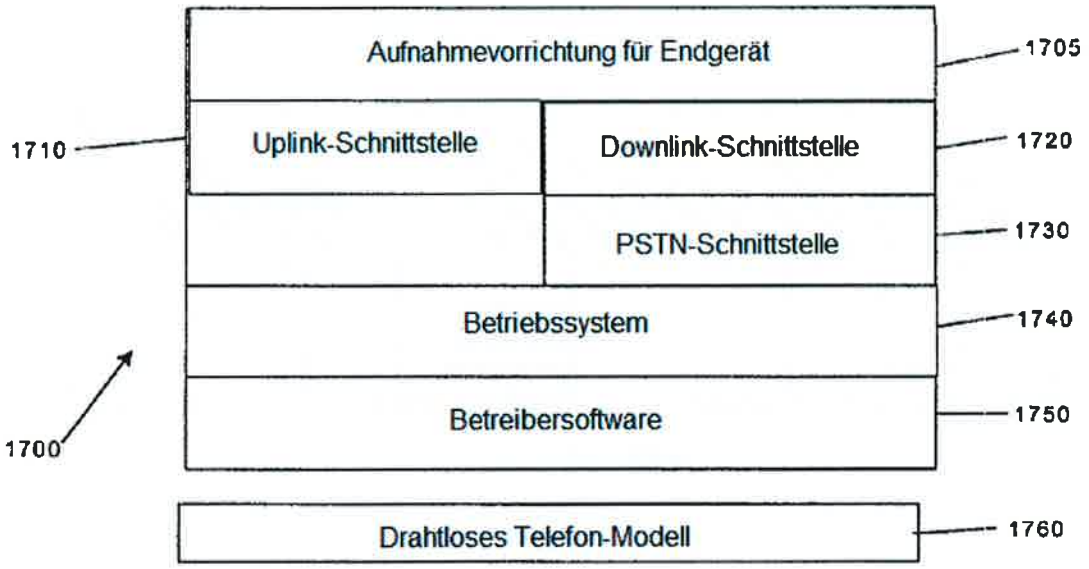
Aufnahmevorrichtung für Endgerät
1705
1710
Uplink-Schnittstelle
Downlink-Schnittstelle
1720
PSTN-Schnittstelle
1730
Betriebssystem
1740
Betreibersoftware
1750
1700
Drahtloses Telefon-Modell
1760

FIG. 16

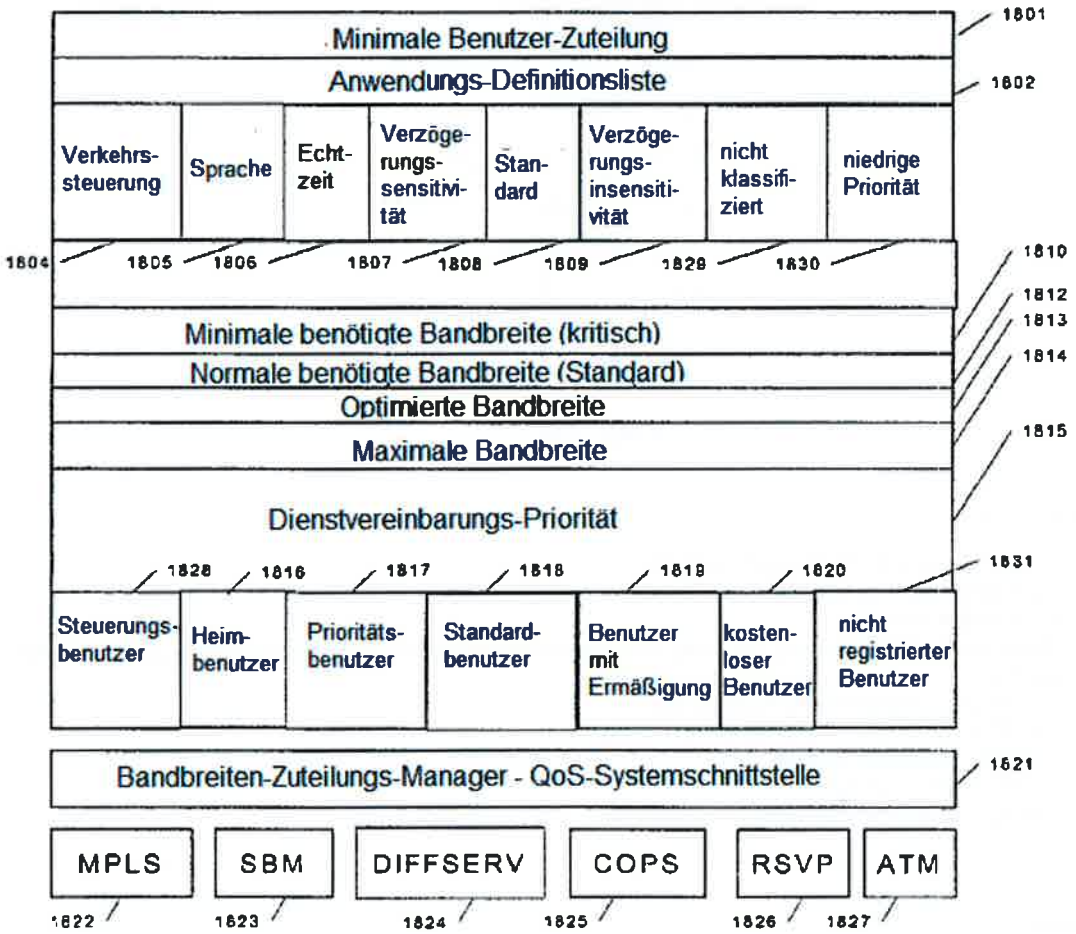
Minimale Benutzer-Zuteilung
1801
Anwendungs-Definitionsliste
1802
Verkehrs-steuerung
Sprache
Echt-zeit
Verzöge-rungs-sensitivi-tät
Stan-dard
Verzöge-rungs-insensiti-vität
nicht klassifi-ziert
niedrige Priorität
1804
1805
1806
1807
1808
1809
1828
1830
1810
1812
1813
1814
1815
Minimale benötigte Bandbreite (kritisch)
Normale benötigte Bandbreite (Standard)
Optimierte Bandbreite
Maximale Bandbreite
Dienstvereinbarungs-Priorität
1828
1816
1817
1818
1819
1820
1831
Steuerungs-benutzer
Heim-benutzer
Prioritäts-benutzer
Standard-benutzer
Benutzer mit Ermäßigung
kosten-loser Benutzer
nicht registrierter Benutzer
Bandbreiten-Zuteilungs-Manager - QoS-Systemschnittstelle
1821
MPLS
SBM
DIFFSERV
COPS
RSVP
ATM
1822
1823
1824
1825
1826
1827

FIG. 17

	1901 Bandwidth Need Type (C,N,O,M)	1902 SLA Type (C,H,P,S,L,F,U)	1903 h-v Contention Scenario	1904 Application Type (Control, Voice, RTP, Delay Sensitive, Regular or Encrypt, Uncat, Low)	1905 BW has metered cost basis ?	1906 Local Global (LG,GL)	1907 Request Originates Outside of Allocation ?
	7,4,2,0	10,6,6,3, 2,1,-2	3	7,5,4,3,1,0,-2	NO EXTRA ALLOCATION EXCEPT FOR METERED PLANS	-1,-3	-3

FIG. 18

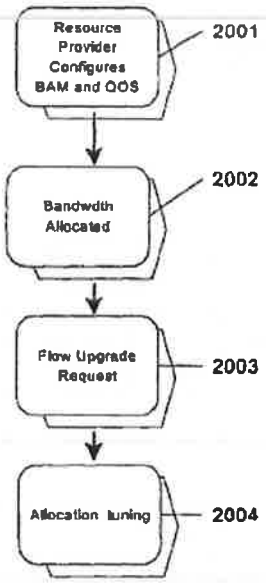

FIG. 19

Legende FIG. 18:

1901: Art des Bandbreitenbedarfs (C, N, O, M)
1902: SLA-Art (C, H, P, S, L, F, U)
1903: h-v-Konflikt-Szenario
1904: Anwendungsart (Steuerung, Sprache, RTP, verzögerungssensitiv, normal oder verschlüsselt, nicht klassifiziert, gering)
1905: Bandbreite hat gemessene Kostenbasis?
KEINE ZUSÄTZLICHE ZUTEILUNG AUSSER FÜR GEMESSENE PLÄNE
1906: Lokal Global (LG, GL)
1907: Anfrage kommt von außerhalb der Zuteilung?

Legende FIG. 19:

2001: Ressourcenanbieter konfiguriert BAM und QoS
2002: Bandbreite zugeteilt
2003: Durchfluss-Upgrade-Anfrage
2004: Anpassen der Zuteilung

INTEGRATION ÖFFENTLICHER UND PRIVATER NETZWERKRESSOURCEN FÜR DEN OPTIMIERTEN DRAHTLOSEN BREITBANDZUGANG UND VERFAHREN

ZUGEHÖRIGER FALL

[0001] Diese Anmeldung steht im Zusammenhang mit der vorläufigen Anmeldung Nr. 60/256,158 mit dem Titel Integrating Public and Private Network Resources for Optimized Broadband Wireless Access and Method, die W. Alexander Hagen als Erfinder nennt und am 15. Dezember 2000 eingereicht wurde, und beansprucht deren Priorität. Der Inhalt dieser Anmeldung soll als Bestandteil dieses Dokuments angesehen werden.

HINTERGRUND DER ERFINDUNG

[0002] 1. Gebiet der Erfindung

[0003] Die Erfindung bezieht sich im Allgemeinen auf digitale Netzwerke. Konkret bezieht sich die Erfindung auf die Integration und Interoperabilität verschiedener privater und öffentlicher Netzwerke, um einen allgegenwärtigen Breitband-Netzwerkzugang bereitzustellen. Noch konkreter bezieht sich die Erfindung auf ein System und Verfahren für die Bereitstellung und das Management des Zugangs zu öffentlichen Netzwerken durch drahtlose, mobile Terminals unter Inanspruchnahme bestehender Netzwerkverbindungsressourcen ansonsten privater Netzwerke.

[0004] 2. Darlegung verwandter Technik

[0005] Bestehende Systeme, die darauf gerichtet sind, drahtlosen Netzwerkzugang bereitzustellen, sind durch eine Reihe von Faktoren eingeschränkt. Zunächst sind solche Systeme typischerweise durch relativ große Zellen gekennzeichnet, die sich nachteilig auf die Signalqualität auswirken und dadurch die Bandbreite einschränken. Heutzutage haben Zellen normalerweise einen Radius von mindestens einer Meile. Im Allgemeinen stehen wirtschaftliche Überlegungen dem Aufbau und Betrieb von Zellen in größerer Dichte im Wege, obwohl das Verringern des Radius jeder Zelle größere spektrale Ressourcen bereitstellen würde. Dies würde zum einen durch die Verringerung der Anzahl von Nutzern entstehen, die von einer einzelnen Zelle aufgenommen werden, und zum anderen durch eine Verbesserung der Signalqualität aufgrund kürzerer Entfernungen zwischen Sender und Empfänger, wodurch der Energiebedarf reduziert wird und effizientere Modulationsschemata ermöglicht werden. Solche Systeme haben daher im Allgemeinen schlechte Voraussetzungen für die Bereitstellung von drahtlosem Breitband-Netzwerkzugang.

[0006] Es werden Bemühungen unternommen, um sog. drahtlose Breitband- bzw. „3G"-Netzwerke zu entwickeln. Es ist jedoch eine Reihe schwerwiegender Probleme aufgetreten. Erstens weisen die vorgeschlagenen Kommunikationsprotokolle bestimmte Einschränkungen auf, die den Breitbandzugang einschränken oder gar verhindern. Diese Einschränkungen machen derartige Protokolle insbesondere für die Verwendung in drahtlosen Anschlussleitungs-Netzwerken ungeeignet. Das Hauptproblem liegt darin, dass derartige Protokolle für die Verwendung mit Datenkommunikation bei relativ hohen Frequenzen konzipiert sind. Datenkommunikation bei solchen Frequenzen funktioniert jedoch nicht zufriedenstellend über weite Entfernungen, insbesondere nicht zu Terminals im Haus oder bei Nicht-Sichtverbindungen. Im allgemeinen Gebrauch fallen die Datenraten gewöhnlich aus dem „Breitband"-Bereich auf 128/64 KBit/s. Unter Umständen kann es sogar unmöglich sein, überhaupt erfolgreich eine Netzwerkdatenverbindung aufzubauen. Zweitens sind die Kosten für den Aufbau und Betrieb von Netzwerken im Frequenzspektrum, das für die Verwendung durch 3G-Netzwerke vorgesehen ist, dem sog.

IMT-2000-Band, so hoch, dass derartige Netzwerke – obwohl sie technisch machbar wären – unter Umständen wirtschaftlich nicht realisierbar sind. Drittens war der ursprüngliche Plan für ein einziges globales Band bislang erfolglos und wurde nun verschoben, um die Entwicklung sog. Netzwerke der vierten Generation bzw. globaler drahtloser 4G-Netzwerke abzuwarten.

[0007] Derzeit sind Protokolle verfügbar, die zumindest theoretisch in der Lage wären, Zugang zu drahtlosen Breitbandnetzwerken zu unterstützen. Derartige Protokolle enthalten das Wireless-LAN-Protokoll, das in IEEE 802.11 spezifiziert ist, und das proprietäre Bluetooth-Protokoll. Das Wireless-LAN-802.11b-Protokoll ist darauf ausgerichtet, drahtlose Kommunikation bei Datenraten von bis zu 11 MBit/s zu ermöglichen. Bluetooth ist derzeit darauf ausgerichtet, eine derartige Kommunikation bei Datenraten von ca. 1 MBit/s zu ermöglichen. Diese Protokolle weisen jedoch eine Reihe von Einschränkungen auf, die echten großflächigen drahtlosen „Breitband"-Zugang erschweren oder unmöglich machen können. Insbesondere sind sie speziell auf drahtlose Kurzstrecken-Netzwerkkommunikation ausgerichtet und ungeeignet für den Aufbau von Datenverbindungen über weite Entfernungen oder bei Nicht-Sichtverbindungen. Somit ist deren Fähigkeit, drahtlosen Breitband-Netzwerkzugang bereitzustellen, normalerweise auf relativ kurze Entfernungen beschränkt. Außerdem arbeiten sie nur im ISM-Band von 2,4 GHz (unlizenziertes Spektrum), in dem Funkstörungen ein Problem darstellen können. Daher sind sie nicht in der Lage, Breitband-Leistungsniveau in offenen Umgebungen zu bieten, in denen Signalstörungen in der Funkfrequenz wahrscheinlich sind. Des Weiteren gibt es derzeit kein effektives Verfahren, das Nutzern solcher Protokolle, die vorrangig auf die proprietäre Verwendung von Wireless-LAN ausgerichtet sind, Roaming abseits ihres „Heim"-Netzwerks ermöglicht. Das heißt, dass es derzeit keinen Betreiber als „Integrator" gibt, der die unterschiedlichen proprietären und privaten drahtlosen Wireless-LAN-Netzwerke und Bluetooth-Zugangspunkte logisch miteinander verbindet, um allgegenwärtige Konnektivität für mobile Nutzer zu bieten. Nutzer können somit nur von den Vorteilen der großen Bandbreite dieser Protokolle profitieren, wenn sie die Möglichkeit haben, auf ihre eigenen privaten Heim-Netzwerke zuzugreifen.

[0008] Schließlich gibt es in den USA ein drittes Netzwerk, das Metricom-Netzwerk. Dieses proprietäre Netzwerk ist derzeit auf einen Betrieb bei 900 MHz beschränkt, eine unlizenzierte Frequenz, und besitzt derzeit kein effektives System für den Umgang mit Funkstörungsproblemen. Es ist ebenfalls auf Datenraten von 128 KBit/s beschränkt und dadurch für Anwendungen in drahtlosen Anschlussleitungen ungeeignet. Es ist außerdem eingeschränkt durch das offensichtliche Unvermögen, ausreichend Infrastruktur für eine zuverlässige landesweite Abdeckung zu bieten, und die Funkmodems, die dafür hergestellt werden, können jedenfalls außerhalb der USA nicht verwendet werden.

[0009] Kurzum, obwohl unterschiedliche Formen drahtloser öffentlicher und privater Netzwerke mit mobilem Zugang existieren oder vorgeschlagen werden, ist keines davon gegenwärtig in der Lage, echten flächendeckenden drahtlosen mobilen Netzwerkzugriff mit Breitband-Datenraten zu gewährleisten. Außerdem bieten aktuelle Netzwerke drahtlosen Terminals nicht die Möglichkeit, ohne weiteres zwischen zellularen und privaten Netzwerken zu umzuschalten. Es besteht zweifellos die Notwendigkeit, einen derartigen Zugang bereitzustellen und zu verwalten, und die vorliegende Erfindung befasst sich mit dieser Notwendigkeit.

KURZE ZUSAMMENFASSUNG DER ERFINDUNG

[0010] Die vorliegende Erfindung sieht ein System und Verfahren vor, das Terminals die Möglichkeit bietet, mit Breitband-Datenraten auf öffentliche Netzwerke zuzugreifen, wie beispielsweise das Internet, über feste, drahtgebundene oder drahtlose Verbindungen und an geografisch verteilten Netzwerkzugangspunkten unter Inanspruchnahme der bestehenden öffentlichen Netzwerkverbindungen privater oder proprietärer Netzwerke. Die vorliegende Erfindung integriert somit effektiv unterschiedliche private und öffentliche Netzwerke, um einen allgegenwärtigen Netzwerkzugang mit Breitband-Datenraten unter Inanspruchnahme der bestehenden Infrastruktur bereitzustellen.

[0011] Erfindungsgemäß ist eine Vielzahl von Netzwerkzugangspunkten an geografisch verteilten Standorten vorgesehen. Einige oder alle dieser Netzwerkzugangspunkte können drahtlose Zugangspunkte sein. Ein Netzwerk-Zugangs-Server („Network Access Server", NAS), der Software, Hardware oder eine Kombination aus beidem sein kann, fungiert als Zwischenglied oder Schnittstelle zwischen einer oder mehreren solcher drahtloser Zugangspunkte und den bestehenden öffentlichen Netzwerkverbindungsressourcen eines verbundenen, ansonsten privaten Netzwerks. Der NAS bietet und verwaltet den Zugang zu einem öffentlichen Netzwerk für autorisierte Terminals, einschließlich mobiler, drahtloser Terminals unter Inanspruchnahme der bestehenden öffentlichen Netzwerkverbindung des verbundenen privaten Netzwerks, während er zugleich unautorisierten Zugang zu dem privaten Netzwerk durch diese Terminals verhindert.

[0012] Der NAS kann eine Vielzahl von Netzwerkzugangs- und Netzwerk-Managementmöglichkeiten bieten einschließlich der Registrierung von Teilnehmern, der Messung der Netzwerkaktivität zu Abrechnungs- und Rechnungsstellungszwecken sowie der Überwachung und Steuerung der Bandbreitennutzung durch autorisierte Teilnehmer.

[0013] Ein anderer Aspekt der Erfindung ist die Bereitstellung verteilter Dienste eines Integrationsbetreibers („Integration Operator Distributed Services", IODS). Der IODS stellt Master-Einrichtungen für Abrechnung, Nutzerautorisierung und Sicherheit sowie für das Management und die Steuerung des NAS bereit. Der IODS und die unterschiedlichen NAS des Systems kommunizieren entfernt über das öffentliche Netzwerk. Die Kombination aus IODS und NAS bietet ein geografisch verteiltes, öffentlich zugängliches, verteiltes Netzwerksystem mit allgegenwärtigem Zugang.

[0014] Ein besonders vorteilhaftes Merkmal der Erfindung im Hinblick auf den Netzwerkzugang mit mobilen drahtlosen Terminals ist die große Verringerung des durchschnittlichen Abstands zwischen drahtlosen, mobilen Terminals und ihren Zugangspunkten zum drahtlosen Netzwerk, wodurch die Qualität der Netzwerkverbindungen und der Datenkommunikation stark verbessert wird, während der Energiebedarf für die Übertragung und die Datenfehlerrate reduziert und somit die Datenraten verbessert werden. Dadurch ist die Erfindung in der Lage, echten großflächigen Breitband-Netzwerkzugang für drahtlose, mobile Terminals zu bieten.

[0015] Ein weiteres vorteilhaftes Merkmal der Erfindung ist, dass keine zusätzliche Software benötigt wird oder Veränderungen an bestehenden Terminals oder Netzwerkzugangsgeräten vorgenommen werden müssen, einschließlich drahtloser Terminals und Geräte. Der NAS und IODS wickeln transparent Konfigurationsanforderungen ab sowie Verbindungen, Registrierung, Sicherheit, Abrechnung, Zahlungen, Management und andere Funktionen. Die vorliegende Erfindung nutzt somit bereits vorhandene Infrastruktur und Geräte.

[0016] Ein weiteres vorteilhaftes Merkmal der Erfindung ist, dass eine manuelle Rekonfiguration des Netzwerkadapters eines Terminals jedes Mal, wenn sich das Terminal mit einem neuen Netzwerkzugangspunkt verbindet, nicht notwendig ist,

selbst wenn sich der Netzwerkzugangspunkt nicht im „Heim"-Netzwerk des Terminals befindet. Der NAS und der IODS wickeln die Konfigurationsfunktionen transparent an der logischen Netzwerkschicht ab.

[0017] Ein weiteres vorteilhaftes Merkmal der Erfindung ist, dass die Terminals keine spezielle Software oder Hardware außer der aktuellen Standardsoftware und -hardware für Netzwerk-Datenkommunikation, einschließlich drahtloser Netzwerkkommunikation, benötigen. Der NAS wickelt transparent die Registrierung der Terminals, die Authentifizierung sowie die Verarbeitung des Netzwerkzugangs ab.

[0018] Zusätzliche Merkmale und Vorteile der Erfindung werden sich durch Bezugnahme in der folgenden detaillierten Beschreibung der bevorzugten Ausführungsformen in Verbindung mit den Zeichnungen erschließen.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0019] **FIG. 1** ist ein Blockdiagramm der derzeit bevorzugten Systemarchitektur gemäß der Erfindung.

[0020] **FIG. 2** ist ein Blockdiagramm, das die Elemente einer derzeit bevorzugten Datenbank eines Integrationsbetreibers zeigt.

[0021] **FIG. 3** ist ein Blockdiagramm, das die Elemente eines derzeit bevorzugten Netzwerk-Zugangs-Servers zeigt.

[0022] **FIG. 4** ist ein Blockdiagramm, das die Elemente eines bevorzugten Gatekeeper-Dienstes des Netzwerk-Zugangs-Servers aus **FIG. 3** zeigt.

[0023] **FIG. 5** ist ein Blockdiagramm, das die funktionalen Elemente der derzeit bevorzugten verteilten Dienste eines Integrationsbetreibers zeigt.

[0024] **FIG. 6** ist ein Flussdiagramm, das einen übergeordneten Prozessablauf in dem System aus **FIG. 1** zeigt.

[0025] **FIG. 7** ist ein Flussdiagramm, das die Einzelheiten des Herstellens einer Kommunikationsverbindung zwischen einem drahtlosen, mobilen Terminal und einem drahtlosen Zugangspunktgerät zeigt.

[0026] **FIG. 8** ist ein Flussdiagramm, das die Einzelheiten der Authentifizierung und Autorisierung eines drahtlosen, mobilen Terminals zeigt.

[0027] **FIG. 9** ist ein Flussdiagramm, das die Einzelheiten der Verarbeitung von Benutzerprofilen zur Autorisierung des Netzwerkzugangs durch drahtlose, mobile Terminals und zum Zuteilen von Netzwerkressourcen an diese zeigt.

[0028] **FIG. 10** ist ein Flussdiagramm, das die Einzelheiten des Managements von Netzwerksitzungen von drahtlosen, mobilen Terminals und der Durchführung der Netzwerkabrechnung zeigt.

[0029] **FIG. 11** ist ein Flussdiagramm, das die Einzelheiten der Zuweisung von IP-Adressen an autorisierte drahtlose, mobile Terminals zur Ermöglichung von Netzwerkkommunikation zeigt.

[0030] **FIG. 12** ist ein Flussdiagramm, das die Einzelheiten bestimmter Sicherheitsprozeduren einschließlich der Erkennung betrügerischer Netzwerknutzung und unautorisierten Eindringens in das Netzwerk zeigt.

[0031] **FIG. 13** ist ein Blockdiagramm, das eine alternative bevorzugte Systemarchitektur gemäß der Erfindung zeigt.

[0032] **FIG. 14** ist eine grafische Darstellung, die verschiedene Optionen für die Bereitstellung verschlüsselter Netzwerkkommunikation zwischen drahtlosen, mobilen Terminals und verschiedenen Elementen des Systems zeigt.

[0033] **FIG. 15** ist ein Flussdiagramm, das optionale Sprach-/Anrufbearbeitung in dem System zeigt.

[0034] **FIG. 16** ist ein Blockdiagramm, das die Elemente einer alternativen bevorzugten Ausführungsform eines drahtlosen Zugangspunkt-/Netzwerk-Zugangs-Servers zeigt, der Komponenten für drahtlose Telefonie verwendet.

[0035] **FIG. 17** ist ein Blockdiagramm, das die bevorzugten Datenelemente für eine Funktionalität des Netzwerk-Zugangs-Servers als Bandbreiten-Zuteilungs-Manager zeigt.

[0036] **FIG. 18** ist eine grafische Darstellung eines beispielhaften Bandbreitenparameter-Schemas zur Verwendung in Verbindung mit den Datenelementen des in **FIG. 17** gezeigten Bandbreiten-Zuteilungs-Managers.

[0037] **FIG. 19** ist ein Flussdiagramm, das einen bevorzugten Prozess des Bandbreitenzuweisungs-Managements durch den Netzwerk-Zugangs-Server zeigt.

DETAILLIERTE BESCHREIBUNG DER ERFINDUNG

BESCHREIBUNG DER KONKRETEN AUSFÜHRUNGSFORMEN

[0038] Die bevorzugten Ausführungsformen der vorliegenden Erfindung werden nun detailliert unter Bezugnahme auf die Zeichnungen beschrieben, in denen ähnliche Elemente durch dieselben Bezugszeichen identifiziert werden. Die folgende Beschreibung ist beispielhaft und nicht beschränkend.

[0039] Im Allgemeinen basiert die hier verwendete Terminologie für die Funkverbindung auf dem Standard IEEE 802.11b für drahtloses Ethernet. Die hier beschriebenen Prinzipien und Ausführungen sollen jedoch nicht auf ein bestimmtes Kommunikationsprotokoll für drahtlose Netzwerke beschränkt sein, sondern vielmehr ein geeignetes Kommunikationsprotokoll für drahtlose Breitband-Netzwerke nutzen, insbesondere das Wireless-LAN-Protokoll, das durch IEEE 802.11 spezifiziert ist, und das Bluetooth-Protokoll, das kürzlich als IEEE 802.15 verabschiedet wurde.

[0040] **FIG. 1** ein Funktionsblockschaltbild, das ein derzeit bevorzugtes System **100** darstellt, das die Erfindung verkörpert. Der Hauptzweck des Systems **100** besteht darin, den mobilen, drahtlosen Terminals **1** den Zugang zu Netzwerkressourcen bereitzustellen, obwohl es diesen Zugang für feste oder mobile Terminals auch über drahtgebundene Verbindungen bereitstellen kann. Ein mobiles, drahtloses Terminal, wie es hier verwendet wird, kann jedes mobile, drahtlose Terminal sein, das eine MAC-Adresse oder eine andere einzigartige Geräteadresse besitzt, wie beispielsweise ein digitales Mobilfunkendgerät, ein drahtloser PIA oder PDA oder ein Computer mit einem drahtlosen Netzwerkadapter. Andere feste und mobile Terminals, die die von dem System **100** bereitgestellten Dienste nutzen können, schließen Desktop- und Laptop-Computer und dergleichen mit ein, insbesondere wenn das Netzwerk eines Fremdbetreibers besucht und eine Verbindung mit diesem hergestellt wird.

[0041] Das mobile drahtlose Terminal **1** kommuniziert mit dem System **100** direkt über Funkwellen **21** unter Verwendung konventioneller drahtloser Netzwerkkommunikationstechnologie. Alternativ kann, falls zusätzliche Reichweite notwendig

oder gewünscht ist, ein konventioneller Repeater oder eine externe Antenne **2** vorgesehen sein, um Funkwellen **19**, **20** zwischen dem mobilen Terminal **1** und dem System **100** zu senden und zu empfangen.

[**0042**] Das System **100** umfasst im Allgemeinen einen oder mehrere geografisch verteilte Netzwerkzugangspunkte, die in dieser Ausführungsform drahtlose Funkfrequenz-Zugangspunkte („Wireless Access Point", WAP) **3**, **4** sind. Die drahtlosen Zugangspunkte **3**, **4** können konventionelle Geräte sein, die mit drahtlosen Netzwerkadaptern ausgestattet sind, die den IEEE 802.11 Wireless-LAN- oder den Bluetooth-Standard für drahtlose Netzwerkkommunikation enthalten, oder andere Geräte, die eine ähnliche Funktionalität bieten. Beispiele für solche Geräte sind die Produkte Home Wireless Gateway, das von der 3COM Corporation angeboten wird, Spectrum High Rate AP 41X1 Ethernet Access Point von Symbol Technologies sowie Aironet 340 Series Access Points von Cisco Systems.

[**0043**] Das System **100** beinhaltet außerdem vorzugsweise einen oder mehrere Netzwerk-Zugangs-Server (NAS) **7**. Der NAS **7** kann in Software implementiert sein oder in einer Kombination aus Software und Hardware, wie hier im Einzelnen beschrieben. Der NAS **7** ist ein Netzwerk-Zwischenglied, dessen Hauptfunktion es ist, dem mobilen Terminal **1** den Zugang zum öffentlichen Netzwerk zu verschaffen, d.h. dem Internet **16**, unter Inanspruchnahme der öffentlichen Netzwerkverbindungen ansonsten privater Netzwerke, wie beispielsweise des LAN **10**. Der NAS steuert und verwaltet außerdem den Zugang zu diesen privaten Netzwerken durch diese mobilen Terminals **1**. Wie hier im Einzelnen beschrieben, führt der NAS somit die Registrierung, Authentifizierung sowie andere Funktionen aus, die notwendig sind, um den mobilen Terminals den Zugang zum öffentlichen Netzwerk **16** zu verschaffen, während er zugleich den Zugang jener Besucher zum lokalen privaten Netzwerk **10** steuert, dessen Ressourcen für die öffentliche Netzwerkverbindung genutzt werden, um diesen Zugang zu ermöglichen. Der NAS **7** stellt außerdem vorzugsweise Dienste zur Verfügung wie beispielsweise Bandbreiten-Zuteilungs-Management, Servicequalitäts-Management, Abrechnung der Netzwerknutzung, Bereitstellen von Sprach-/Telefonie-Diensten über die Telefonieausrüstung **12**, und andere.

[**0044**] Während nur ein NAS **7** in dem beispielhaften System **100** gezeigt wird, wird der Fachmann verstehen, dass mehrere NAS eingesetzt werden können, um als Schnittstellen zwischen mehreren WAPs **3**, **4** und einem oder mehreren privaten Netzwerken **10** und dem öffentlichen Netzwerk **16** zu fungieren. Ebenso dient es lediglich der Veranschaulichung, dass der WAP **4** ohne ein entsprechendes mobiles Terminal **1** oder einen Repeater/eine Antenne **2**, die mit ihm verbunden sind, gezeigt wird.

[**0045**] Der Fachmann wird verstehen, dass jeder WAP einen drahtlosen Netzwerkzugangspunkt repräsentiert und dass die WAPs an verschiedenen geografischen Orten bereitgestellt werden können, wobei jeder mit seinem eigenen Repeater/seiner eigenen Antenne **2** ausgestattet sein kann, sofern dies gewünscht oder notwendig ist. Somit stellt jeder WAP **3**, **4** einen Punkt für drahtlose Netzwerkverbindung für ein oder mehrere mobile Terminals **1** bereit. Zusätzlich oder alternativ können mehrere WAPs **3**, **4** am selben geografischen Ort bereitgestellt werden, und jeder WAP kann für ein anderes drahtloses Netzwerkprotokoll konfiguriert sein, um mobile Terminals **1** unterschiedlicher Typen und/oder von unterschiedlichen Herstellern aufzunehmen und/oder mit unterschiedlichen privaten Netzwerken zu verknüpfen. Ein WAP **3** kann somit beispielsweise für drahtlose LAN-Kommunikation gemäß dem Standard IEEE 802.11b für drahtloses Ethernet konfiguriert sein, und ein anderer WAP **4** kann für drahtlose Kommunikation gemäß Bluetooth-Standard konfiguriert sein. Alternativ kann ein einzelnes WAP-Gerät so konfiguriert werden, dass es eine Vielzahl unterschiedlicher Netzwerk-Kommunikationsprotokolle unterstützt.

[0046] Der Fachmann wird außerdem verstehen, dass während ein privates LAN **10** in dem beispielhaften System dargestellt ist, eine Vielzahl geografisch verteilter privater Netzwerke ein verteiltes Netzwerk bilden kann, wobei jedes von ihnen mit einem oder mehreren WAPs und einem oder mehreren NAS assoziert ist. Jeder NAS kann mehrere WAPs bedienen, die für dasselbe logische Netzwerk oder Subnetzwerk konfiguriert sind.

[0047] Das System **100** umfasst vorzugsweise außerdem entfernte verteilte Dienste eines Integrationsbetreibers (IODS) **18**. Im Zusammenhang mit dem IODS **18** wird die Bezeichnung „verteilte Dienste" verwendet, da solche Dienste vorzugsweise von einem oder einer Vielzahl von vernetzten Servern bereitgestellt werden, die u.a. eine oder mehrere verbundene verteilte relationale Datenbanken verwenden. Vorzugsweise kommuniziert der IODS **18** entfernt mit den NAS **7** über das öffentliche Netzwerk **16** und jede Anschlussleitung **15** und jeden Router, jedes Modem oder jede andere Netzwerkverbindung **14** am NAS, die beteiligt sind. Die Netzwerkverbindung **14** kann die öffentliche Netzwerkverbindung eines privaten LAN **10** umfassen, mit dem der NAS **7** verbunden ist, oder eine andere Verbindung, die dem NAS **7** zugeordnet ist.

[0048] Im Allgemeinen wird ein mobiles Terminal **1** entweder direkt oder über einen Repeater **2** eine Anfrage zum Herstellen einer Verbindung senden, wenn es in die Funkreichweite eines WAP **3**, **4** kommt. Die WAPs **3**, **4** akzeptieren einfach die Verbindungsanfragen, während der NAS **7** den Netzwerkzugang verwaltet. Sobald eine Kommunikationsverbindung zwischen dem mobilen Terminal **1** und dem WAP **3** hergestellt wurde, fungiert der WAP **3** als Kommunikationsverknüpfung zwischen dem NAS **7** und dem mobilen Terminal **1**. Der NAS **7** hat zunächst die Funktion, das Roaming-Terminal als Teilnehmer zu identifizieren und wenn nötig zu registrieren. Wenn das mobile Terminal **1** versucht, mit dem Netzwerk zu kommunizieren, empfängt der NAS ein Paket aus einer Schicht **3**, in dem die MAC-Adresse des mobilen Terminals enthalten ist. Der NAS schlägt diese Adresse in einer lokalen Datenbank nach, um zu bestimmen, ob es sich bei dem mobilen Terminal um einen registrierten und autorisierten Nutzer handelt. Der NAS **7** kann auch mit dem IODS **18** kommunizieren, um das mobile Terminal **1** zu identifizieren und u.a. seine Autorisierungs- und Netzwerkzugangsparameter zu bestimmen. Der NAS 7 unterhält eine lokale Datenbank, die gemeinsam mit der Datenbank des IODS **18** Daten zu Sicherheit, Abrechnung und ähnliche Daten liefert, um den NAS **7** in die Lage zu versetzen, diese Funktionen zu erfüllen. Falls der NAS beispielsweise die Adresse nicht in seiner lokalen Datenbank findet, kann er eine Anfrage an eine Master-Datenbank senden, die sich im IODS **18** befindet. Beide Datenbanken werden hier detailliert beschrieben.

[0049] Während des anfänglichen Verbindungsprozesses kann eine verschlüsselte Kommunikation zwischen dem mobilen Terminal **1** und dem WAP **3** aufgebaut werden. Falls der WAP **3** mittels Programmierung zugänglich ist oder gesteuert werden kann, kann der NAS **7** den WAP **3** so programmieren, dass dieser Anfragen zum Aufbau einer verschlüsselten Verbindung über eine Schicht **2** (Verbindungsschicht) mit einem besuchenden Terminal **1** akzeptiert. Der WAP **3** beinhaltet daher vorzugsweise eine Netzwerk-Zugangs-Server-Schnittstelle **5** oder wird mit dieser versehen, wodurch der NAS in der Lage ist, mit dem NAP zu kommunizieren und diesen zu programmieren. Die NAS-Schnittstelle **5** ist vorzugsweise in der Lage, Steuerbefehle vom NAS **7** über ein konventionelles einfaches Netzwerk-Management-Protokoll („Simple Network Management Protocol", SNMP) oder ein ähnliches Protokoll zu empfangen. Eine geeignete mittels Programmierung zugängliche Anwendungsprogrammierschnittstelle („Application Programming Interface", API) ist derzeit von Symbol Technologies als SpectrumSoft WNMS 2.0 erhältlich. Da unterschiedliche Hersteller von WAP-Geräten verschlüsselte Kommunikationssitzungen über die Verbindungsschicht auf unterschiedliche Weise handhaben, können einige mobile Terminals, die so konfiguriert sind, dass sie verschlüsselte Sitzungen über die Verbindungsschicht ermöglichen, möglicherweise inkompatibel mit einem bestimmten WAP sein. Um die Kompatibilität zwischen WAPs unterschiedlicher

Hersteller zu erhöhen, ist die erweiterte Service-Set-Identifikation („Extended Service Set ID", ESS ID) (Name der drahtlosen Domain) vorzugsweise für alle Netzwerke, die WAPs enthalten, gleich, z.B. „wan". Wenn ein mobiles Terminal mit einem WAP in seinem Heim-Netzwerk kommuniziert, wird sein drahtloser Netzwerkadapter vorzugsweise so konfiguriert sein, dass er das konventionelle drahtlose Verschlüsselungsprotokoll („Wireless Encryption Protocol", WEP) mit der größtmöglichen Verschlüsselungsstärke nutzt. Wenn sich das mobile Terminal jedoch außerhalb seines eigenen Heim-Netzwerks befindet und eine Kommunikationsverbindung mit dem WAP eines fremden Netzwerks aufbauen will, wird seine WEP-Einstellung vorzugsweise in einen Nicht-Sicherheitsmodus umgeschaltet werden, um eine erfolgreiche Verbindung zu gewährleisten. Die WAPs sollten daher vorzugsweise sowohl Anfragen für verschlüsselte als auch für offene Sitzungen akzeptieren, so dass mobile Terminals, die keine verschlüsselte Sitzung über die Verbindungsschicht aufbauen können, dennoch eine offene Sitzung aufbauen können.

[0050] Sollte sich herausstellen, dass das mobile Terminal **1** vorab festgelegte Kriterien erfüllt und daher für den Netzwerkzugang autorisiert ist, wird der NAS **7** als Zwischenglied zwischen dem mobilen Terminal **1** und der öffentlichen Netzwerkverbindung **14** des verbundenen privaten Netzwerks **10** des NAS fungieren, um es dem mobilen Terminal **1** zu ermöglichen, sich mit dem öffentlichen Netzwerk **16** zu verbinden und darüber zu kommunizieren. Im Allgemeinen wird, wenn die MAC-Adresse des mobilen Terminals beim Betreiber als Teilnehmer registriert ist, der für die Nutzung des Netzwerks autorisiert ist, ein gespeichertes, dem Inhaber der MAC-Adresse entsprechendes Teilnehmerprofil abgerufen, in der lokalen NAS-Datenbank kurzzeitig abgelegt und vom NAS verarbeitet, um die Netzwerkzugangs- und Bandbreitenparameter zu bestimmen, für die der Nutzer autorisiert ist, den zugewiesenen Quality-of-Service-Level (QoS) des Teilnehmers, alle anzuwendenden geltenden Sicherheitsregelwerke, etc. Der NAS initiiert außerdem die Erfassung von Statistiken zu Rechnungsstellungszwecken und initialisiert einen Sitzungseintrag in seiner lokalen Datenbank.

[0051] Außer der Bestätigung, dass das mobile Terminal autorisiert ist und der Zuteilung von Netzwerkressourcen an das Terminal stellt der NAS vorzugsweise weitere Dienste bereit. Er stellt z.B. vorzugsweise sicher, dass jegliche Kommunikation zwischen dem privaten LAN **10** und dem mobilen Terminal **1** angemessen verschlüsselt ist. Der NAS **7** verifiziert somit vorzugsweise, dass die Verschlüsselung vor der Ermöglichung der Weiterleitung zwischen dem Netzwerksegment für den Roaming-Zugang **6** und dem privaten LAN-Netzwerksegment **8** erfolgt ist. Außerdem führt der NAS vorzugsweise Funktionen aus wie beispielsweise die Messung der Netzwerknutzung durch das mobile Terminal zu Abrechnungszwecken sowie die entsprechende Verwaltung und Begrenzung des Zugangs des mobilen Terminals **1** zum privaten Netzwerk **10**. Ferner unterstützt der NAS vorzugsweise die Sprach-/Telefoniekommunikation durch das mobile Terminal. Das mobile Terminal kann beispielsweise einen IP-Telefonie- oder VoIP-Client aktivieren, um es dem Teilnehmer zu ermöglichen, Sprach- oder Videoanrufe über das Netzwerk zu tätigen. Der NAS ist vorzugsweise mit einem Telefonie-Gateway und -Agent ausgestattet, die diesen Zugang unterstützen und die Verbindung über das Netzwerk, eine ISDN-Schnittstelle oder die PSTN-Schnittstelle **11**, **12** ermöglichen, falls der NAS [Satz unvollständig; Anm. d. Übers.].

[0052] Falls sich die MAC-Adresse des mobilen Terminals oder eine andere Geräteadresse weder in der lokalen NAS-Datenbank noch in der IODS-Master-Datenbank befindet, wird dem mobilen Terminal als einziger Netzwerkzugang der Zugang zum NAS erlaubt. In diesem Fall weist der NAS dem mobilen Terminal eine temporäre IP-Adresse unter Verwendung konventioneller DHCP- und/oder DHCP-Relay-Dienste zu, doch jegliche Netzwerkkommunikation durch das mobile Terminal wird an den NAS umgeleitet, der das Angebot macht, den Host als Teilnehmer für das Netzwerk des Integrationsbetreibers zu registrieren, d.h. das Gefüge aus privaten und öffentlichen Netzwerken, die vom Integrationsbetreiber über den IODS und den NAS integriert werden. Der NAS unterhält zu diesem Zweck vorzugsweise

einen HTTP-Server, um eine Registrierungsseite an das mobile Terminal zu kommunizieren. Die Registrierungsseite kann eine einfache HTML-Seite sein, die vom mobilen Terminal Informationen für die Registrierung wie z.B. Kreditkartennummer, Rechnungsname und -adresse etc. anfordert.

[0053] Der Fachmann wird verstehen, dass die Möglichkeit für Nutzer mobiler Terminals, über einen beliebigen von mehreren geografisch verteilten WAPs drahtlos auf das Internet zuzugreifen, während sie sich außerhalb ihres Heim-Netzwerks befinden und die Internetverbindung ansonsten privater Netzwerke nutzen, den Internetzugang stark erweitert, äußerst praktisch ist und außerdem die Produktivität potenziell verbessern kann. Ein besonders vorteilhaftes Merkmal der Erfindung ist, dass diese unter Verwendung bestehender konventioneller mobiler Terminals **1** arbeitet. Zu den mobilen Terminals muss keine spezielle Software hinzugefügt werden außer der, die normalerweise für konventionelle drahtlose Netzwerkkommunikation benötigt wird, um Kommunikationsverbindungen zwischen den WAPs **3**, **4** und dem NAS **7** aufzubauen, wo auch immer diese implementiert sind, und dadurch auf das Internet zuzugreifen.

[0054] Der NAS **7** kann als Stand-Alone-Gerät implementiert oder in einen WAP **3**, **4**, eine Schnittstelle **14** oder beides integriert werden. In den Fällen, in denen das NAS **7**, der WAP **3**, **4** und die Schnittstelle **14** integriert sind, wird in der bevorzugten Ausführungsform ein Universalrechner eingesetzt. In dieser Ausführungsform wird der NAS als Software-Modul oder Subsystem implementiert, das mit den Betriebssystemen UNIX, WINDOWS, LINUX oder einem ähnlichen Betriebssystem zusammenwirkt und unter diesen läuft. Bei dieser Ausführungsform läuft der NAS außerdem vorzugsweise in Abstimmung mit einer geeigneten Firewall, Netzwerkadressübersetzung („Network Address Translation", NAT), HTTP oder eventuell mit Mobile-IP-Softwarekomponenten. Alternativ können einige oder alle dieser allgemein bekannten Software-Elemente in die NAS-Software selbst integriert werden. Der Rechner wird einen drahtlosen Netzwerkadapter haben, der als WAP fungiert, sowie einen zweiten Netzwerkadapter, der sich mit der Anschlussleitung **15** verbindet und als Schnittstelle **14** fungiert. Bei dieser Ausführungsform ist es notwendig, sofern Wireless-LAN als Protokoll für die Kommunikation mit den mobilen Terminals verwendet wird, dass entweder das mobile Terminal so konfiguriert ist, dass es mit dem WAP in einer Peer-to-Peer-Sitzung ad hoc kommuniziert, oder dass ein geeignetes Software-Zugangspunkt-Modul auf dem Rechner zur Verfügung gestellt wird, falls das mobile Terminal mit dem WAP im Infrastruktur-Modus kommunizieren soll. Eine solche Zugangspunkt-Software ist von mehreren Firmen erhältlich, einschließlich des WL300 Wireless LAN Software Access Point, der von Compaq Computer angeboten wird.

[0055] Aktuelle WAP-Geräte von unterschiedlichen Herstellern weisen unterschiedliche Konfigurationen auf. Wenn also der NAS in einem WAP integriert sein soll, kann es somit erforderlich sein, für jeden WAP eine andere Ausführungsform des NAS zu konfigurieren. Diese Ausführungsform hat jedoch den Vorteil, dass kein physikalisches Gerät zwischen dem WAP und der Anschlussleitung **15** eingefügt werden muss.

[0056] Falls der NAS in der Schnittstelle **14** integriert ist, ist er vorzugsweise als Universalrechner mit einem Kabelmodem, einer ISDN- oder DSL-Karte als Netzwerkschnittstelle implementiert. Alternativ kann ein Router verwendet werden, sofern er LDAP oder die Anforderungen anderer Verzeichnisdienste unterstützt. Die andere Netzwerkschnittstelle kann ein drahtloser Adapter, ein Kabelmodem oder eine ISDN-/T-1-Karte sein. Durch das Bereitstellen eines dritten Netzwerkadapters kann diese Ausführungsform ein vollkommen sicheres internes Netzwerk zusätzlich zum drahtlosen Zugang und Uplink zum öffentlichen Netzwerk bieten. Der Vorteil dieser Ausführungsform ist, dass im Wesentlichen alle Netzwerkaktivitäten in einem einzigen Gerät untergebracht sein können.

[0057] Die bevorzugteste Ausführungsform besteht jedoch derzeit darin, das Netzwerk in drei logische Netzwerksegmente aufzugliedern. Bei dieser Ausführung ist der NAS **7** in einen Universalrechner integriert, der drei Netzwerkschnittstellen besitzt. Die erste Netzwerkschnittstelle ist die zum Downlink **6**, der über seinen verbundenen WAP **3**, **4** die Konnektivität zu mobilen Terminals bereitstellt. Die zweite Netzwerkschnittstelle ist die zum Uplink **13**, der die Konnektivität zum Netzwerk mit öffentlichem Zugang, also dem Internet **16** bereitstellt. Die zweite Schnittstelle und der Uplink **13** stellen vorzugsweise einen Datenpfad vom NAS zum Internet bereit, der frei ist von Firewalls oder ähnlichen Mechanismen der Datenbeschränkung, weshalb diese Schnittstelle als DMZ bezeichnet wird. Die dritte Netzwerkschnittstelle **8** verbindet den NAS **7** mit dem privaten Netzwerk, also dem LAN **10**. Diese Verbindung ist vorzugsweise durch einen IP-Filter oder am besten mit einer kompletten Firewall geschützt, um den Zugang des mobilen Terminals **1** zum privaten Netzwerk **10** zu steuern und zu begrenzen bzw. zu verhindern. Der IP-Filter ist vorzugsweise so konfiguriert, dass er die IP-Adressinformation enthält, die notwendig ist, um den mobilen Terminals **1**, die für den Zugang zum privaten LAN **10** autorisiert sind, diesen Zugang über den NAS **7** zu ermöglichen, während unautorisierten mobilen Terminals der Zugang verwehrt wird. Das LAN **10** kann beispielsweise das interne private Firmennetzwerk eines lokalen Ressourcenanbieters sein, also dem Betreiber des Netzwerks, durch welches das mobile Terminal Zugang zum öffentlichen Netzwerk erhält. Der Ressourcenanbieter kann bestimmen, dass der Ressourcenanbieter zusätzlich zum Hosten unbekannter oder fremder mobiler Terminals **1**, die keinen Zugang zum LAN **10** erhalten sollen, außerdem mobile Terminals **1** hostet, die dem Ressourcenanbieter gehören oder für die er aus anderen Gründen bestimmt hat, dass sie Zugang zum LAN **10** erhalten sollen. In diesem Fall kann der IP-Filter oder die Firewall so konfiguriert sein, dass Kommunikationen zu oder von IP-Adressen, die mobilen Terminals entsprechen, die dem Ressourcenanbieter gehören oder anderweitig berechtigt sind, auf das LAN **10** zuzugreifen, der Zugang gewährt wird, während Kommunikationen zu oder von einer unbekannten oder fremden IP-Adresse der Zugang verwehrt wird. Zahlreiche handelsübliche Firewalls und IP-Adressen sind für diesen Zweck geeignet und müssen hier nicht weiter beschrieben werden.

[0058] In der vorhergehenden Implementierung [im Original fälschlicherweise „implantation"; Anm. d. Übers.] kann das LAN **10** auch eine direkte Verbindung **9** zur öffentlichen Netzwerkschnittstelle **14** haben, z.B. eine Router- oder DSL-Verbindung. Dies erlaubt es den eigenen Client-Knoten des LAN oder einem mobilen Terminal-Host, der Zugangsrechte zum LAN **10** hat und über den NAS **7** mit dem LAN **10** verbunden ist, die Steuerung des Zugangs zum öffentlichen Netzwerk durch den NAS zu umgehen und direkt auf das öffentliche Netzwerk **16** zuzugreifen. Dementsprechend ist bei der Netzwerkverbindung **9** vorzugsweise außerdem eine Firewall an der Schnittstelle **14** implementiert.

[0059] Eine alternative bevorzugte Systemarchitektur wird in **FIG. 13** gezeigt. Diese Architektur ist der in **FIG. 1** gezeigten Architektur ähnlich. Der Hauptunterschied besteht darin, dass der NAS **7** keine direkte Netzwerkverbindung mit den WAPs **3**, **4** oder dem privaten Netzwerk **10** hat. Stattdessen wird ein Netzwerk-Hub oder Router **19** zwischen den WAPs **3**, **4** und den Router, das Modem etc. **14** des privaten Netzwerks geschaltet. Der NAS **7** fungiert als weiterer Netzwerkknoten, der mit dem Hub oder Router **19** in demselben Netzwerk oder Subnetzwerk verbunden ist. Bei dieser Architektur kommunizieren die WAPs **3**, **4** mit dem Router, Modem etc. **14** des privaten Netzwerks **10** über den Hub oder Router **19**. Der NAS kommuniziert ebenfalls mit dem privaten Netzwerk **10** über den Hub oder Router **19** und den Router, das Modem etc. **14** des privaten Netzwerks. Der NAS kommuniziert ebenfalls mit den WAPs **3**, **4** über den Hub oder Router **19**. Der NAS kommuniziert weiterhin mit dem IODS **18** über den Router, das Modem etc. **14** des privaten Netzwerks, wie bei der Architektur von **FIG. 1**, obwohl der Hub bzw. Router **19** nun ein Zwischenknoten in diesem Pfad ist. Bei dieser Architektur routet der NAS selbst keine Pakete, sondern stützt sich für diese Funktionalität auf den Hub oder Router. Der NAS hat jedoch vorzugsweise mittels Programmierung Kontrolle über den Hub oder den Router, um Anfragen an den Hub oder

Router zu senden und die SNMP-, ARP- und IP-Filter und deren Bandbreiten-Zuteilungsparameter angemessen zu steuern. Die Funktionalität des NAS, des IODS und des WAP ist ansonsten im Wesentlichen dieselbe wie in Bezug auf **FIG. 1** beschrieben.

[**0060**] Diese Architektur ist insbesondere dann geeignet, wenn es möglicherweise eine relativ große Zahl von Benutzern gibt und/oder unter den Benutzern sowohl Benutzer des öffentlichen als auch des privaten Netzes sind, und es wünschenswert ist, diese getrennt zu halten. In dieser Ausführungsform kann somit beispielsweise Teilnehmern mit öffentlichem Netzwerkzugang, die drahtlose mobile Terminals **1** nutzen, der Zugang zum öffentlichen Netzwerk nur über öffentlich zugängliche WAPs **3**, **4** erlaubt werden. Für diese Benutzer ist der einzige Zugangspunkt zum privaten Netzwerk **10** der durch den netzwerkeigenen Router **14**, der durch den Netzwerkadministrator einfach gesichert wird. Gleichzeitig kann Benutzern/Clients des privaten Netzwerks erlaubt werden, über drahtgebundene Netzwerkverbindungen oder über drahtlose mobile Terminals **23** durch private WAPs **21** auf das private Netzwerk **10** zuzugreifen. Private WAPs werden vorzugsweise an Orten betrieben, die nicht öffentlich zugänglich sind, oder sie sind anderweitig so konfiguriert, dass der Zugang auf autorisierte Clients des privaten Netzwerks **10** beschränkt ist. Diese Benutzer können dann durch den Router **14** des privaten Netzwerks auf das öffentliche Netzwerk zugreifen.

[**0061**] Eine weitere mögliche Ausführungsform des NAS wird in **FIG. 16** gezeigt. In dieser Ausführungsform **1700** ist der NAS in einem drahtlosen Telefon integriert. Bei dieser Ausführungsform sind die NAS-Komponenten, d.h. die Uplink-Netzwerkschnittstelle **1710**, die Downlink-Netzwerkschnittstelle **1720** und die Telefon(PSTN)-Schnittstelle **1730** vorzugsweise alle in einer Aufnahmevorrichtung oder Basisstation für ein Endgerät **1705** integriert. Ein universell programmierbarer Mikroprozessor implementiert vorzugsweise ein Betriebssystem **1740** und Betreibersoftware **1750**, wie beispielsweise verschiedene Anwendungsprogramme, sowie die NAS-Software. Das drahtlose Telefon-Endgerät **1760** ist vorzugsweise als PDA-Gerät implementiert, das einen Bildschirm zum Anzeigen von Daten sowie Eingabetasten zum Eingeben von Telefonnummern und Daten besitzt. Außerdem ist das Endgerät **1760** vorzugsweise batteriebetrieben, und die Aufnahmevorrichtung **1705** mit einer konventionellen elektrischen Verbindung, elektrischen Anschlüssen zum Verbinden des Endgeräts **1760** sowie einer Aufladeschaltung ausgestattet, damit die Aufnahmevorrichtung und das Endgerät verbunden werden können, um das Endgerät ggf. aufzuladen.

[**0062**] Bezugnehmend auf **FIG. 3**, **4** und **15-19** wird die bevorzugte Ausführungsform des NAS **7** ausführlicher beschrieben. **FIG. 3**, **4** und **15-19** zeigen den NAS **7** in der bevorzugten Ausführungsform, in welcher der NAS ein vom WAP **3**, **4** und der Netzwerkschnittstelle **14** separates physikalisches Element ist. Wie zuvor beschrieben, kann der NAS jedoch in einem oder beiden Geräten integriert sein, falls dies gewünscht ist. Auf der untersten Schicht (Medienzugriffs- und Bitübertragungsschicht) beinhaltet der NAS Komponenten, die notwendig sind, um sich physikalisch mit dem Netzwerk zu verbinden. Wie zuvor beschrieben, wird der NAS **7** mindestens zwei konventionelle Netzwerkschnittstellen **21** haben. Eine ist eine Downlink-Schnittstelle für die Kommunikation mit mobilen Terminals **1**. Die andere ist eine Uplink-Schnittstelle zum öffentlichen Netzwerk, d.h. dem Internet. Außerdem ist vorzugsweise eine dritte konventionelle Netzwerkschnittstelle **21** für die Verbindung mit dem privaten Netzwerk **10** vorgesehen. Es sind konventionelle Gerätetreiber **22** in Verbindung mit den Netzwerkschnittstellen **21** vorgesehen, um die Daten aus der Multiplex-/Demultiplex-Schicht **2** (Verbindungsschicht) in Daten der Schicht **3** (Netzwerkschicht) umzuwandeln. Der NAS hat außerdem vorzugsweise eine Schnittstelle **47** mit dem PSTN und einem verbundenen Gerätetreiber **22**. Obwohl die Gerätetreiber **22** in **FIG. 3** der Klarheit halber separat dargestellt sind, wird der Fachmann erkennen, dass diese normalerweise Teil der Netzwerkschnittstellen **21** selbst sind.

[0063] In der nächsten Schicht (Netzwerkschicht) erkennt und verarbeitet der NAS konventionellen paketierten Netzwerkverkehr, indem er das Netzwerk mittels konventioneller TCP-/IP-Adressierung und konventionellem TCP-/IP-Routing durchläuft. Ein konventioneller Netzwerk-Stapel **25** implementiert ein konventionelles Adress-Auflösungs-Protokoll(„Address Resolution Protocol", ARP)-Subsystem **23** und ein Paket-Ablaufplaner-Subsystem **46**, um diese Funktionalität zu bieten. Der Netzwerk-Stapel kann entweder die Standard IP Version 4 oder IP Version 6 beinhalten, obwohl am besten Stapel bereitgestellt werden, die beide Standards unterstützen. Die Standard IP Version 6 kann einige Vorteile im Hinblick auf bestimmte Anwendungen haben, wie beispielsweise IPSec und einige kostenlose VoIP-Anwendungen, die oftmals mit aktueller konventioneller Software für Netzwerkadressübersetzung, die die Standard IP Version 4 beinhalten, nicht besonders gut funktionieren.

[0064] Das ARP-Subsystem **23** empfängt Pakete von den mobilen Terminals **1** über die WAPs **3**, **4**, liest deren MAC-Adressen aus den Headern, damit diese von anderen NAS-Softwarekomponenten verwendet werden können, und legt diese Adressen kurzzeitig ab. Eine solche Software ist konventionell und überall erhältlich. Falls der Software-Quellcode für das ARP **23** erhältlich ist, wird dieser vorzugsweise so modifiziert, dass das ARP **23** alle neu erhaltenen MAC-Adressen an die Gatekeeper-Komponente **24** des NAS übermittelt, die unten beschrieben ist. Falls verfügbar, bietet dies einen Leistungsvorteil, da der Gatekeeper **24** nicht den Mehraufwand betreiben muss, der mit dem Abfragen neuer MAC-Adressen vom ARP-Cache verbunden ist.

[0065] Vorzugsweise verarbeitet ein IP-Filter **26** oder alternativ eine Firewall alle Pakete, die in den NAS gelangen und an das öffentliche oder private Netzwerk gerichtet sind. Wenn ein registriertes mobiles Terminal anhand seiner in der lokalen NAS-Datenbank oder in der IODS-Master-Datenbank aufgefundenen MAC-Adresse authentifiziert wird, wird eine IP-Adresse, die der MAC-Adresse entspricht, explizit aktiviert. Es werden Pakete weitergeleitet, deren IP-Adress-Header Adressen enthalten, die zuvor registrierten und authentifizierten mobilen Terminals entsprechen. Diejenigen, bei denen das nicht der Fall ist, werden vorzugsweise verworfen. Falls eine Filterung anhand der MAC-Adressen verfügbar ist, kann diese statt der oder zusätzlich zur IP-basierten Filterung als Schutz vor Eindringlingen verwendet werden.

[0066] Der NAS implementiert außerdem vorzugsweise eine Reihe von routerbezogenen Diensten **30** auf der Netzwerkschicht. Die Router-Dienste **30** bieten Host-Konfiguration, Netzwerk-Datenerhebung, IP-basiertes Routing, mobiles Roaming und Netzwerk-Management-Funktionen. Die Router-Dienste müssen ICMP Router Discovery Messages (RFC 1256) und andere standardmäßige Router-Anforderungen unterstützen, die in den veröffentlichten Standards IETF RFC 1812 und IP Version 6 RFC 2460 spezifiziert sind. Die routerbezogenen Dienste des NAS beinhalten vorzugsweise Netzwerkadressübersetzung **27**, Erhebung von Netzwerkstatistikdaten **29**, DHCP-/DHCP-Relay-Dienste **31**, Verschlüsselungs-/Entschlüsselungs-Dienste **32**, Mobile-IP-Unterstützung **33** sowie SNMP-Netzwerk-Management-Dienste **41**.

[0067] Konventionelle Software für Netzwerkadressübersetzung (NAT) **27** liefert bei Bedarf dynamisch routingfähige IP-Adressen für registrierte, authentifizierte mobile Terminals. Die NAT **27** ist möglicherweise nicht erforderlich, wenn ein Ressourcenanbieter genügend IP-Adressen zur Verfügung hat, um besuchende mobile Terminals sowie lokale Benutzer zu versorgen. Dies ist jedoch normalerweise nicht der Fall.

[0068] Die Komponente für die Erhebung der Netzwerkstatistikdaten **29** speichert vorzugsweise eine Zählung aller Bits, die von den IP-/MAC-Adressen, die jedem registrierten, authentifizierten mobilen Terminal entsprechen, das auf das Netzwerk

zugreift, gesendet und empfangen wurden. Wenn eine IP-Adresse einem registrierten, authentifizierten mobilen Terminal zugeteilt wird, initialisiert der NAS vorzugsweise einen mit einem Zeitstempel versehenen Eintrag in seiner lokalen Datenbank. Sobald eine Sitzung abgeschlossen ist und die Verbindung durch das mobile Terminal getrennt wurde, aktualisiert der NAS den Eintrag mit einem weiteren Zeitstempel. Der Eintrag wird vorzugsweise außerdem um die Gesamtzahl von Bits ergänzt, die während der Sitzung gesendet und empfangen wurden, sowie um etwaige Weiterübertragungen. Diese Information wird beim NAS kurzzeitig abgelegt, und der NAS lädt diese Einträge periodisch auf dem IODS **18** über das öffentliche Netzwerk hoch. Diese Information ist hilfreich für Abrechnungs- und Rechnungsstellungszwecke, wie beispielsweise um Teilnehmern die Möglichkeit zu geben, ihre Rechnungen zu überprüfen sowie Umsätze lokalen Dienstanbietern zuzuordnen, falls dies gewünscht ist. Es ist eine Reihe konventioneller Softwarelösungen erhältlich, um die Funktionalität der Erhebung von Netzwerkstatistikdaten auszuführen. Die Betriebssysteme MicroSoft Windows NT und Windows 2000 stellen beispielsweise beide eine Performance-Monitor-API zur Verfügung, die solche Informationen mittels Programmierung sammeln kann. Es existieren ähnliche APIs für andere geeignete Betriebssysteme, die die Bildung von Netzwerken unterstützen.

[0069] Die Komponente DHCP-/DHCP-Relay-Agent **31** stellt vorzugsweise entweder dynamisch eine Host-IP-Konfiguration im NAS selbst zur Verfügung oder fungiert als Übertragungsagent zu einem externen DHCP-Server für solch eine Konfiguration. Vorzugsweise konfiguriert das DHCP mindestens zwei Subnetzwerke. Eines davon ist ein nicht vertrauenswürdiges oder unsicheres Netzwerk für öffentlichen Zugang. Das andere ist ein sicheres Netzwerk für ausschließlich privaten Zugang. Das DHCP **31** würde beispielsweise ein unsicheres Subnetzwerk 10.0.X.X und ein sicheres Subnetzwerk 10.0.Y.Y einrichten. Autorisierte Benutzer des privaten Netzwerks **10** würden das sichere Subnetzwerk benutzen, um auf das private Netzwerk zuzugreifen, welches sich vorzugsweise hinter einer Firewall befindet. Das passende Subnetzwerk wird jedem mobilen Terminal vom NAS zugewiesen anhand der Feststellung durch den NAS, ob der Teilnehmer mit dem mobilen Terminal ein autorisierter Client des privaten Netzwerks **10** ist oder ein Teilnehmer, der ausschließlich Zugang zum öffentlichen Netzwerk hat. Eine angemessene Unterscheidung zwischen Clients des privaten Netzwerks und Teilnehmern mit ausschließlich öffentlichem Zugang kann erreicht werden, indem zuvor abgestimmte Adressreservierungen im DHCP für bestimmte Geräteadressen mobiler Terminals eingerichtet und verwaltet werden, oder alternativ indem der DHCP-Server so eingerichtet wird, dass ihm der programmierte Zugriff auf Adress-Tabellen des Netzwerkadapters im mobilen Terminal im NAS erlaubt wird. In der bevorzugten Ausführungsform kommt ein DHCP-Relay statt des Betriebs eines DHCP-Servers als Bestandteil des NAS selbst zum Einsatz. Die Verwendung eines DHCP-Agenten vermeidet Skalierungsprobleme, die auftreten können, wenn die DHCP-Parameter verändert werden. Alternativ können Skalierungsprobleme aber auch durch eine verteilte Datenbank vermieden werden. Die bevorzugte Anordnung der Komponente DHCP/DHCP-Agent setzt voraus, dass das Netzwerk der Standard IP Version 4 entspricht. Eine ähnliche Anordnung kann für Netzwerke der IP Version 6 implementiert werden, außer dass in diesem Fall keine privaten Internetprotokolle verwendet werden müssen und die IP-Adressen anhand der vom NAS zur Verfügung gestellten Informationen selbst konfiguriert werden, wie im Standard IETF RFC für IP Version 6 spezifiziert.

[0070] Die Verschlüsselungs-/Entschlüsselungs-Komponente **32** umfasst vorzugsweise Einrichtungen, um Authentifizierungen durchzuführen und eine verschlüsselte Kommunikation zwischen dem NAS und mobilen Terminals sicherzustellen, falls vorhanden, sowie zwischen dem NAS und dem IODS, insbesondere für die Übertragung vertraulicher und sensibler Daten, wie beispielsweise Abrechnungsdaten. Die bevorzugte Implementierung verwendet ein konventionelles Internetsicherheitsprotokoll (IPSec) und eine konventionelle Authentifizierungs-/Verschlüsselungs-/Entschlüsselungseinrichtung oder ISAKMP/IKE, die mit einem konventionellen digitalen PKI-Zertifizierungsdienst

arbeiten. Alternativ kann auch das SSL-Protokoll verwendet werden. Wie dem Fachmann bekannt ist, wird das IPSec vorzugsweise im Tunnelmodus betrieben, um einen sicheren Kommunikationstunnel zwischen dem NAS und dem IODS zu schaffen, wodurch ein virtuelles privates Netzwerk (VPN) gebildet wird und die zwischen dem NAS und dem IODS übertragenen Daten gekapselt werden. Die ISAKMP/IKE-Einrichtung ermöglicht die gegenseitige Authentifizierung zwischen dem NAS und dem IODS sowie das Aushandeln einvernehmlicher kryptografischer Algorithmen und Schlüssel, um die Verschlüsselung und Entschlüsselung der gesendeten bzw. empfangenen Daten zu ermöglichen. SSL bietet eine ähnliche Funktionalität. Kryptografische Zertifikate und Schlüssel sind passend über einen konventionellen Zertifizierungsdienst sowie viele private und kommerziellen Quellen erhältlich, die im Stand der Technik bekannt sind. Der IPSec-Tunnel kann auch verwendet werden, um Datenverkehr von einem mobilen Terminal durch das Netzwerk entweder an das Betreiber-Netzwerk-Gateway, das sich am nächsten zum endgültigen Zielort befindet (Betrieb des IPSec im Tunnelmodus), oder den endgültigen Zielort selbst zu senden (Betrieb des IPSec im Transportmodus). Wie hier beschrieben, wird vorzugsweise ein im Wesentlichen identischer Satz von Einrichtungen als Teil des IODS bereitgestellt.

[**0071**] Die Komponente Mobile-IP **33** des NAS unterstützt vorzugsweise mobile Terminals, welche die Mobile-IP-Standards verkörpern, die in dem veröffentlichten Standard IETF RFC 2002, Mobile-IP Version 4 spezifiziert sind. Die Unterstützung von Mobile-IP Version 4 bietet die Möglichkeit, eine Sitzung mit einem passend ausgestatteten mobilen Terminal aufrecht zu erhalten, obwohl das mobile Terminal seinen Verbindungspunkt zum Netzwerk verändert. Wenn also Mobile-IP Version 4 unterstützt wird, kann ein mobiles Terminal somit weiterhin mit dem Netzwerk kommunizieren, obwohl seine Netzwerkverbindung während der Sitzung von einem NAS zu einem anderen übergeht. NAS, die Mobile-IP gemäß den Standards von Mobile-IP Version 4 unterstützen, berechnen die Übergabe der Netzwerkverbindung des mobilen Terminals an ein anderes Terminal sowie die Umleitung von Paketen zum und vom mobilen Terminal und einen „Korrespondenz-Knoten" über das Netzwerk.

[**0072**] Die Komponente Einfaches Netzwerk-Management-Protokoll (Simple Network Management Protocol, SNMP) **41** umfasst eine konventionelle SNMP-Netzwerkprotokoll-Schnittstelle. Der NAS verwendet vorzugsweise das SNMP-Protokoll, um die WAPs programmiert zu steuern und Sicherheitswarnungen, Fehlermeldungen und andere Netzwerksteuerungs- und Netzwerk-Management-Meldungen zwischen den verschiedenen Komponenten des NAS und IODS über das Netzwerk zu übermitteln.

[**0073**] In der nächsten Schicht beinhaltet der NAS vorzugsweise Zugangssteuerungsdienste. Die Zugangssteuerungsdienste beinhalten vorzugsweise einen Alt-AAA-Dienst für Authentifzierung, Autorisierung und Abrechnung **40** sowie eine Zugangssteuerungs-Komponente **42**.

[**0074**] Der AAA-Dienst **40** ist eine optionale Komponente, die vorzugsweise vorgesehen ist, um mobile Terminals aufzunehmen, die für Pre-IPSec-Radius- (veröffentlicht als IETF RFCs 2165 und 2865) oder Pre-IPSec-Diameter-Netzwerkauthentifizierungs- und Netzwerkzugangskontrollstandards und/oder -dienste ausgerüstet sind. Für diese mobilen Terminals ist vorzugsweise der Radius- bzw. Diameter-Dienst aktiviert, um ihnen den Zugang zum Netzwerk zu erlauben und die Möglichkeit zu geben, an sicherheitsverschlüsselten Sitzungen teilzunehmen.

[**0075**] Die Zugangssteuerungs-Komponente **42** beinhaltet vorzugsweise eine Liste von Netzwerkbenutzern, die Kontrollzugriff haben, um als Systemadministrator zu fungieren. Die Liste wird normalerweise vom Ressourcenanbieter bei der Konfiguration des NAS erstellt werden. Der Kreis typischer Benutzer, die Kontrollzugriff haben, wäre beschränkt auf

den Ressourcenanbieter und den Integrationsbetreiber sowie deren Vertreter. Diese Komponente wird normalerweise und vorzugsweise vom Betriebssystem implementiert. In Windows NT basiert sie z.B. auf dem Sicherheitsverwaltungssystem („Security Account Manager", SAM).

[**0076**] In der Anwendungsschicht stellt der NAS vorzugsweise Datenbank-Dienste, Netzwerkzugangspunkt-Steuerungsdienste, Web-Dienste sowie Telefon-Dienste zur Verfügung. Von größter Bedeutung ist möglicherweise, dass der NAS in dieser Schicht außerdem einen Gatekeeper **24** implementiert, der als eine Art Master-Prozessregler fungiert.

[**0077**] Die Datenbank-Dienste werden von der lokalen Datenbank **45** des NAS bereitgestellt, die eine Replikation von Teilen der IODS-Master-Datenbank ist, einem Verzeichnis-Agent-/Location-Server **34**, einem Cache **44**, einem Dienstagent **43** sowie einem LDAP-Server **38**.

[**0078**] Die lokale NAS-Datenbank **45** speichert vorzugsweise eine Kopie der IODS-Master-Datenbank, wie in **FIG. 2** gezeigt. Vorzugsweise werden jedoch normalerweise nur Einträge für die Heimbenutzer des Ressourcenanbieters, d.h. private Netzwerkkunden, sowie Daten, die das Netzwerk des Ressourcenanbieters betreffen, in der lokalen Datenbank gespeichert. Der Fachmann kann eine beliebige Anzahl von Synchronisierungs- und Replikationsschemata zwischen der IODS-Master-Datenbank und der lokalen NAS-Datenbank zum Speichern von Informationen über besuchende mobile Terminals konstruieren, oder Terminals, die das Netzwerk vor Kurzem besucht haben oder sich im Gebiet des NAS befinden. Sofern der lokale NAS genügend Netzwerkressourcen hat und ausreichend Bandbreite verfügbar ist, könnte er versuchen, die Synchronisation mit einem oder mehreren der in **FIG. 2** gezeigten Datensätze aufrecht zu erhalten, insbesondere den Teilnehmer- und Adapter-Tabellen. Es ist möglich, aber unwahrscheinlich, dass es für den Ressourcenanbieter notwendig sein wird oder er den Wunsch haben wird, die Informationen des Sitzungseintrags und des Abrechnungseintrags zu synchronisieren, und bei einigen Ausführungen könnte der IODS solche Informationen möglicherweise sogar sperren und deren Herunterladen auf die lokale NAS-Datenbank aus Sicherheitsgründen verhindern.

[**0079**] Der Verzeichnisagent/Location Service **34** ist eine Standardkomponente des konventionellen Service Location Protocol, das als IETF RFC 2608 veröffentlicht wurde. Dieser Dienst gibt die Information über Netzwerkressourcen an Benutzer zurück, die eine Anfrage senden. Es ist notwendig, den Internet Location Server (ILS) der Parteien und die Information aus dem Session Initiation Protocol (SIP) zu lokalisieren.

[**0080**] Der Cache **44** ist vorzugsweise ein konventioneller Cache, der von den Komponenten des NAS verwendet wird, um Informationen bezüglich mobiler Terminals zu speichern und abzurufen, die mit dem Netzwerk verbunden sind oder sich damit verbinden. Solche Informationen beinhalten vorzugsweise die Dienststufenvereinbarung des Teilnehmers sowie die Geräte-Adressinformation. Der NAS aktualisiert vorzugsweise seine lokale Datenbank **45** periodisch aus dem Cache und aktualisiert die IODS-Master-Datenbank.

[**0081**] Der Dienstagent **43** fungiert als Schnittstelle zwischen dem Verzeichnisagent **34** und dem Dienstanforderer, wie im Standard IETF RFC 2608 spezifiziert.

[**0082**] Der LDAP-Server **38** ist ein konventioneller Server, der als Zwischenglied zwischen Netzwerk-Clients fungiert, z.B. in diesem Fall einem mobilen Terminal und einem LDAP-Verzeichnis oder einer LDAP-Datenbank von Netzwerkressourcen. Ein konventionelles LDAP-Verzeichnis enthält normalerweise E-Mail-Kontaktinformationen für Netzwerkkunden sowie die Identität und den Ort von Netzwerk-Diensten und -Geräten. In der vorliegenden bevorzugten

Ausführungsform wird diese Information vorzugsweise vom IODS in die lokale Kopie des NAS kopiert. Außerdem wird vorzugsweise der gesamte Datensatz des Ressourcenanbieters bei der Konfiguration des NAS vom Ressourcenanbieter bereitgestellt. Vorzugsweise ist ein Verarbeitungsserver für Datenbankabfragen vorgesehen, um Zugriff auf die Daten und deren Änderung durch den Ressourcenanbieter und/oder Integrationsbetreiber zu erlauben. Die LDAP-Datenbank sollte die Adapter-, die Teilnehmer- und die Ressourcenanbieter-Tabelle enthalten, die in der IODS-Datenbank in **FIG. 2** identifiziert sind. Sie kann außerdem die Sitzungs- und Rechnungseinträge aus der IODS-Datenbank enthalten. Falls gewünscht, können die Sitzungs- und Rechnungseinträge von einem zweiten Verarbeitungsserver für Datenbankabfragen verarbeitet werden, der diese an dieselbe Datenbank weitergibt, möglicherweise unter Verwendung eines anderen Datenschemas. Die LDAP-Datenbank **38** enthält außerdem vorzugsweise mindestens die folgende Zusatzinformation:

[0083] 1. Die Messaufzeichnungen, die von der Komponente zur Erhebung von Netzwerkstatistikdaten **29** erzeugt wurden;

[0084] 2. Bandbreiten-Zuteilungsparameter für besuchende mobile Terminals;

[0085] 3. Kryptografische Schlüssel des Integrationsbetreibers und von Benutzern, die verschlüsselte Netzwerkkommunikation verwenden werden;

[0086] 4. IP-Adresse des IODS.

[0087] 5. Abrechnungseinträge für Sprachanrufe, z.B. Anrufer-Identifikation, angerufene Telefonnummer sowie Länge des Anrufs.

[0088] 6. DHCP-Konfigurationsinformation (optional);

[0089] 7. IP-Filterparameter (optional);

[0090] 8. Zeiger zur Version des öffentlichen Schlüssels, der für die Verschlüsselung von Einträgen verwendet wird (vorzugsweise ist die Datenbank mit dem öffentlichen Verschlüsselungsschlüssel des Betreibers verschlüsselt).

[0091] Die Datenelemente 1, 5 und 8 werden vorzugsweise von den IODS-Subsystemen geschrieben, die in **FIG. 2** dargestellt sind. Die Datenelemente 2, 4, 6 und 7 werden vorzugsweise vom Ressourcenanbieter konfiguriert. Das Datenelement 1 liefert die Basisinformation, die die Grundlage für nutzungsbasierte Rechnungsstellung bildet. Das Datenelement 2 liefert die Bandbreite, auf welcher das QoS-Management basiert, wie hier im Einzelnen beschrieben. Das Datenelement 3 wird von der zentralen IODS-Datenbank aus geschrieben und enthält die öffentlichen Verschlüsselungsschlüssel des Integrationsbetreibers und der Teilnehmer, die an sicheren Sitzungen über das Netzwerk teilnehmen werden. Das Datenelement 4 stellt die logische Netzwerkverbindung/-adresse für den IODS bereit, um die Kommunikation des NAS mit dem IODS über das Netzwerk zu ermöglichen. Das Datenelement 5 ist im Wesentlichen dieselbe Information für die Abrechnung von Anrufen **3950**, die in **FIG. 2** dargestellt ist und hier im Einzelnen beschrieben wird. Das Datenelement 6 stellt die DHCP-Konfiguration aus Datenbankparametern bereit. Das Datenelement 7 stellt die IP-Filter-Adressinformation für die IP-Filterung bereit, um den Zugang zu dem privaten Netzwerk zu beschränken.

[0092] Die Netzwerkzugangspunkt-Steuerungsdienste werden vorzugsweise von einer Management-Schnittstelle für den drahtlosen Zugangspunkt **36** bereitgestellt, z.B. einer programmierten Schnittstelle mit den WAPs **3**, **4**. Die Management-Schnittstelle für den drahtlosen Zugangspunkt **36** stellt eine optionale Schnittstelle bereit, um die Verschlüsselung der Funkverbindung (Verschlüsselung der Verbindungsschicht) für Benutzer mobiler Terminals, die Roaming betreiben, zu

ermöglichen. Vorzugsweise wird dies durch die Verwendung von SNMP erreicht, um die WAPs über eine programmierbare API wie hier beschrieben mittels Programmierung zu steuern. Der bevorzugte Betrieb eines solchen Subsystems ist in **FIG. 7** detailliert dargestellt.

[**0093**] Die Web-Dienste **37** werden von HTTP- und HTTPS-Servern bereitgestellt. Der HTTPS-Server stellt einen sicheren SSL-HTTP-Server bereit. Der HTTPS-Server hat zwei Funktionen: erstens, dem Ressourcenanbieter die Administration des NAS zu erlauben, und zweitens, die Registrierung besuchender mobiler Terminals zu ermöglichen. Diese Funktionen sind in **FIG. 8** detailliert dargestellt. Der Ressourcenanbieter wird vorzugsweise über den HTTPS-Server auf den NAS zugreifen, um (1) das Regelwerk für den öffentlichen Netzwerkzugang zu konfigurieren, wie in den **FIG. 18-20** gezeigt; (2) den Umfang des DHCP so zu konfigurieren, dass ein Pool bzw. Pools verfügbarer IP-Adressen konfiguriert werden; (3) die Firewall und/oder den IP-Filter falls nötig zu modifizieren; und (4) Rechnungsdaten einzusehen. Bezüglich der Registrierung wird jedes mobile Terminal, das versucht, auf das Netzwerk zuzugreifen und sich nicht vorab registriert hat und authentifiziert wurde, vom NAS unter Verwendung des HTTP-Servers zu einer Registrierungsseite weitergeleitet.

[**0094**] Die Telefonie-Dienste werden von einem Telefonie-Gateway-Routing-Server **35**, einem lokalen Telefonie-Gateway **39** und einem Anrufanfragen-Server **43** bereitgestellt. Die Einzelheiten der Verarbeitung der Echtzeit-Kommunikation sind in den **FIG. 15** und **16** dargestellt. Im Allgemeinen akzeptiert jedoch der Anrufanfragen-Server **43** IP-Telefonie-Anfragen von mobilen Terminals und verarbeitet diese, z.B. VoIP-Anfragen. Das Anrufanfragen-Gateway **43** verwendet den Telefonie-Gateway-Routing-Server **35**, um die IP-Telefonanrufe über das Netzwerk über ein passendes Telefonie-Gateway zu routen, je nach Kostenerwägungen und Netzwerkbedingungen. Der Server **35** kann beispielsweise einen Anruf für Ende-zu-Ende-Kommunikation über das Netzwerk unter Verwendung von IP-Routing übermitteln, falls der beabsichtigte Korrespondenz-Knoten IP-Telefonie unterstützt und die Netzwerkbedingungen förderlich für Sprachkommunikation sind. Alternativ kann der Server **35**, falls der beabsichtigte Korrespondent IP-Telefonie nicht unterstützt, einen Anruf an das lokale Telefonie-Gateway **39**, ein entferntes Telefonie-Gateway oder das PSTN senden, je nach Kosten und vorherrschenden Netzwerkbedingungen. Der Server **35** verwendet vorzugsweise das Session Initiation Protocol (SIP), wie in IETF RFC 2543 veröffentlicht, zusammen mit Erweiterungen für Schnittstellen mit dem PSTN, veröffentlicht in IETF RFC 2848. Alternativ kann der Server **35** den Standard ITU H.323 implementieren, zusammen mit einer JAIN- oder PARLAY-konformen Internet-/PSTN-API. Viele IP-Telefonie-Anbieter einschließlich Lucent unterstützen sowohl SIP als auch H.323,.

[**0095**] Das lokale Telefonie-Gateway **39** hat außerdem vorzugsweise eine geeignete API, wie beispielsweise die Telefonie-API von Microsoft (TAPI), die H.323- oder andere standardmäßige Telefonie-Signale für die Übertragung über PSTN konvertiert, sowie eine PSTN-Hardware-Schnittstellenkarte wie beispielsweise eine Sprachmodem- oder Multiport-VoIP-Gateway-Karte. Vorzugsweise ermöglichen solche Geräte bidirektionales Routing von Anrufen. Ein geeignetes Produkt für diesen Zweck ist das Dialogic D/41ESC 4 Port SCSA Voice Processing Board. WebSwitch, erhältlich von L.M. Ericsson, könnte ebenfalls geeignet sein.

[**0096**] Der Master-Steuerungsprozess des NAS wird als Gatekeeper **24** bezeichnet. Der Gatekeeper **24** stellt eine zentrale Prozesssteuerung für die NAS-Komponenten bereit, einschließlich des Versendens von Steuerungsnachrichten an verschiedene Prozesse und Software-Komponenten, wie beispielsweise den IP-Filter **26** und die lokale Datenbank des NAS **45**, die, wie hier beschrieben, vorzugsweise eine Teilmenge der in **FIG. 2** gezeigten IODS-Master-Datenbank umfasst, die durch LDAP-Replikation (LDUP) erstellt wird. Unter anderem empfängt der Gatekeeper **24** vorzugsweise

periodische Benachrichtigungen vom ARP **23**, dass eine neue MAC-Adresse empfangen wurde, d.h. dass ein neues mobiles Terminal eine Kommunikationsverbindung mit einem WAP aufgebaut hat. Der Gatekeeper leitet dann diese Information über die APIs an andere NAS-Komponenten weiter, die bestimmte Funktionen ausführen, die unten detailliert beschrieben sind. Wenn jedoch, wie zuvor erwähnt, der ARP **23** nicht in der Lage ist, MAC-Adressen an den Gatekeeper **24** weiterzuleiten, wird der Gatekeeper **24** periodisch die Inhalte des Cache des ARP abrufen und bestimmen, ob neue MAC-Adressen empfangen worden sind. Alle Pakete, die von mobilen Terminals gesendet werden, deren IP-Adressen weder in der lokalen Datenbank des NAS **45** noch in der IODS-Master-Datenbank **3000** vorhanden sind, werden vorzugsweise durch die Betrugserkennungs-Verarbeitungsroutine verarbeitet, die hier beschrieben ist, und dann vom ARP und dem Gatekeeper verworfen bzw. ignoriert.

[**0097**] Der Gatekeeper **24** steuert außerdem vorzugsweise die QoS-Funktionalität des Netzwerks. Zu diesem Zweck beinhaltet der Gatekeeper **24** vorzugsweise einen Bandbreiten-Zuteilungs-Manager („Bandwidth Allocation Manager", BAM) **28**. Der BAM fungiert im Wesentlichen als Schicht zwischen einem bestehenden QoS-System, von dem viele allgemein bekannt sind, und dem Gatekeeper, um die Priorisierungsfunktionen des bestehenden QoS-Systems zu verbessern. Der BAM implementiert vorzugsweise Regelwerke des Ressourcenanbieters für die Nutzung und Zuteilung von Bandbreite durch Teilnehmer und private Netzwerkkunden, einschließlich der Beschränkung der Bandbreite, die allen Teilnehmern mit öffentlichem Zugang und privaten Netzwerkkunden zur Verfügung steht. Der BAM verwaltet außerdem vorzugsweise Warteschlangen zwischen Teilnehmern mit öffentlichem Zugang, d.h. registrierten, authentifizierten mobilen Terminals, die gleiche Prioritäten für Netzwerkressourcen etc. haben. Der BAM kann diese Funktionen ausführen, indem er die passenden Funktionen und Routinen aufruft, die in den Bibliotheken enthalten sind, die normalerweise durch die QoS-Dienste des Betriebssystems zur Verfügung gestellt werden, wie beispielsweise die generischen QoS-Bibliotheken, die in der Windows-Sockets-API vorhanden sind. Alternativ kann ein kommerzieller Bandbreiten-Manager verwendet werden. Ein kommerzieller Bandbreiten-Manager ist von Emerging Technologies unter dem Produktnamen Bandwidth Manager erhältlich. Der Bandbreiten-Manager kann auch auf dem RSVP von Cisco System oder ähnlichen Softwareprodukten basieren, die ohne Weiteres von anderen Anbietern von Produkten für Remote-Netzwerkzugang erhältlich sind, oder auf dem IETF-Standard für verteilte Dienste, DIFFSERV, wie in den IETF RFCs 2475, 2983 und damit verbundenen RFCs veröffentlicht.

[**0098**] In **FIG. 4** sind die Komponenten und die Funktionalität des bevorzugten Gatekeepers **24** ausführlicher dargestellt. Wie ausgeführt, umfasst der Gatekeeper **24** den Master-Steuerungsprozess für den NAS. Er speichert den Sitzungsstatus jedes erkannten mobilen Terminals im Netzwerk, überwacht die Uplink-Ressourcen und führt damit verbundene Aktionen aus. Der Gatekeeper-Master-Steuerungsprozess arbeitet in drei bevorzugten Modi: dem Betreiberstammberechtigungsprozessmodus **423** („Betreibermodus"), dem Teilnehmerstammberechtigungsprozessmodus **424** („Teilnehmermodus") und dem Ressourcenanbieterstammberechtigungsprozessmodus **425** („Anbietermodus"). Um beispielsweise die Bandbreite zu steuern, die besuchenden mobilen Terminals zugeteilt ist, ist administrativer Zugang zu dem Uplink-Port des Ressourcenanbieters erforderlich. Da jedoch in vielen Fällen, z.B. bei einem Firmennetzwerk, der Ressourcenanbieter nicht wollen wird, dass der Integrationsbetreiber Zugriff auf seine Routing-Tabellen oder Bandbreiten-Zuteilungseinrichtungen hat, werden solche Aktionen vorzugsweise im Anbietermodus ablaufen. Andere Funktionen, wie beispielsweise das Aktualisieren von Rechnungsstellungs- und Abrechnungsinformationen, könnten dem Ressourcenanbieter nicht zugänglich sein und werden deshalb vorzugsweise im Betreibermodus laufen. Weitere Funktionen könnten im Teilnehmermodus laufen.

[0099] Es gibt eine Reihe von Datenstrukturen **402** innerhalb des bevorzugten Gatekeeper-Master-Steuerungsprozesses. Diese beinhalten vorzugsweise die Host-Klassen-Datenstruktur **403** und die Ressourcen-Klassen-Datenstruktur **426**. In diesem Dokument bezieht sich der Begriff „Host" auf mobile Terminals im Netzwerk, und die Host-Klassen-Datenstruktur **403** speichert Daten zu jedem mobilen Terminal im Netzwerk. Die Host-Klassen-Datenstruktur **403** beinhaltet eine Anzahl von Datenelementen, die dem Status und den Attributen jedes dieser mobilen Terminals entsprechen. Diese beinhalten einen Inaktivitätszähler **404**, eine Host-Hardware-Adresse **405**, ein Host-Prioritätsregelwerk **406**, ein Host-Kreditlimit **407**, ein Host-IP **408** und einen Host-Status **433**. Der Host-Status **433** enthält Flags für alle kritischen Status, wie beispielsweise den Authentifizierungsstatus **434**, den Filteraktualisierungsstatus **435** und den Sitzungsstatus **436**. Der Status dieser Flags wird verwendet, um die Steuerung zwischen den verschiedenen Software-Routinen auszuführen, welche die Hauptfunktionen des Gatekeepers darstellen, wie unten detailliert in Verbindung mit den **FIG. 6-12** beschrieben. Die Ressourcen-Klassen-Datenstruktur **426** enthält Daten, die sich auf den Status und die Attribute des Gutes des Ressourcenanbieters, also der Netzwerkbandbreite, beziehen. Die Ressourcen-Klassen-Datenstruktur **426** enthält Datenelemente für den prozentualen Anteil der verwendeten Netzwerkbandbreite **427**, den prozentualen Anteil der Netzwerkbandbreite, die dem internen bzw. dem privaten Netzwerkverkehr zugeteilt ist **428**, den prozentualen Anteil der Netzwerkbandbreite, die dem öffentlichen Verkehr bzw. dem Teilnehmerverkehr zugeteilt ist **429**, sowie Bandbreiten-Zuteilungs-Regelwerke **430**, die im Wesentlichen die Information zu Bandbreiten-Regelwerken in der Regelwerk-Tabelle **3650** der IODS-Master-Datenbank **3000** aus **FIG. 2** widerspiegeln.

[0100] Der Gatekeeper **24** umfasst außerdem vorzugsweise eine Reihe funktionaler Komponenten **409**, die Host-Sitzungen initiieren, aufrechterhalten, modifizieren, verarbeiten und beenden. Der Gatekeeper beinhaltet vorzugsweise eine Funktion **416**, die Anrufe an andere NAS-Subsysteme und -Komponenten über eine SNMP-Schnittstelle **410** weiterleitet, eine Funktion **417** zum Aufrufen des TCP-/IP-Stapels im Kernel des Betriebssystems über ein TCP-/IP-Schnittstellen-Protokoll **411**, wie beispielsweise eine Anschlussdosen-Funktion, die von einer Reihe von Anbietern angeboten wird, sowie eine Funktion **418** zum Aufrufen des Treibers der Netzwerkschicht **2**, z.B. NDIS, über die Ethernet-Schnittstelle **412**. Der Gatekeeper beinhaltet außerdem vorzugsweise eine Funktion **432** für die Verschlüsselung und Entschlüsselung von Daten sowie für Operationen mittels öffentlicher Schlüssel über eine Verschlüsselungs-Schnittstelle **431**, wie beispielsweise die GSS-API, eine Funktion **419** zum Aufrufen der lokalen NAS-Datenbank unter Verwendung einer Datenbank-Schnittstelle **432**, wie beispielsweise einer LDAP-API, eine Funktion **420** zum Managen der Netzwerk-QoS **413** über den BAM, eine Funktion **421** zum Aufrufen von IP-Telefonie-Diensten unter Verwendung einer IP-Telefonie-Schnittstelle **414**, wie beispielsweise TAPI- und SIP-APIs, sowie eine Funktion **422** zum Managen von WAPs über eine Basisstation-Management-Schnittstelle **415** wie beispielsweise die SET-Funktion von SNMP. Der Gatekeeper beinhaltet außerdem vorzugsweise eine Funktion **441** für die Kommunikation von Registrierungsdaten und damit verbundenen Daten mit dem HTTP-/HTTPS-Server über eine Web-Server-Schnittstelle **440**.

[0101] Die **FIG. 17-19** zeigen die Einzelheiten des BAM **28** und der QoS-Funktionalität **413**, die er bereitstellt. Im Allgemeinen wird bereits eine Reihe von QoS-Systemen verwendet. Es handelt sich bei diesen jedoch häufig um Ende-zu-Ende-Systeme, bei denen jeder Hop in einem Netzwerk bekanntermaßen dasselbe QoS-System ausführt. Im Übrigen kann bei der vorliegenden Erfindung nicht davon ausgegangen werden, dass jeder Hop dasselbe oder irgendein QoS implementieren wird, da der NAS und der IODS sich über das Internet verbinden. Darüber hinaus müsste sowohl beim Host als auch beim Router QoS aktiviert sein, um bestehende QoS zwischen einem Host und einem Router zu implementieren. Die vorliegende Erfindung ist bestrebt, QoS-Funktionalität und -Unterstützung für Netzwerkknoten mobiler Terminals zu bieten, die Roaming betreiben, bei denen QoS aktiviert oder nicht aktiviert ist, unabhängig von ihrer betreiberspezifischen

Software und Hardware. Die QoS-Funktionalität der vorliegenden Erfindung wie vom BAM implementiert ist daher so ausgestaltet, dass sie bestehende Ende-zu-Ende-QoS-Systeme, die möglicherweise bereits vorhanden sind, ergänzt und mit ihnen zusammenarbeitet, wie beispielsweise das RSVP-Protokoll oder eines, das auf den IETF-DIFFSERV-Standards basiert, oder alleine funktioniert, falls kein derartiges System vorhanden ist.

[**0102**] In der folgenden Beschreibung wird durchweg auf Flüsse bzw. Paketflüsse Bezug genommen. Ein Fluss oder Paketfluss in dieser Beschreibung bedeutet einen Fluss oder Strom IP-basierter Pakete von einer Quell-IP-Adresse und einem QuellPort zu einer Ziel-IP-Adresse und einem Ziel-Port unter Verwendung eines bestimmten Netzwerkprotokolls, wie z.B. TCP. Die vorliegende Erfindung basiert auf TCP in Verbindung mit QoS-Software für die Anwendungsebene, um Netzwerküberlastung zu erkennen und die Übertragungsrate anzupassen, d.h. die Paketflussrate, zu dem Port oder den Ports, bei denen eine Überlastung am wahrscheinlichsten ist. Vorzugsweise erreicht der BAM eine programmierte Steuerung dieser Ports entweder durch eine Schnittstelle über ein bestehendes QoS-System, das die Ports steuert, falls vorhanden, oder über ein bestehendes QoS-Protokoll. In der hier beschriebenen beispielhaften Ausführungsform sind die Netzwerkpunkte, bei denen eine beträchtliche Überlastung am wahrscheinlichsten ist, die Netzwerkverbindungen in den und aus dem NAS. Die QoS-Funktionalität, die vom BAM ausgeführt wird, ist vorzugsweise so ausgestaltet, dass sie auf den NAS-Knoten des Netzwerks zugeschnitten ist. Noch spezifischer ist die QoS-Funktionalität des BAM vorzugsweise so ausgestaltet, dass sie speziell auf die Uplink-Bandbreite des öffentlichen Netzwerks des NAS zugeschnitten ist. Es ist nicht notwendig, dass der BAM explizit die Zuteilung der Downlink-Bandbreite des NAS steuert, da das normale Verhalten der meisten sitzungsorientierten Netzwerkprotokolle, wie beispielsweise TCP und RTP über UDP einen nahezu äquivalenten Grad an Bandbreite am Downlink des NAS erzeugen wird, sobald der Uplink entsprechend gedrosselt wurde.

[**0103**] Der BAM teilt vorzugsweise die verfügbare Bandbreite des Uplink des NAS zwischen privater Netzwerknutzung und der Nutzung mit öffentlichem Zugang auf. Der Ressourcenanbieter weist dem Uplink des NAS vorzugsweise einen Schwellwert für die Auslastung auf Grundlage seiner berichteten und beobachteten Bandbreite zu, die voraussichtliche Anzahl privater Netzwerkbenutzer und der Benutzer mit öffentlichem Zugang sowie den Anteil der verfügbaren, jedem Benutzer zugeteilten Bandbreite, wie hier beschrieben. Wenn die Auslastung des Uplink den Schwellwert überschreitet, wie vom TCP bestimmt und berichtet, wird ein Ereignis generiert, vorzugsweise über SNMP, und vorzugsweise protokolliert und sowohl an den Ressourcenanbieter als auch den IODS weitergeleitet. In Erwiderung auf die Generierung des Ereignisses verhindert der BAM durch den Gatekeeper **24** weiteren öffentlichen Zugriff auf den Uplink, bis die öffentliche Auslastungsrate in einem festgelegten Zeitraum unter den Schwellwert fällt. Diese Zeitspanne kann vom Ressourcenanbieter verkürzt oder verlängert werden, je nach Erfahrung mit der Häufigkeit und Länge der Zeit, in der der Schwellwert überschritten wird. Der Ressourcenanbieter kann außerdem Bandbreite zwischen privaten Netzwerkbenutzern und Benutzern mit öffentlichem Zugang umverteilen, je nachdem, wie dies angemessen bzw. gewünscht ist.

[**0104**] Der BAM teilt außerdem vorzugsweise einen Teil der verfügbaren Uplink-Bandbreite des NAS jedem Netzwerkbenutzer bis zu einer bestimmten maximalen Anzahl gleichzeitiger Benutzer zu. Wenn weniger Benutzer als die maximale Anzahl mit dem Netzwerk verbunden sind, teilt der BAM jedem von ihnen einen Teil der verfügbaren Uplink-Bandbreite des NAS zu, um Anwendungen auszuführen etc. Während sich weitere Benutzer mit dem Netzwerk verbinden, verringert der BAM die Bandbreiten-Zuteilung eines jeden Benutzers. Unterschiedlichen Benutzern können unterschiedliche Bandbreiten-Zuteilungen zugewiesen werden, je nachdem, ob es sich dabei um Teilnehmer mit ausschließlich öffentlichem Zugang oder um Kunden des privaten Netzwerks handelt. Unterschiedliche Zuteilungen können auch auf den Zugangsplänen der Teilnehmer oder auf anderen Überlegungen basieren, die für den Ressourcenanbieter von

Wichtigkeit sind. Wie in **FIG. 17** gezeigt, setzt der BAM eine minimale Benutzer-Bandbreiten-Zuteilung **1801** fest, die vom Ressourcenanbieter geändert werden kann. Wenn sämtliche Benutzer-Bandbreiten-Zuteilungen ausgelastet sind, benachrichtigt der BAM den Gatekeeper **24**, der verhindert, dass neuen Benutzern die Verbindung mit dem Netzwerk erlaubt wird. Es stellt eine Ausnahme dar, wenn ein bestehender Benutzer seine Zuteilung reduzieren lässt oder dessen Verbindung aufgrund von Prioritätsverlust bezüglich seiner Bandbreiten-Zuteilung getrennt wird.

[**0105**] Beginnend mit der Basis-Bandbreiten-Zuteilung an jeden Netzwerkbenutzer verwendet der BAM eine konventionelle Anwendungs-Definitionsliste **1802** als Vorgabe, um die Bandbreiten-Zuteilungen weiterhin zu steuern. Die Anwendungs-Definitionsliste **1802** enthält einen Satz von Kriterien, der den Fluss von Paketen über das Netzwerk beschreibt. Vorzugsweise verwendet der BAM ein Klassifizierungssystem in Übereinstimmung mit den Klassifizierungskriterien, die in bestehenden Ende-zu-Ende-QoS-Systemen Anwendung finden. Bei der in **FIG. 17** dargestellten Ausführungsform sind die Paketflüsse beispielsweise breit gefasst als Verkehrssteuerung **1804**, Sprache **1805**, Echtzeit **1806**, Verzögerungssensitivität **1807**, Standard **1808**, Verzögerungsinsensivität **1809**, nicht klassifiziert **1829** und niedrige Priorität **1830**. Der BAM kann dementsprechend die Informationen aus der Anwendungs-Definitionsliste **1802** einholen, indem er auf die Liste eines bestehenden, bereits eingerichteten Ende-zu-Ende-QoS-Systems zugreift, z.B. das RSVP oder eines, das auf den IETF-DIFFSERV-Standards basiert, über eine Programmierschnittstelle **1821**. Alternativ kann der BAM das Type-of-Service(ToS)-Feld, das im IP-Header der vom NAS empfangenen Pakete enthalten ist, teilen, die Information extrahieren und seine eigene Anwendungs-Definitionsliste erzeugen und verwalten. Außerdem kann der Integrationsbetreiber eine interne Anwendungs-Definitionsliste verwalten, die auf den NAS anwendbar ist, und kann diese in regelmäßigen Abständen in die lokale Datenbank des NAS kopieren.

[**0106**] Jeder Anwendungsart ist eine minimale benötigte Bandbreite **1810**, eine normale benötigte Bandbreite **1812**, eine optimierte Bandbreite **1813** sowie eine maximale Bandbreite **1814** zugewiesen. Eine Hauptfunktion des BAM besteht darin, sicherzustellen, dass mindestens die minimalen Netzwerkbandbreitenressourcen für jede Anwendung verfügbar sind. Falls ausreichend freie Bandbreite verfügbar ist, nachdem jeder Anwendung ihre minimale benötigte Bandbreite zugeteilt wurde, versucht der BAM, den Anwendungen die normalen Bandbreiten **1812** zuzuteilen. Falls noch immer freie Bandbreite verfügbar ist, versucht der BAM, jeder Anwendung die optimierte Bandbreite zuzuteilen. Falls noch immer freie Bandbreite verfügbar ist, versucht der BAM, jenen Anwendungen maximale Bandbreite zuzuteilen, die für stark variierenden Datenverkehr optimiert sind, wobei es sich dabei normalerweise um verzögerungsinsensitive Anwendungen wie beispielsweise E-Mail handelt. Falls schließlich noch immer freie Bandbreite verfügbar ist, versucht der BAM, anderen Anwendungen maximale Bandbreite zuzuteilen. Somit wird vorzugsweise jedem Paketfluss, also jeder Anwendung, eine der vier Bandbreitenstufen minimal, Standard, optimiert oder maximal zugewiesen, abhängig von der gesamten verfügbaren Bandbreite. Vorzugsweise stuft der BAM Anwendungen von einer Bandbreitenstufe auf die nächste hoch und stuft Anwendungen von einer Bandbreitenstufe auf die nächste herab, und zwar quantisiert statt schrittweise.

[**0107**] Anwendungen werden vorzugsweise anhand eines hier beschriebenen Benutzer-Prioritäts- und Gewichtungsschemas zwischen den Bandbreitenstufen hoch- und herabgestuft. Eine Dienststufenvereinbarungs-Prioritätsliste bezeichnet verschiedene Kategorien von Netzwerkbenutzern. In der bevorzugten Ausführungsform werden die Kategorien von Benutzern als Steuerungsbenutzer **1828**, Heimbenutzer oder lokale Benutzer **1816**, Prioritätsbenutzer **1817**, Standardbenutzer **1818**, Benutzer mit Ermäßigung **1819**, Benutzer mit kostenlosem Zugang **1820** sowie nicht registrierte Benutzer **1831** bezeichnet. Beispiele für Steuerungsbenutzer sind der NAS selbst, das IODS-Netzwerk-Gateway, ein mit dem NAS verbundener Router sowie andere Netzwerk-Infrastruktur-Geräte und

Steuerungssitzungen mit solchen Geräten. Heimbenutzer oder lokale Benutzer sind normalerweise eher Benutzer, die Kunden des privaten Netzwerks oder der Organisation des Dienstanbieters sind, als Roaming-Teilnehmer mit öffentlichem Zugang. Solche Benutzer erhalten vorzugsweise im Vergleich zu anderen Netzwerkbenutzern eine sehr hohe Priorität. Prioritätsbenutzer sind Teilnehmer mit öffentlichem Zugang, die einen Aufpreis für zusätzliche Bandbreite bezahlen, sofern diese verfügbar ist, um sicherzustellen, dass keine Pakete fallengelassen werden. Diese Benutzer erhalten im Vergleich zu anderen Benutzern ebenfalls eine sehr hohe Priorität. Standardbenutzer sind normale Teilnehmer mit öffentlichem Zugang. Benutzer mit Ermäßigung sind Teilnehmer mit öffentlichem Zugang, die eine niedrigere Priorität gegen Zugang zu niedrigeren Kosten akzeptieren. Benutzer mit kostenlosem Zugang sind Benutzer mit besonderem Zugang. Diesen Benutzern wird normalerweise kein Zugang zum Netzwerk gewährt, außer in Verbindung mit bestimmten Programmen, wie beispielsweise Universitäts- oder Konferenzprogrammen oder Ähnlichem. Nicht registrierte Benutzer sind diejenigen Benutzer, die nicht für den Zugang zum Netzwerk autorisiert sind. Obwohl nicht registrierten Benutzern falls gewünscht Netzwerkzugang gewährt werden kann, ist dies nicht bevorzugt.

[**0108**] Wie oben ausgeführt ist der BAM über eine QoS-System-Schnittstelle **1821** mit einem bestehenden Ende-zu-Ende-QoS-System verbunden, sofern vorhanden. Derzeit existieren unterschiedliche QoS-Schemata, einschließlich Multi-Protocol Label Switching (MPLS) **1822**, Subnet Bandwidth Manager (SBM) **1823**, IETF Differentiated Services (DIFFSERV) **1824**, COPS **1825**, ReSerVation Protocol (RSVP) (IETF RFC 2205) **1826** und Asynchronous Transfer Mode (ATM) **1827**. Vorzugsweise ist die Schnittstelle **1821** so implementiert, dass Duplizierung vermieden wird und sie ähnlich wie diese Schemata arbeitet, um im Wesentlichen ähnliche QoS-Bedingungen am NAS-Uplink bereitzustellen, unabhängig davon, welches Ende-zu-Ende-QoS-System vorhanden ist.

[**0109**] **FIG. 18** zeigt eine beispielhafte Möglichkeit, wie ein Ressourcenanbieter die verschiedenen Bandbreiten-, Benutzer-, Anwendungs- und andere Parameter parametrisieren und gewichten kann, um die Bandbreitenstufe zu bestimmen, die Anwendungen zugeordnet wird. Im Wesentlichen wird in der bevorzugten Ausführungsform vom Ressourcenanbieter jedem Parameter eine Gewichtung zugeordnet. Die Gewichtungen der verschiedenen Parameter, die einer Anwendung entsprechen, werden addiert, und die gewichtete Summe bestimmt, welche Bandbreitenstufe der Anwendung zugeordnet wird. Vorzugsweise werden die Gewichtungswerte so zugewiesen, dass das QoS-System dergestalt abgestimmt wird, dass alle Anwendungen tendenziell auf ihrer minimalen Bandweitenstufe laufen.

[**0110**] In der bevorzugten Ausführungsform beinhalten die Parameter die Art des Bandbreitenbedarfs **1901**, die Art der Dienststufenvereinbarung oder der Benutzerpriorität **1902**, eine Präferenz von Heimbenutzern gegenüber besuchenden Benutzern **1903**, die Art der Anwendung **1904**, einen an der Bandbreite gemessenen Kostenbasis-Parameter **1905**, einen lokalen allgemeinen Konfliktparameter **1906** sowie Durchfluss-Anfrage-Ursprungs-Parameter **1907**. Die Arten des Bandbreitenbedarfs **1901** beinhalten die kritische oder minimale Bandbreitenstufe (C), die normale oder standardmäßige Bandbreitenstufe (N), die optimierte Bandbreitenstufe (O) sowie die maximale Bandbreitenstufe (M). In dem bestimmten in **FIG. 18** gezeigten Beispiel sind diesen Parametern die Gewichtungen 7 bzw. 4 bzw. 2 bzw. 0 zugeordnet. Diese QoS-Implementierung ist daher so abgestimmt, dass einer Anwendung, die die Zuteilung ihrer minimalen benötigten Bandbreitenstufe anfragt, eine wesentliche höhere Gewichtung zugewiesen wird als einer, die ihre maximale Bandbreitenstufe anfragt. Ähnlich beinhalten die Arten der Dienststufenvereinbarung oder der Benutzerpriorität **1902** den Steuerungsbenutzer (C), den Heimbenutzer oder lokalen Benutzer (H), den Prioritätsbenutzer (P), den Standardbenutzer (S), den Benutzer mit kostenlosem Zugang (F) sowie den nicht registrierten Benutzer (U). Hier hat der Ressourcenanbieter jeder der Benutzerprioritätsarten die Gewichtungen 10 bzw. 6 bzw. 6 bzw. 3 bzw. 2 bzw. 1 bzw. -2 zugewiesen. Der

Heimbenutzer-Präferenz-Parameter **1903** kommt ins Spiel, wenn ein Benutzer die Zuteilung von Bandbreite anfragt, die über seine eigene Zuteilung hinausgeht, und die zusätzliche Zuteilung die Verringerung der Zuteilung eines anderen Benutzers erfordert. Dem Benutzer, dem Bandbreite weggenommen werden soll, d.h. der Benutzer mit der Anwendung, die die niedrigste Gewichtung hat, wird irgendein Gewichtungsfaktor zugewiesen, in diesem Fall eine Gewichtung von 3. Diese zusätzliche Gewichtung stellt vorzugsweise sicher, dass zusätzliche Bandbreiten-Zuteilungen nicht auf Kosten anderer Benutzer an Benutzer mit Anwendungen gegeben werden, die im Wesentlichen dieselbe Gewichtung haben, sondern nur wenn eine Anwendung eine wesentlich höhere Gewichtung hat als eine, der Bandbreite entzogen werden soll. Die Anwendungsarten **1904** beinhalten vorzugsweise Steuerung, Sprache, RTP, verzögerungssensitiv, normal oder verschlüsselt, verzögerungsinsensitiv, nicht klassifiziert oder nicht kategorisiert sowie geringe Priorität. In diesem Beispiel sind diesen Anwendungsarten Gewichtungen von 7, 5, 4, 3, 1, 1, 0 und -2 zugewiesen, die die relative Wichtigkeit jeder Anwendung widerspiegeln, denen eine höhere Stufe an Bandbreite zugeteilt wird. Der an der Bandbreite gemessene Kostenbasis-Parameter **1905** spiegelt die Situation wider, in der die Bandbreite auf gemessenen Nutzungskosten basiert. In diesem Fall erhält in diesem Beispiel keine Anwendung eine Gewichtung im Hinblick auf die Zuteilung zusätzlicher Bandbreite, außer Anwendungen, die von Benutzern mit Nutzungsplänen mit gemessenem Verbrauch ausgeführt werden. Der lokale allgemeine Konfliktparameter **1906** stellt eine Präferenz zwischen privaten Netzwerkkunden (lokale Benutzer) und Teilnehmern mit öffentlichem Zugang (globale Benutzer) zur Verfügung, wenn der Ressourcenanbieter die Uplink-Bandbreite zwischen Benutzung durch öffentlichen Zugang und Benutzung durch private Netzwerkkunden geteilt hat. In diesem Fall wird in diesem Beispiel, falls ein lokaler Benutzer versucht, übermäßig Bandbreite in Anspruch zu nehmen, die den globalen Benutzern zugeteilt ist, eine Gewichtung von -1 zugewiesen, wohingegen in dem Fall, dass ein globaler Benutzer versucht, übermäßig Bandbreite in Anspruch zu nehmen, die lokalen Benutzern zugewiesen ist, eine vergleichsweise schwerwiegendere Strafe von -3 zugewiesen wird. Der Durchfluss-Anfrage-Ursprungs-Parameter **1907** kommt ins Spiel, wenn ein Benutzer Bandbreiten-Zuteilung für eine Anwendung anfragt und der Benutzer seine zugewiesene Bandbreiten-Zuteilung bereits überschritten hat. Falls ein Benutzer mit einer Bandbreiten-Zuteilung von 100 KBit/s beispielsweise eine Sprachanwendung ausführt, der 70 KBit/s zugeteilt sind, und einen Web-Browser, dem 32 Kbit/s zugeteilt sind, und dann versucht, einen Dateitransfer über das Netzwerk durchzuführen, beginnt die Anfrage zusätzlicher Bandbreite für die Anwendung des Dateitransfers bei einer gesamten Bandbreite, die bereits über der Bandbreiten-Zuteilung des Benutzers liegt. In diesem Fall wird in diesem Beispiel der Anfrage des Benutzers bezüglich zusätzlicher Bandbreite eine Strafgewichtung von -3 zugewiesen.

[0111] Das vorliegende Beispiel basiert auf dem Ansatz gewichteter Summen. Andere Ansätze für die Bestimmung der relativen Wichtigkeit verschiedener QoS-bezogener Parameter sind ebenfalls akzeptabel, vorausgesetzt, dass sie eine Abstimmung des QoS-Systems durch den Ressourcenanbieter ermöglichen und nicht in Konflikt mit (einem) bereits vorhandenen QoS-System(en) stehen. Statt des beschriebenen Ansatzes gewichteter Summen könnte beispielsweise ein Ansatz verschachtelter Parameter verwendet werden. Beim Ansatz verschachtelter Parameter würde der Ressourcenanbieter einfach die Reihenfolge der Datenfluss-Klassifizierungsparameter innerhalb einer verschachtelten Auswahlanweisung festlegen, wie beispielsweise (1) öffentlich oder privat, (2) verzögerungssensitiv oder verzögerungsinsensitiv, (3) Einzelbenutzer oder reservierter Datenfluss, (4) Dienstplan. Wenn bei diesem Ansatz jedem Pfad entlang der Kette gefolgt wird, hätte dies die Zuweisung eines Bandbreiten-Zuteilungswertes zur Folge. Unterschiedliche Pfade, also unterschiedliche Kombinationen von Klassifizierungsparametern, haben damit unterschiedliche Bandbreiten-Zuteilungswerte zur Folge, die relativ zueinander zugewiesen werden.

[0112] **FIG. 19** zeigt im Allgemeinen den Gesamtaufbau und -betrieb des BAM und des QoS-Systems. Unabhängig davon, welcher Ansatz verwendet wird, um den verschiedenen Klassifizierungsparametern Werte zuzuordnen, überprüft der Ressourcenanbieter vorzugsweise die historischen Statistiken zur Netzwerknutzung, bestimmt die gesamte verfügbare zuzuteilende Bandbreite und schätzt die Anzahl der Benutzer, unter denen die verfügbare Bandbreite zugeteilt werden soll. Der Ressourcenanbieter legt dann vorzugsweise Regelwerke für die Bandbreiten-Zuteilung auf Grundlage der angebotenen Dienstpläne fest, den Schutzgrad, der einzelnen Benutzern gewährt werden soll, bestimmt, ob Ursprungs-Datenverkehr aus dem privaten Netzwerk oder Einnahmen generierender Datenverkehr aus dem öffentlichen Zugang priorisiert werden soll, und legt den Bedarf fest, zumindest einen minimalen QoS für verzögerungssensitive Anwendungen wie VoIP bereitzustellen. Auf Grundlage dieser Regelwerke und Bestimmungen legt der Ressourcenanbieter vorzugsweise die Gewichtungen fest, die den verschiedenen Parametern zugewiesen werden sollen bzw. die Werte, die den verschiedenen Zweigen in der verschachtelten Kette zugewiesen werden sollen, und konfiguriert den BAM und die QoS **2001**. Jedem Benutzer wird, sobald er sich mit dem Netzwerk verbindet, anfangs eine Basis-Bandbreiten-Zuteilung **2002** zugewiesen. Während Benutzer über das Netzwerk Anwendungen ausführen, werden Anfragen zum Upgrade des Datenflusses an den BAM und die QoS **2003** gesendet und von diesen verarbeitet. Außerdem werden Paketflüsse geschaffen und zerstört, während Anwendungen ausgeführt und abgeschlossen werden. Während die Paketflüsse geschaffen und zerstört werden, wird die tatsächliche Bandbreiten-Zuteilung an jeden Benutzer durch BAM und QoS **2004** verändert und abgestimmt, und zwar auf Grundlage der Werte, die den Klassifizierungsparametern zugewiesen werden und der Werte, die vom Ressourcenanbieter jeder Bandbreiten-Zuteilungsstufe **1810-1814** zugewiesen werden. Der BAM versucht permanent, die Paketflüsse auf ihre maximalen Bandbreiten-Zuteilungen hochzustufen und stimmt permanent jeden Paketfluss so ab, dass maximale Übertragungseffizienz und eine zuverlässige und reibungslose Funktion eines jeden Flusses erreicht wird. Der Fachmann wird erkennen, dass, obwohl sich die Bandbreiten-Zuteilungen zu einer bestimmten Zeit dynamisch verändern werden, die Basis-Bandbreiten-Zuteilungen vorzugsweise eine Ausgangsbasis oder Kennzahl für das System bereitstellen und gleich bleiben werden, bis sie vom Ressourcenanbieter durch Rekonfiguration von BAM und QoS verändert werden.

[0113] **FIG. 15** zeigt die Einzelheiten der Echtzeitverarbeitung/der Telefonie-Dienste des NAS, wie in **FIG. 3** gezeigt. Ein mobiles Terminal, das das Netzwerk besucht, kann mit einem Agent für IP-Telefonie oder Videokonferenzen ausgestattet sein. Es gibt heute viele solcher Agenten, wie z.B. das Session Initiation Protocol (SIP), veröffentlicht als IETF RFC 2543, mit seinen Erweiterungen für PSTN-Zugang mit dem Titel „PSTN/Internetworking (PINT) Service", veröffentlicht als IETF RFC 2848. Der ITU-Standard H.323 bietet eine ähnliche Funktionalität, und JAIN und PARLAY stellen zusätzliche Telefonie-/Internet-Integrations-Dienste bereit. Viele IP-Telefonanbieter, wie beispielsweise Lucent Technologies, unterstützen sowohl SIP als auch H.323. Die folgende Beschreibung geht davon aus, dass der NAS und der IODS mindestens den SIP-Standard und seine Erweiterungen unterstützen.

[0114] Ein mobiles Terminal initialisiert eine Echtzeit-Konferenz-Sitzung in Schritt **1601**. Bei Initiierung ruft der Echtzeit-Konferenz-Agent die Adresse eines geeigneten Echtzeit-Konferenz-/Telefonie-Server-Parameters ab. Es gibt eine Reihe verschiedener Möglichkeiten, dies zu erreichen. Das mobile Terminal kann die Adresse vom DHCP abrufen, falls vorhanden (siehe Internet Engineering Task Force SIP Work Group Internet Draft „draft-ietf-sip-dhcp-03.txt" auf http://ietf.org von G. Nair und H. Schulzrinne von der Universität von Columbia, veröffentlicht am 20. Januar 2001 mit dem Titel „DHCP Option for SIP Servers"). Alternativ kann das mobile Terminal die Adresse vom SLP (IETF RFC 2608) abrufen. Eine andere Alternative besteht darin, dass das mobile Terminal die Adresse des Telefonie-Servers manuell intern konfigurieren kann. Außerdem kann das mobile Terminal die Adressen für geeignete Echtzeit-Konferenz-/Telefonie-Server beim DNS anfragen.

[0115] Falls das mobile Terminal die Adresse des Telefonie-Servers dynamisch abfragt, wird die Anfrage des mobilen Terminals an den Anrufanfragen-Server **43** des NAS weitergeleitet, wie in Schritt **1603** gezeigt. Falls das mobile Terminal intern eine statische Server-Adresskonfiguration beibehält, wird sich der Agent des mobilen Terminals mit diesem Server verbinden, der entweder ein Echtzeit-Konferenz-/Telefonie-Server eines dritten Drittanbieters sein kann, wie in Schritt **1604** gezeigt, oder der IODS, wie in Schritt **1602** gezeigt, abhängig von der internen Adresskonfiguration des mobilen Terminals. Falls der IODS kontaktiert wird, leitet dieser die Anfrage des mobilen Terminals an den Anrufanfragen-Server **43** des NAS weiter, wie in Schritt **1603** gezeigt.

[0116] Falls der Drittanbieter eine Dienstvereinbarung mit dem Integrationsbetreiber oder dem Ressourcenanbieter hat (oder mit beiden), wie in Schritt **1605** gezeigt, wird der Drittanbieter die Anfrage des mobilen Terminals durch den IODS entweder direkt an den NAS oder indirekt an den NAS weiterleiten, wie in den Schritten **1605**, **1603** und **1602** gezeigt. Die Anfrage und Verbindung des mobilen Terminals wird dann vom NAS abgewickelt. Falls jedoch der Drittanbieter weder mit dem Integrationsbetreiber noch mit dem Ressourcenanbieter eine Dienstvereinbarung hat, wird der Anbieter die Verbindung verarbeiten, und weder der NAS noch der IODS werden beteiligt sein, wie in Schritt **1606** dargestellt.

[0117] Bei Empfang der Anfrage des mobilen Terminals ruft der Anrufanfragen-Server **43** des NAS die Information aus dem geltenden Teilnehmer-Regelwerk aus der lokalen Datenbank des NAS ab, wie in Schritt **1607** gezeigt. Diese Information wird von der IODS-Master-Datenbank an die lokale Datenbank des NAS abgerufen, wenn die Gatekeeper-Komponente des NAS die Profilinformation des Benutzers als Teil des Verbindens des Benutzers mit dem Netzwerk verarbeitet, wie in **FIG. 9** gezeigt. Sofern der Benutzer die Konferenzparameter (bestehend aus Qualität versus Kosten) nicht speziell angepasst hat, wird der NAS einen Satz von Latenzzeit- und Kosten-Kennzahlen anhand der Dienstvereinbarung des Teilnehmers bestimmen. Wenn der Teilnehmer beispielsweise eine Dienstvereinbarung hoher Priorität hat, werden die Kosten nach der Qualität berücksichtigt, während bei Teilnehmern, die eine Vereinbarung mit Ermäßigung haben (niedrige QoS), die Kosten eine stärkere Gewichtung haben werden als die Latenzzeit. Das mobile Terminal kann die automatische Gewichtung umgehen, indem es sich direkt mit dem NAS-Web-Server verbindet, wie in Schritt **1618** gezeigt.

[0118] Der Anrufanfragen-Server **43** des NAS bestimmt außerdem anhand der Teilnehmer-Vereinbarung die Mindestqualitätsstandards für die angefragte Echtzeit-Konferenz, wie in Schritt **1608** gezeigt. Diese Information wird im IODS gespeichert, und eine Teilmenge davon wird in die lokale Datenbank des Ressourcenanbieters repliziert. Die Mindestqualitätsstandards werden vom Anrufanfragen-Server **43** verwendet, um zu bestimmen, ob der Anruf oder eine andere Echtzeit-Konferenz-Anfrage Ende-zu-Ende über das IP-Netzwerk geroutet werden können oder ob das Routing über ein Telefonie-Gateway erfolgen soll oder direkt an das PSTN vom Netzwerk des Ressourcenanbieters.

[0119] Der Anrufanfragen-Server kontaktiert dann den NAS-Verzeichnisagenten **34**, um eine Adressliste für den Korrespondenten abzurufen, mit dem das mobile Terminal kommunizieren möchte, wie in den Schritten **1609** und **1610** gezeigt. Sobald der Anrufanfragen-Server die IP-Adressen für den Korrespondenz-Knoten hat, geht er zur Messung der Latenzzeit für jede IP-Adresse über das IP-Netzwerk über. Dies erfolgt vorzugsweise, indem der Anrufanforderungs-Server vier ICMP-Pakete an jede Korrespondenz-IP-Adresse sendet und die Roundtrip-Latenzzeit misst. Falls die Latenzzeit für eine Adresse innerhalb der Mindestqualitätsstandardanforderung liegt und die IP-Adresse tatsächlich über das Netzwerk erreicht werden kann, wie in den Schritten **1615** und **1616** festgelegt, ruft der Server alle geltenden Kosteninformationen aus der lokalen Datenbank des Ressourcenanbieters ab, wie in Schritt **1622** gezeigt. Der Ressourcenanbieter kann beispielsweise einen Aufpreis von zwei Cent pro Minute auf IP-Anrufe berechnen, die über sein Netzwerk geroutet werden.

Falls in der lokalen Datenbank des Ressourcenanbieters keine geltende Kosteninformation verfügbar ist, ruft der NAS alle geltenden Kosteninformationen aus der IODS-Master-Datenbank ab.

[0120] Falls die Anruf- oder Echtzeit-Konferenz-Anfrage nicht mittels IP-Routing gestellt werden kann, wie in Schritt **1611** festgelegt, kontaktiert der Anrufanfragen-Server **43** den Telefonie-Gateway-Routing-Server **35** des NAS, um ein geeignetes Telefonie-Gateway zum Herstellen der Verbindung auszuwählen, wie in Schritt **1612** gezeigt. Der Telefonie-Gateway-Routing-Server **35** bietet den Anruf dem PSTN-Gateway mit der kürzesten Latenzzeit an, das die niedrigsten Kosten unter Verwendung konventioneller Routing-Algorithmen hat. Falls der NAS mit einem lokalen NAS-Telefonie-Gateway **39** ausgestattet ist und falls das lokale NAS-Telefonie-Gateway **39** die beste Kombination aus Kosten und Latenzzeit hat, verbindet der Telefonie-Gateway-Routing-Server den Anruf oder die Konferenzanfrage über das lokale Telefonie-Gateway **39**, wie in Schritt **1614** gezeigt. Falls jedoch ein entferntes Telefonie-Gateway eine bessere Kombination aus Kosten und Latenzzeit hat, wird der Telefonie-Gateway-Routing-Server den Anruf oder die Konferenzanfrage über das entfernte Telefonie-Gateway mit der besten verfügbaren Kombination verbinden, wie in Schritt **1613** gezeigt. Falls kein Telefonie-Gateway mit einer Kombination aus Latenzzeit und Kosten verfügbar ist, die die Mindestqualitätsanforderungen erfüllt, wie in Schritt **1623** festgelegt, teilt der Telefonie-Gateway-Routing-Server dem Anrufer die verfügbaren Optionen mit, einschließlich der Latenzzeit und der Kosten, die mit jeder Route verbunden sind, wie in den Schritten **1620**, **1622** und **1629** gezeigt. Der Anrufer kann dann das Tätigen des Anrufs bzw. der Anfrage ablehnen oder eine der angebotenen Optionen annehmen, wie in Schritt **1619** gezeigt.

[0121] Sobald die optimale Route festgelegt wurde oder der Kunde eine bestimmte Route ausgewählt hat, führt der NAS eine Kostenkalkulation durch, wie in Schritt **1622** gezeigt. Falls der NAS feststellt, dass keine Kosten anfallen und der Anruf kostenlos ist, wie in Schritt **1628** gezeigt, wird der Anruf direkt getätigt und es wird ein Abrechnungseintrag erzeugt, wie in den Schritten **1624** und **1627** gezeigt. Falls der NAS in Schritt **1629** feststellt, dass der Anruf ein kostenpflichtiger Anruf ist, übermittelt der NAS in Schritt **1617** die voraussichtlichen kalkulierten Kosten an die Telefonie-Client-Software des mobilen Terminals und aktualisiert in Schritt **1618** die Kosteninformation auf der Client-Internetseite. Dies erfolgt, wenn die Telefonie-Agent-Software des mobilen Terminals nicht in der Lage ist, die vom NAS erhaltene Kosteninformation zu verarbeiten. In diesem Fall kann sich der Benutzer des mobilen Terminals direkt mit der Internetseite verbinden und die Kosteninformation einholen. Der Benutzer des mobilen Terminals kann außerdem in Schritt **1628** einen Bericht über alle Routing-Optionen anfordern; in diesem Fall werden alle möglichen Routing-Optionen unabhängig von Kosten und Latenzzeit berichtet. Falls der Benutzer des mobilen Terminals in Schritt **1621** die Verbindung des Anrufs oder der Anfrage über alle Optionen ablehnt, wird der Prozess beendet. Falls jedoch der Benutzer des mobilen Terminals die voraussichtlichen Kosten akzeptiert, die er entweder direkt vom NAS oder der Internetseite erhalten hat, wie in Schritt **1619** gezeigt, wird der Anruf getätigt und ein Abrechnungseintrag erstellt, wie in den Schritten **1624** und **1627** gezeigt.

[0122] Wenn der Anruf beendet wird, wie in Schritt **1626** gezeigt, wird in Schritt **1625** ein abschließender Abrechnungseintrag erstellt. Der NAS speichert die Abrechnungsinformation in seiner lokalen Datenbank für die spätere Rechnungsstellung an den Benutzer. Der NAS aktualisiert schließlich auch die entsprechende Sprachanruf-Abrechnungsinformation in der IODS-Master-Datenbank.

[0123] Bezugnehmend auf **FIG. 2 und 5** wird die bevorzugte Ausführungsform des IODS **18** nun ausführlicher beschrieben. Der IODS **18** umfasst im Allgemeinen eine Datenbank **3000** sowie eine Reihe funktioneller Dienstkomponenten **500**. Während die Datenbank **3000** als zentrale Datenbank auf einem einzigen Server oder einer kleinen Anzahl verbundener

Server implementiert werden kann, wird die Datenbank **3000** vorzugsweise in einer verteilten Anordnung implementiert, die auf mehrere Server verteilt ist. Die Datenbank-Elemente können beispielsweise auf ein System von Servern verteilt sein, die strategisch in einer Vielzahl von Internetknoten und zentralen Büros untergebracht und durch Router verbunden sind. Ein verteiltes Schema bietet u.a. Vorteile im Hinblick auf die Skalierbarkeit. Verteilte Serversysteme und Datenbankanordnungen, die für diesen Zweck geeignet sind, sind dem Fachmann bekannt und müssen hier nicht im Einzelnen beschrieben werden.

[**0124**] Wie in **FIG. 2** gezeigt, ist die IODS-Datenbank **3000** logisch hierarchisch aufgebaut und umfasst in der bevorzugten Ausführungsform drei Schichten bzw. Ebenen. Die oberste Schicht **3010** bezieht sich auf die Identifizierung von Informationen für Benutzer (Teilnehmer), Ressourcenanbieter und Integrationsbetreiber. Die zweite Ebene **3020** bezieht sich auf verschiedene Netzwerk-Objekte und Regelwerke und ist logisch mit der Teilnehmer- und Ressourcenanbieter-Information der ersten Ebene verbunden. Die dritte Ebene **3030** bezieht sich auf Netzwerkereignisse, -transaktionen und -status und ist durch die Beziehung zwischen Status und dem verbundenen Netzwerkobjekt (Netzwerkkomponente) mit der zweiten Ebene verbunden.

[**0125**] Die erste Ebene **3010** beinhaltet vorzugsweise eine Teilnehmer-Tabelle **3100**, eine Ressourcenanbieter-Tabelle **3200** sowie eine oder mehrere Betreiber-Tabellen **3300**. In diesem Dokument bezieht sich der Begriff „Tabelle" nicht zwangsläufig nur auf eine flache Datei oder Liste, sondern kann sich auch auf eine relationale Datenbank oder ein relationales Datenbanksegment beziehen. Die Teilnehmer-Tabelle **3100** enthält vorzugsweise Informationen über jeden Benutzer, der zuvor registriert wurde und autorisiert ist, auf das Netzwerk zuzugreifen, also einen Teilnehmer. Solche Informationen beinhalten vorzugsweise Name und Kontaktdaten, ggf. Angaben zur Zahlungsart, falls gewünscht, wie beispielsweise Kreditkarte oder Rechnung, ggf. Kreditkartendaten sowie Firmenkreditkontoinformationen, wie z.B. ob eine Rechnung auf ein Konto ausgestellt oder von einer Kreditkarte abgebucht werden soll.

[**0126**] Die Ressourcenanbieter-Tabelle **3200** enthält vorzugsweise Informationen über das Unternehmen, das die Netzwerkressourcen zur Verfügung stellt, die den Teilnehmern den Zugang zum öffentlichen Netzwerk ermöglichen. Die Eckdaten, die vorzugsweise in dieser Tabelle enthalten sind, sind Name und Kontaktdaten des Ressourcenanbieters.

[**0127**] Die Integrationsbetreiber-Tabelle **3300** ist im Wesentlichen mit der Ressourcenanbieter-Tabelle **3200** identisch, da Integrationsbetreiber auch als Ressourcenanbieter betrachtet werden. Der Hauptunterschied besteht darin, dass der Integrationsbetreiber drahtlosen Zugang bereitstellt sowie Netzwerkinfrastruktur und -dienste, -abrechnung, -sicherheit und -support.

[**0128**] Die zweite Ebene **3020** beinhaltet vorzugsweise eine Adapter-Tabelle **3400**, eine Regelwerk-Tabelle **3500**, eine Ressourcenobjekt-Tabelle **3600** sowie eine Bandbreiten-Regelwerk-Tabelle des Ressourcenanbieters für den öffentlichen Zugang **3650**. Die Adapter-Tabelle **3400** beinhaltet vorzugsweise Informationen, die die ID der Geräte bezeichnet, z.B. die MAC-Adressen der Netzwerkschicht **2** für jedes zuvor autorisierte mobile Terminal jedes registrierten Teilnehmers, sowie eine Bezeichnung des Zugangsplans für jeden von ihnen. Die Adapter-Tabelle **3400** ist logisch mit der Teilnehmer-Information auf der ersten Ebene **3010** verbunden. Jede Geräteadresse, d.h. jedes mobile Terminal, kann seinen eigenen Zugangsplan erhalten, und umgekehrt kann ein einziger Zugangsplan mehrere Geräteadressen abdecken. Vorzugsweise bezeichnet die Adapter-Tabelle **3400** außerdem die Sicherheitsregelwerke für jedes mobile Terminal, die mit der Geräteadresse des mobilen Terminals verbunden sind, und optional einen Satz kryptografischer Schlüssel aus der Schicht **2**,

die bei der verschlüsselten Kommunikation mit dem mobilen Terminal verwendet werden, falls vorhanden. Es gibt mehrere Sicherheitsregelwerke, die potenziell anwendbar sind. Ein Regelwerk bezieht sich auf Kommunikation zwischen den mobilen Terminals und den WAPs. Falls verschlüsselte Kommunikation über die Netzwerkschicht **2** nicht möglich ist, z.B. weil der Hersteller des mobilen Terminals und der Hersteller der WAPs inkompatible Verschlüsselungsschemata implementiert haben, wird gemäß diesem Regelwerk die Verschlüsselung in der Schicht **2** abgeschaltet, und das mobile Terminal kommuniziert mit den WAPs in einer offenen Sitzung. Ein zweites Regelwerk bezieht sich auf die Kommunikation zwischen NAS und IODS. Falls dieses Regelwerk gilt, legt es die Schaffung eines sicheren Tunnels für die Kommunikation zwischen NAS und IODS fest. Es gibt zahlreiche Algorithmen, um zu bestimmen, ob und für welche Kommunikation solch ein sicherer Tunnel verwendet werden soll, und die Auswahl eines oder mehrerer Tunnel hängt von den Erfordernissen des jeweiligen Systems ab. Falls jedoch dieses Regelwerk gilt, wird vorzugsweise solch ein Kommunikationsregelungsalgorithmus verwendet, statt lediglich sämtliche Kommunikation durch den Tunnel zu routen, um potenziell schwerwiegende Latenzprobleme zu vermeiden. Ein drittes Regelwerk bezieht sich auf die Verwendung von IPSec-Verschlüsselung in der Schicht **3** für die Kommunikation zwischen den mobilen Terminals und dem NAS. Falls dieses Regelwerk gilt, regelt es ausschließlich die Sicherheit der drahtlosen Verbindung, die den abhöranfälligsten Abschnitt des Netzwerks darstellt. Eine über die Schicht **3** verschlüsselte Kommunikation bringt jedoch einigen Mehraufwand mit sich, der zu Leistungseinschränkungen führen kann. Ein viertes Regelwerk soll lediglich Standardsicherheit ermöglichen. In diesem Fall wird sämtliche Kommunikation unverschlüsselt sein, was derzeit bei Internetzugang meistens der Fall ist. Ein fünftes Regelwerk gilt, wenn eine programmierbare Schnittstelle zwischen den WAPs und dem NAS verfügbar ist. Falls die WAPs beispielsweise eine API haben, auf die der NAS mittels Programmierung zugreifen und dadurch Befehle an die WAPs senden kann, kann eine zusätzliche Sicherheitsoption (Verschlüsselung über die Verbindungsschicht auf Ebene **2**) angeboten werden. Falls dies verfügbar ist, wird ein Verschlüsselungsschlüssel vom mobilen Terminal an den WAP kommuniziert und vom WAP an den NAS zur Verarbeitung weitergeleitet. Falls die lokale Datenbank des NAS (LDAP **38**, **FIG. 3**) keinen Eintrag mit dem Schlüssel enthält, wird dieser an den IODS weitergeleitet, um dort mit den kryptografischen Schlüsseln, die in der Adapter-Tabelle **3400** enthalten sind, abgeglichen zu werden. Falls keine Übereinstimmung gefunden wird, ist der Schlüssel dem Netzwerk unbekannt, und es ist keine über die Schicht **2** verschlüsselte Kommunikation unter Verwendung des Schlüssels möglich. Der NAS leitet das mobile Terminal auf eine Registrierungsseite weiter. Falls jedoch entweder in der lokalen NAS- oder der entfernten IODS-Datenbank eine Übereinstimmung für den Schlüssel gefunden wird, wird die entsprechende Verschlüsselungsinformation vom NAS an den WAP gesendet, um zwischen dem WAP und dem mobilen Terminal eine verschlüsselte Kommunikation über die Schicht **2** zu ermöglichen.

[0129] Diese Regelwerke werden von jedem Ressourcenanbieter und jedem Teilnehmer entschieden, vorzugsweise anhand einer Liste von Kompatibilitätsempfehlungen, die vom Integrationsbetreiber herausgegeben wird. Daher wird der Integrationsbetreiber für jedes mobile Terminalgerät und jeden Software-Revisionsstand vorzugsweise einen empfohlenen Sicherheitsmodus herausgeben. Ein mobiles Terminal kann beispielsweise Probleme haben, sich mit einem bestimmten WAP zu verbinden, wenn es sich im Modus „Verschlüsselung anfragen aber offene Sitzung erlauben" befindet. Im Ergebnis wird der Teilnehmer vorzugsweise angewiesen werden, das mobile Terminal im „offenen Modus" zu konfigurieren, wenn er unterwegs ist, während das mobile Terminal zu Hause recht gut im dualen Modus arbeiten kann, wenn es eine Schnittstelle mit einer bestimmten Basisstation mit einem bestimmten Firmware-Revisionsstand hat.

[0130] Zusätzlich stellt die Adapter-Tabelle **3400** vorzugsweise ein Flag „verloren" oder „gestohlen" bereit, um anzuzeigen, wenn ein bestimmtes mobiles Terminal mit einer bestimmten Geräteadresse als verloren oder gestohlen gemeldet wurde.

Falls solch ein Terminal versucht, auf das Netzwerk zuzugreifen, kann eine entsprechende Abhilfemaßnahme oder Berichterstattung stattfinden.

[0131] Die Regelwerk-Tabelle **3500** stellt vorzugsweise Informationen zu verschiedenen Kontodaten sowie zur Verfügbarkeit und den Einzelheiten von Dienstplänen zur Verfügung und ist logisch mit der Teilnehmer-Information auf der ersten Ebene **3010** verbunden. Verfügbare Dienstpläne könnten einen nutzungsbasierten oder einen Flatrate-Plan beinhalten, einen nutzungsbasierten oder einen Flatrate-Plan mit einem Aufpreis, der für Premium-Zugang zu Bandbreiten-Ressourcen gegenüber Standard-Benutzern/-Teilnehmern anfällt, oder einen Plan mit kostenlosem Zugang. Prioritäts-Zugangspläne können priorisierten Netzwerk- und/oder Bandbreitenzugang gegenüber Plänen ohne Priorität erhalten. Kostenlose Zugangspläne sind eine Zusatzoption für besondere Umstände, um beispielsweise Universitäten oder Programmen zur Unterstützung wirtschaftlich benachteiligter Menschen Netzwerkzugangskonten zur Verfügung zu stellen.

[0132] Die Ressourcenobjekt-Tabelle **3600** ist logisch mit der Ressourcenanbieter-Information auf der ersten Ebene **3010** verbunden. Die Ressourcenobjekt-Tabelle bezeichnet vorzugsweise einen IP-Adressbereich, der dem Ressourcenanbieter zur Verfügung steht, einschließlich der IP-Unteradressbereiche und Orte zum Einholen von DHCP-IP-Adresszuteilungen. Die Ressourcenobjekt-Tabelle beinhaltet außerdem vorzugsweise eine Liste der Geräteadressen aller registrierten Teilnehmer sowie einen Satz kryptografischer Schlüssel, um verschlüsselte Kommunikation zwischen dem Netzwerk und den Teilnehmern zu ermöglichen.

[0133] Die Bandbreiten-Regelwerk-Tabelle des Ressourcenanbieters für den öffentlichen Zugang **3650** ist logisch mit der Ressourcenanbieter-Information auf der ersten Ebene **3010** verbunden. Die Bandbreiten-Regelwerk-Tabelle des Ressourcenanbieters für den öffentlichen Zugang **3650** beinhaltet vorzugsweise die Informationen des Bandbreiten-Regelwerks des Anbieters für den öffentlichen Zugang. Dies könnte die Bezeichnung oder Definition von priorisiertem Datenverkehr, normalem Datenverkehr und kostenlosem Datenverkehr beinhalten sowie die Festlegung einer Obergrenze für die öffentliche Bandbreitennutzung, wie in Verbindung mit dem BAM **28** ausführlich beschrieben.

[0134] Die dritte Ebene **3030** enthält vorzugsweise eine Adapter-Status-Tabelle **3700**, eine Sitzungseinträge-Tabelle **3750**, eine Teilnehmerkonto-Status-Tabelle **3800** sowie eine Anruf-Abrechnungs-Tabelle **3950**, die logisch mit der Teilnehmer-Information auf der ersten **3010** und der zweiten Ebene **3020** verbunden sind. Die dritte Ebene enthält außerdem vorzugsweise eine Ressourcenanbieter-Status-Tabelle **3850** sowie eine Ressourcen-Status-Tabelle **3900**, die logisch mit der Ressourcenanbieter-Information auf der ersten **3010** und der zweiten Ebene **3020** verbunden sind.

[0135] Die Adapter-Status-Tabelle **3700** enthält vorzugsweise für jedes mobile Terminal einen Satz von Verschlüsselungsschlüsseln, die auf das mobile Terminal zugeschnitten sind, die Identität des registrierten Eigentümers des mobilen Terminals, die Identität des Protokolls/der Protokolle, die das mobile Terminal unterstützt sowie das Sicherheits-Regelwerk, das für das mobile Terminal gilt.

[0136] Die Sitzungseinträge-Tabelle **3750** enthält vorzugsweise Informationen über die Nutzung des Netzwerks durch den Teilnehmer, um die Berechnung von Gebühren an den Teilnehmer zu Rechnungsstellungs- und Abrechnungszwecken zu ermöglichen. Vorzugsweise beinhaltet jeder Eintrag in der Sitzungseinträge-Tabelle **3750** eine Adapter-Identifikation, d.h. die Geräteadresse eines registrierten mobilen Terminals, die Startzeit einer Sitzung, an der dieses Terminal beteiligt ist, die Geräteadresse eines mobilen Korrespondenz-Terminals (falls vorhanden), die Anzahl der während der Sitzung gesendeten und empfangenen Bits sowie einen Orts-Identifizierer, d.h. die Identifikation des Ressourcenanbieters. Der Orts-

Identifizierer ist die geografische Lage des WAP, die vom Ressourcenanbieter bei der Veröffentlichung der WAP-Ressourcen, die Teilnehmern mit öffentlichem Zugang zur Verfügung stehen, eingetragen wird. Die Adresse des Korrespondenz-Knotens unterstützt den Teilnehmer bei der Überprüfung seiner Rechnung und wird als Teil der Netzwerkstatistik erfasst und periodisch im Sitzungseintrag gespeichert, z.B. alle 60 Sekunden. Die Sitzungsinformation kann mit dem öffentlichen Schlüssel des Teilnehmers verschlüsselt werden, so dass der Teilnehmer sicher sein kann, dass er seine Rechnung überprüfen kann, ohne dass seine Besuche auf der Seite heimlich aufgezeichnet werden. Diese Information kann unter Verwendung konventioneller Datenbank-Abfrage-Software abgefragt werden, um zusammenfassende Nutzungsberichte über jeden registrierten Teilnehmer bereitzustellen.

[**0137**] Gleichermaßen beinhaltet die Anruf-Abrechnungs-Tabelle **3950** vorzugsweise Informationen über die Nutzung der Sprachkommunikations-Einrichtungen des Netzwerks durch den Teilnehmer, um die Berechnung von Gebühren an den Teilnehmer zu Rechnungsstellungs- und Abrechnungszwecken zu ermöglichen. Jeder Eintrag der Anruf-Abrechnungs-Tabelle **3950** beinhaltet vorzugsweise eine Adapter-Identifikation, d.h. die Geräteadresse eines registrierten mobilen Terminals, die Startzeit einer Sitzung, an der das Terminal beteiligt ist, den Ort des Terminals, d.h. eine Identifikation des Ressourcenanbieters, die angerufene Telefonnummer, die Dauer der Sitzung sowie die Kosten pro Minute bzw. deren Erhöhung. Diese Information kann unter Verwendung konventioneller Datenbank-Abfrage-Software abgefragt werden, um zusammenfassende Nutzungsberichte über jeden registrierten Teilnehmer bereitzustellen und um die Gebühren für nutzungsbasierte Pläne zu berechnen.

[**0138**] Die Teilnehmerkonto-Status-Tabelle **3800** beinhaltet vorzugsweise Informationen über die Zahlungshistorie des Teilnehmers, wie beispielsweise vorhergehende Zahlungen, die vom Teilnehmer getätigt wurden, vorhergehende Gebühren, die dem Teilnehmer in Rechnung gestellt wurden, den aktuellen Kontostand des Teilnehmers, den Abrechnungszyklus des Teilnehmers sowie die Anzahl der Bits, die vom Teilnehmer über das Netzwerk in dem aktuellen Abrechnungszyklus gesendet und empfangen wurden. Letztere Information kann die Grundlage für die Berechnung von Gebühren an den Teilnehmer unter einem nutzungsbasierten Netzwerk-Zugangsplan darstellen.

[**0139**] Die Ressourcenanbieter-Status-Tabelle **3850** hat einen ähnlichen Zweck und enthält vorzugsweise ähnliche Informationen wie die Teilnehmerkonto-Status-Tabelle **3800**. Der Hauptunterschied ist, dass die Ressourcenanbieter-Status-Tabelle **3850** vorzugsweise Informationen zur Verfügung stellt, die Abrechnungen zwischen dem Ressourcenanbieter und dem Integrationsbetreiber ermöglichen, wohingegen die Teilnehmerkonto-Historien-Tabelle **3800** Abrechnungen zwischen dem Ressourcenanbieter und den Teilnehmern regelt. Die Ressourcenanbieter-Status-Tabelle **3850** beinhaltet somit vorzugsweise die Gesamtzahl von Bits, die von Teilnehmern mit öffentlichem Netzwerkzugang in dem aktuellen Abrechnungszyklus unter Verwendung der Zugangseinrichtungen des Ressourcenanbieters zum öffentlichen Netzwerk empfangen und gesendet wurden. Diese Information wird vorzugsweise der Information entnommen, die in der Sitzungseinträge-Tabelle **3750** enthalten ist. Die Tabelle beinhaltet außerdem vorzugsweise eine Identifikation des Abrechnungs- bzw. Rechnungsstellungszyklus zwischen dem Ressourcenanbieter und dem Integrationsbetreiber. Schließlich enthält die Tabelle außerdem vorzugsweise Einträge über vorhergehende Zahlungen vom Integrationsbetreiber an den Ressourcenanbieter sowie vorhergehende Gutschriften, die vom Ressourcenanbieter an den Integrationsbetreiber ausgestellt wurden. Auf Wunsch kann der Kontostand ebenfalls als Datenfeld oder berechnetes Feld mit aufgenommen werden.

[0140] Die Ressourcenanbieter-Status-Tabelle **3900** beinhaltet vorzugsweise den Betriebsstatus jedes Netzwerk-Geräts, seine aktuelle Verfügbarkeit sowie seine Auslastung.

[0141] Der Fachmann wird verstehen, dass zusätzlich zu den Datenelementen und -strukturen, die in **FIG. 2** bezeichnet und dargestellt sind, weitere Datenstrukturen und -elemente bei der Konfiguration eines Netzwerks mit drahtlosem Zugang wie dem hier beschriebenen notwendig sind, um Kommunikation über Mobile-IP, DHCP, SIP, DNS und IPSec zu unterstützen. Da diese Strukturen und Elemente jedoch konventionell und dem Fachmann auf dem Gebiet der drahtlosen Kommunikationsnetzwerke bekannt sind, ist es nicht notwendig, sie hier im Einzelnen zu beschreiben.

[0142] Wie zuvor beschrieben, werden jene Komponenten des IODS, die auf der NAS-Ebene am häufigsten verwendet werden, vorzugsweise an den NAS unter Verwendung von Caching und Verteilungsmechanismen, die dem Fachmann bekannt sind, repliziert. Für diesen Zweck kann beispielsweise die bekannte „LDAP Replication Architecture" (LDUP) verwendet werden, die unten ausführlicher beschrieben ist. Wie oben beschrieben wird die IODS-Datenbank außerdem vorzugsweise periodisch mit neuen Informationen aktualisiert, die durch ihre entsprechenden NAS abgerufen werden. Die Replikation und Aktualisierung der IODS-Datenbank werden vorzugsweise unter Verwendung der veröffentlichten IETF LDAP Duplication/Replication/Update Protocols durchgeführt. Diese Protokolle sind unter dem Titel „LDAP Replication Architecture" veröffentlicht und unter http://www.ietf.org/internetdrafts/draft-ietf-ldup-model-05.txt aufrufbar. Der Fachmann wird erkennen, dass LDAP die Basis eines Verzeichnisdienstes darstellt und hochkompatibel ist mit Kommunikation, die mit öffentlichen Schlüsseln verschlüsselt ist und mit Interoperabilität zwischen verschiedenen Netzwerken. Aus diesen Gründen gilt LDAP als geeigneter Mechanismus für die Verbreitung der IODS-Datenbank **3000** über das Netzwerk zwischen dem IODS und verschiedenen NAS. Dem Fachmann wird jedoch außerdem bewusst sein, dass die vom LDAP bereitgestellten Einrichtungen für die Aktualisierung/Replikation von Datenbanken möglicherweise nicht so flexibel oder effizient sind wie ein spezielles Netzwerk-Datenbank-Management-Tool. Deshalb wäre ein alternativer geeigneter Ansatz, die IODS-Datenbank in ihre Transaktions- und Verzeichnisdienst-Elemente zu zerlegen und ein geeignetes Netzwerk-Datenbank-Management-Tool für die Aktualisierung und Replikation der IODS-Datenbank über das Netzwerk zu verwenden. Solche Tools sind von verschiedenen Anbietern von Datenbankprodukten erhältlich, wie beispielsweise der IBM Corporation, der Oracle Corporation und der Microsoft Corporation. Ein derartiges Management-Tool könnte beispielsweise periodisch aufgerufen werden und als getakteter Prozess ablaufen, um die Aktualisierung und Replizierung der IODS-Datenbank über die verschiedenen Netzwerke bereitzustellen, die sie bedient.

[0143] Die funktionalen Komponenten des IODS sind allgemein als **500** in **FIG. 5** dargestellt. Wie oben beschrieben, wird der IODS vorzugsweise als verteiltes Netzwerk aus Servern und Routern **501** implementiert, die strategisch in Internetknoten und zentralen Büros untergebracht sind, um die Skalierbarkeit zu verbessern. Der IODS kann jedoch trotz seines Namens auch auf einem Server oder einer relativ geringen Anzahl eng verbundener Server an einem Ort implementiert werden. Bei dieser Implementierung kann es erforderlich sein, Techniken wie beispielsweise DNS von Akamai oder Round Robin zu verwenden, um einen bestimmten NAS mit einem verbundenen IODS-Server zu verbinden, während sich das System erweitert. Unabhängig von der gewählten Ausführung wird der Netzwerkzugangspunkt zum IODS hier als Betreiber-Netzwerk-Gateway bezeichnet. Wie unten ausführlicher beschrieben, erfolgt die Kommunikation zwischen dem NAS uns dem Betreiber-Netzwerk-Gateway vorzugsweise über einen IPSEC-Tunnel zwischen dem NAS und dem Gateway. In Fällen, in denen der IODS auf verteilten Servern implementiert ist, werden vorzugsweise standardmäßige Lastverteilungsalgorithmen **502** verwendet, um zu bestimmen, welcher bestimmte IODS-Server einem bestimmten NAS Dienste zu einer bestimmten Zeit bereitstellen wird.

[0144] Der IODS beinhaltet einen konventionellen TCP/IP-Stapel **503** der IP Version 4 oder IP Version 6, um dem IODS die Kommunikation und Verbindung über das Internet zu ermöglichen. Wie dem Fachmann bekannt ist, wird die exakte Konfiguration des TCP/IP-Stapels unter anderem von der Konfiguration des Netzwerks und des Gateways sowie des verwendeten Betriebssystems/der verwendeten Betriebssysteme abhängen. Der IODS kann außerdem andere konventionelle TCP/IP-Dienste **504** beinhalten, wie beispielsweise RSVP.

[0145] Der IODS beinhaltet außerdem vorzugsweise einen konventionellen DHCP-Server **506**, der dem NAS IP-Adressbereiche für deren Zuteilung an besuchende Terminals liefert. Der IODS beinhaltet außerdem Routing-Dienste **505**, um das IODS-Netzwerk zu verbinden und vorzugsweise Dienste auf höherer Ebene zu unterstützen, wie beispielsweise Lastenverteilung und Verteilung von Inhalten.

[0146] Der IODS beinhaltet vorzugsweise sichere Datenkommunikations-Einrichtungen wie die als **507**, **508** und **509** gezeigten Einrichtungen. Die Einrichtungen führen vorzugsweise Authentifizierungen durch und sorgen für eine verschlüsselte Kommunikation zwischen dem NAS und dem IODS, insbesondere für die Übertragung vertraulicher und sensibler Daten, wie beispielsweise Abrechnungsdaten. Die bevorzugte Ausführung verwendet ein konventionelles Internetsicherheitsprotokoll (IPSec) und eine konventionelle Authentifizierungs-/Verschlüsselungs-/Entschlüsselungseinrichtung oder ISAKMP/IKE, die mit einem konventionellen digitalen PKI-Zertifizierungsdienst arbeiten. Alternativ kann auch das SSL-Protokoll verwendet werden. Wie dem Fachmann bekannt ist, wird das IPSec vorzugsweise im Tunnelmodus betrieben, um einen sicheren Kommunikationstunnel zwischen dem NAS und dem IODS zu schaffen, wodurch ein virtuelles privates Netzwerk (VPN) gebildet wird und die zwischen dem NAS und dem IODS übertragenen Daten gekapselt werden. Die ISAKMP/IKE-Einrichtung ermöglicht die gegenseitige Authentifizierung zwischen dem NAS und dem IODS sowie das Aushandeln einvernehmlicher kryptografischer Algorithmen und Schlüssel, um die Verschlüsselung und Entschlüsselung der gesendeten bzw. empfangenen Daten zu ermöglichen. SSL bietet eine ähnliche Funktionalität. Kryptografische Zertifikate und Schlüssel sind passend über einen konventionellen Zertifizierungsdienst sowie viele private und kommerziellen Quellen erhältlich, die im Stand der Technik bekannt sind. Der IPSec-Tunnel kann auch verwendet werden, um Datenverkehr von einem mobilen Terminal durch das Netzwerk entweder an das Netzwerk-Gateway, das sich am nächsten am endgültigen Zielort befindet (Betrieb des IPSec im Tunnelmodus), oder den endgültigen Zielort selbst zu senden (Betrieb des IPSec im Transportmodus).

[0147] In der bevorzugten Ausführungsform stellt der IODS außerdem Mobile-IP-Unterstützung zur Verfügung, wie bei **509** gezeigt. Spezifikationen für Mobile-IP-Unterstützung **509** für Mobile-IP-Netzwerke der Version 4 und Version 6 sind veröffentlicht in den IETF RFCs 2002 und dem IETF-Entwurf „draft-ietf-mobileip-ipv613.txt“ mit dem Titel „Mobility Support in Ipv6“ unter http://search.ietf.org/internetdrafts/draft-ietf-mobileip-ipv6-13.txt. Mobile-IP-Unterstützung ermöglicht dem IODS, über das Netzwerk übermittelte Pakete an mobile Terminals, die Roaming betreiben, weiterzuleiten ohne jedes Mal den Home-Agenten des mobilen Terminals kontaktieren zu müssen.

[0148] Vorzugsweise unterstützt der IODS außerdem konventionelle HTTP- und (sichere) HTTPS-Dienste. Der IODS verwendet einen konventionellen HTTP-Agent, beispielsweise um Ressourcenanbietern die Registrierung und Veröffentlichung von Ressourcen, und Teilnehmern die Einsicht und Aktualisierung ihrer Kontoinformationen zu ermöglichen.

[0149] Der IODS unterstützt außerdem vorzugsweise konventionelle IP-Telefonie-Dienste **511** und Kreditkartenverarbeitung **512**. Die Kreditkartenverarbeitungs-Komponente **512** übernimmt vorzugsweise die Online-Verarbeitung von Kreditkarteninformationen, um neuen Teilnehmern sofortigen Netzwerkzugang zu ermöglichen. Ein im Handel erhältliches Produkt, das für diesen Zweck geeignet ist, wird unter dem Namen „Cash Register" von Cybercash Inc. angeboten. Andere geeignete Einrichtungen dieser Art sind dem Fachmann bekannt und müssen hier nicht im Einzelnen beschrieben werden.

[0150] Der IODS beinhaltet außerdem vorzugsweise konventionelle LDAP- und LDAP-Replikations- und Aktualisierungs-Schnittstellen (LDUP), um den Zugang zu Online-Verzeichnisdiensten über einen eigenständigen LDAP-Verzeichnisdienst oder einen Verzeichnisdienst mit X.500-Back-End zu ermöglichen. Diese Schnittstellen ermöglichen außerdem vorzugsweise den Zugriff auf und den Betrieb mit verteilten LDAP-Diensten.

[0151] Falls gewünscht, kann der IODS außerdem auch Schnittstellen für andere Datenbanken **514** beinhalten, wie beispielsweise Netware Directory Services oder Datenbanken von Telekommunikationsdienstleistern zum Zwecke der gegenseitigen Authentifizierung.

[0152] Der IODS beinhaltet außerdem vorzugsweise Alt-AAA-Schnittstellen für Authentifzierung, Autorisierung und Abrechnung **515**. Die AAA-Schnittstelle **515** basiert auf einem konventionellen LDAP, das über IPSec oder SSL läuft. Ihre Hauptaufgabe besteht darin, Geräte(MAC)-Adressen mobiler Terminals zu empfangen und zu verifizieren, dass diese in der IODS-Datenbank registriert sind. Sobald verifiziert wurde, dass eine Adresse in der Datenbank vorhanden ist und auf einen registrierten Teilnehmer hinweist, sendet sie eine Antwort mit dem Dienstplan des Teilnehmers an den NAS. Sie empfängt außerdem vorzugsweise periodisch von jedem NAS Einträge zur Netzwerknutzung, d.h. alle 60 Sekunden, um die Sitzungseinträge in der IODS-Datenbank zu aktualisieren. Solche Einträge beinhalten vorzugsweise die Start- und Endzeit der Übertragung, die Anzahl der übertragenen und empfangenen Bits sowie die kontaktierten Netzwerkressourcen. Die Informationen zu den besuchten Netzwerkressourcen werden vorzugsweise für den Teilnehmer vertraulich behandelt und sind mit dem öffentlichen Schlüssel des Teilnehmers verschlüsselt, um Zugriff durch den Integrationsbetreiber zu verhindern.

[0153] Der IODS beinhaltet außerdem vorzugsweise einen Datenbanküberwachungsdienst **531**. Der Datenbanküberwachungsdienst **531** empfängt Trigger, die von der in **FIG. 2** dargestellten IODS-Datenbank erzeugt werden, und übermittelt diese an das entsprechende Netzwerk-Kommunikationsprotokoll bzw. den entsprechenden Netzwerk-Kommunikationsdienst, wie beispielsweise SNMP, damit dort die entsprechende Aktion erfolgen kann. Dieser Dienst ist besonders nützlich, um Betrug zu entdecken und entsprechend zu handeln. Derzeit sind verschiedene Ereignisüberwachungsdienste für die Abwicklung solcher Datenbank-Wartungsaufgaben im Handel erhältlich. Bei Windows 2000 bietet beispielsweise das Produkt Microsoft SQL Server die Funktion, Datenbankereignisse in einem Ereignisprotokoll aufzuzeichnen. Andere Produkte, wie beispielsweise Manage X von Hewlett Packard, erlauben einem Netzwerkadministrator das Definieren von Ereignissen, deren Auftreten dazu führt, dass Warnmeldungen gesendet werden. Die Warnmeldungen können per E-Mail oder an eine Managementkonsole gesendet werden, sie können in SNMP umgewandelt werden oder die automatische Ausführung vorher festgelegter Abläufe auslösen.

[0154] Die IODS-Datenbank **3000**, die in **FIG. 5** im Zusammenhang mit den funktionalen Komponenten des IODS als **520** gezeigt ist, ist in **FIG. 2** ausführlich dargestellt und wurde oben ausführlich beschrieben. Die Datenbank enthält

Informationen, auf die der Ressourcenanbieter und der Integrationsbetreiber **521** zugreifen können, wie z.B. Sitzungseinträge besuchender Teilnehmer; Daten, die nur vom Ressourcenanbieter **522** aktualisierbar sind und auf die nur dieser zugreifen kann, wie z.B. die IP-Subnetze der Ressourcenanbieter oder Informationen zu deren kryptografischen Schlüsseln; Daten, die nur vom Integrationsbetreiber **523** aktualisierbar sind und auf die nur dieser zugreifen kann, wie z.B. Informationen zur IODS-Konfiguration oder kryptografische Schlüssel von IODS-Personal; Daten, die nur vom Teilnehmer **524** aktualisierbar sind und auf die nur dieser zugreifen kann, wie z.B. besuchte Netzwerkseiten und Ressourcenkontakte; sowie Daten, auf die nur der Teilnehmer und der Integrationsbetreiber zugreifen können **525**, wie z.B. aktuelle Kontostände. Daten, die entweder von einem Teilnehmer oder einem Ressourcenanbieter sind und nicht für den Betreiber zugänglich sein sollen, sind vorzugsweise verschlüsselt, um dem Integrationsbetreiber den Zugang unmöglich zu machen.

[0155] Der IODS enthält vorzugsweise auch fremde Betreiberschnittstellen **530**, welche Gateways umfassen, um die Interoperation mit großen drahtlosen Betreibern zu ermöglichen und registrierten Teilnehmern das Roaming zu erlauben. Zum Beispiel könnten diese Gateways als ESN für die MAC-Adressen-Cross-Authentifizierungssysteme verwendet werden, oder um das Inter-Operator-Roaming durch registrierte mobile Terminals zu erlauben.

[0156] Die Einzelheiten des Netzwerkbetriebs werden nun unter Bezugnahme auf **FIG. 6-12** beschrieben. **FIG. 6** zeigt eine allgemeine Übersicht über den Systembetrieb. Allgemein ist es so, dass das mobile Terminal, wenn ein besuchendes mobiles Terminal in die Nähe eines WAP **3, 4** kommt, beginnt, Funksendungen vom WAP zu empfangen, die die Anwesenheit des WAP melden. Als Antwort initiiert das mobile Terminal die Aushandlung einer Kommunikationsverbindung mit dem WAP in Schritt **700**. Wie vorher beschrieben, und in Abhängigkeit von der Herstellung und den Konfigurationen des mobilen Terminals und des WAP, kann die ausgehandelte Kommunikationsverbindung eine verschlüsselte Verbindung der sicheren Schicht **1** oder **2** oder eine offene Verbindung sein. Einzelheiten des Verhandlungsprozesses sind hier beschrieben, aber für die gegenwärtigen Zwecke reicht der Hinweis aus, dass der Verhandlungsprozess so ist, wie er im IEEE 802.11-Standard spezifiziert ist.

[0157] Sobald eine Kommunikationsverbindung zwischen dem mobilen Terminal und dem WAP eingerichtet ist, beginnt der WAP mit dem Senden von Paketen und/oder Frames vom mobilen Terminal an den NAS **7**. Der NAS analysiert die MAC- oder die Geräteadresse des mobilen Terminals von den Paketen oder Frames und verwendet die Adresse, um in Schritt **800** zu bestimmen, ob das mobile Terminal ein registrierter Teilnehmer ist. Im Wesentlichen wird die Authentifizierung des mobilen Terminals, wie vorher beschrieben, dadurch bewerkstelligt, dass seine MAC- oder Geräteadresse mit einer Liste solcher Adressen in der lokalen NAS-Datenbank oder der IODS-Master-Datenbank verglichen wird, um zu sehen, ob das mobile Terminal sich zuvor als Teilnehmer registriert hat.

[0158] Wenn die MAC- oder die Geräteadresse des mobilen Terminals mit einer Adresse in der lokalen NAS-Datenbank oder der IODS-Master-Datenbank übereinstimmt, wird das mobile Terminal allgemein als authentifiziert betrachtet. Als nächstes holt der NAS eine IP-Adressen-Zuweisung für das mobile Terminal in Schritt **1100** über einen lokalen DHCP-Relay-Agent oder einen DHCP-Server ein und teilt dem mobilen Terminal Netzwerk-Ressourcen, z.B. Bandbreite, in Schritt **900** zu. Die Brandbreite wird dem mobilen Terminal durch den Bandbreitenzuteilungsmanagerprozess zugeteilt, der unter der Kontrolle des NAS läuft.

[0159] Sobald dem mobilen Terminal eine IP-Adresse und Netzwerk-Ressourcen zugeteilt wurden, kann es auf das Netzwerk zugreifen. Der NAS überwacht die Netzwerkaktivitäten des mobilen Terminals und erzeugt Sitzungsabrechnungsdaten für die Abrechnung und andere Zwecke bei **1000**. Einige Netzwerkaktivitäten können jedoch auf eine betrügerische Aktivität durch das mobile Terminal hindeuten. Wenn der NAS eine solche Aktivität in Schritt **1200** detektiert, ergreift er geeignete Abhilfemaßnahmen.

[0160] In Schritt **1600** schließlich verwaltet und verarbeitet der NAS Echtzeit-Netzwerkanwendungen für registrierte, autorisierte mobile Terminals. Solche Anwendungen können z.B. Dateiübertragung, Internetzugang, Internetsurfen, E-Mail und Echtzeit-Konferenzen wie z.B. VoIP („Voice over Internet Protocol") und Video-Konferenzen sein.

[0161] **FIG. 7** veranschaulicht die Einzelheiten des Aushandlungsprozesses einer Kommunikationsverbindung zwischen mobilen Terminals und WAPs. Bevor oder während ein Benutzer sein eigenen Heim-Netzwerk verlässt, kann er eine Abdeckungskarte in Schritt **100** konsultieren, um festzustellen, wo WAPs verfügbar sind, deren Abdeckung und andere Informationen inklusive der WAP-Konfiguration und dergleichen. Solche Informationen werden bevorzugt durch den IODS für registrierte Teilnehmer entweder in Papierform veröffentlicht, oder, noch bevorzugter, durch Bereitstellung der Informationen auf einer für Teilnehmer zugänglichen Webseite über die IODS-http/https-Dienste **510**. Wenn der Teilnehmer in Schritt **101** in den Funkverbindungsbereich eines WAP gelangt (oder eine physische Verbindung zum Netzwerk in einer drahtgebundenen Netzwerkanordnung herstellt), beginnt das mobile Terminal damit, Funksendungen vom WAP zu erhalten, der seine Anwesenheit bekannt gibt. Das mobile Terminal sendet dann bei **102** dem WAP eine Anfrage zur Aushandlung einer Verbindung. Wie bei **103, 104** gezeigt, kann das mobile Terminal beim WAP eine Verbindung in drei oder vier Modi anfordern, je nach seiner Konfiguration. Die Modi sind: Verschlüsselung erforderlich, Verschlüsselung angefragt, offen (Klartext) erforderlich, und offen angefragt. Wie vorher beschrieben, hängt es von seiner eigenen internen Konfiguration ab, ob das mobile Terminal versucht, eine verschlüsselte oder eine offene Verbindung einzurichten. Ungeachtet des Verbindungsmodus werden die Kommunikationen über die Verbindungsschicht zwischen dem mobilen Terminal und dem WAP bevorzugt entsprechend dem IEEE 802.11- oder dem 802.15-(Bluetooth)Standard ausgeführt, je nachdem, welcher Standard bei dem mobilen Terminal und dem WAP implementiert ist.

[0162] Wenn das mobile Terminal eine verschlüsselte Verbindung anfragt oder anfordert, und wenn das Regelwerk des WAP über verschlüsselte Verbindungen mit der Anforderung des mobilen Terminals kompatibel ist, z.B. wenn der WAP so konfiguriert ist, dass es die Anforderung einer verschlüsselten Verbindung in jedem Modus akzeptieren kann, kann eine verschlüsselte Verbindung (Schicht **1/2**) möglich sein. Es gibt zwei Methoden zur Verarbeitung der Anforderung des mobilen Terminals, je nachdem, ob der WAP mittels Programmierung durch den NAS steuerbar ist oder nicht.

[0163] Die erste Methode ist bei der Ausführungsform anwendbar, in der der WAP kein API aufweist, über welches der NAS der WAP steuern kann, wie bei **107** gezeigt. Bei dieser Ausführungsform bestimmt der WAP, ob er einen Satz nativer, bei **108** lokal gespeicherter Schlüssel hat. Gegenwärtig verfügbare WAP-Geräte sind im Allgemeinen fähig, native Schlüssel von 32 bis 64 40-Bit oder 128-Bit lokal zu speichern. Typischerweise wählt ein Netzwerkadministrator diese Schlüssel aus und konfiguriert mit ihnen den WAP unter Verwendung einer Telnet- oder Web-Schnittstellenverbindung, z.B. wenn der Administrator den WAP im Netzwerk installiert. Auf ähnliche Weise kann der Netzwerkadministrator mobile Terminals, die autorisierte Clients des Netzwerks sind, mit einem oder

mehreren der nativen Schlüssel des WAP konfigurieren, um eine verschlüsselte Verbindung einzurichten. Wenn entweder der WAP oder ein mobiles Terminal nicht mit Schlüsseln konfiguriert ist, oder wenn sie konfiguriert sind, aber keiner der Schlüssel übereinstimmt, dann ist es nicht möglich, eine verschlüsselte Sitzung über die Verbindungsschicht zwischen dem mobilen Terminal und dem WAP einzurichten, wie bei **115** angegeben. Sogar dann, wenn der WAP und das mobile Terminal beide mit passenden Schlüsseln konfiguriert sind, können sie immer noch außer Stande sein, eine verschlüsselte Verbindung auszuhandeln. Der Grund hierfür liegt darin, dass Hersteller von gängigen WAPs und mobilen Terminals manchmal ihre Verschlüsselungsalgorithmen etwas unterschiedlich implementieren. Das hat zur Folge, dass es manchmal vorkommt, dass sogar ein mobiles Terminal und ein WAP, die sich denselben Schlüssel teilen, nicht in der Lage sind, eine verschlüsselte Verbindung einzurichten. Somit ist der wahrscheinlichste Fall, dass bei dieser Ausführungsform eine verschlüsselte Verbindung möglich ist, jener, in welchem der WAP und das mobile Terminal beide zum lokalen Netzwerk des Ressourcenanbieters gehören und sie beide vom selben Hersteller stammen. Wenn jedoch der WAP und das mobile Terminal passende native Schlüssel haben und wenn ihre jeweiligen Verschlüsselungsalgorithmen kompatibel sind, reagiert der WAP vorzugsweise auf die Anforderung des mobilen Terminals, indem es dem mobilen Terminal einen Satz von Challenges zuleitet, welche bei **116** mit einer beliebigen Anzahl nativer Verschlüsselungsschlüssel verschlüsselt sind, und eine verschlüsselte Verbindung wird bei **119** eingerichtet.

[0164] Ein anderer Mechanismus ist erforderlich, um den/die native(n) Schlüssel für die mobilen Terminals bereitzustellen, die das Netzwerk des Ressourcenanbieters besuchen und keine Clients des Netzwerks sind und nicht vom Ressourcenanbieter konfiguriert sind. In diesem Fall kann der Ressourcenanbieter den/die native(n) Schlüssel des WAP über den IODS unmittelbar oder mittelbar den autorisierten Teilnehmern und anderen Ressourcenanbietern offenbaren, welche möglicherweise über der WAP einen Zugang zum Netzwerk suchen. Solch eine Offenlegung kann durch den IODS als allgemeine Verteilung solcher Informationen an alle Teilnehmer und Ressourcenanbieter erfolgen. Vorzugsweise kann es für den IODS etwas sicherer sein, solche Informationen nur solchen Teilnehmern und Ressourcenanbietern zukommen zu lassen, die den/die Schlüssel für bestimmte WAPs kennen müssen. Wenn sich beispielsweise ein Teilnehmer registriert, kann der IODS Secure Sockets Layer (SSL) verwenden, um dem Teilnehmer die Schlüssel für WAPs mitzuteilen, die sich in dem oder in der Nähe des Heimbereichs des Teilnehmers befinden, wenn nicht Schlüssel für andere WAPs in bestimmten Gebieten ausdrücklich angefordert werden. Das kann als Teil des Registrierungsvorgangs umgesetzt werden oder durch Autorisierung der bestehenden Teilnehmer, Schlüssel für zusätzliche Standorte über eine Webseite oder dergleichen anzufordern, wenn nötig.

[0165] Der Fachmann wird erkennen, dass, obwohl die Verteilung der nativen Schlüssel des WAP einen gewissen Grad an Sicherheit bietet, das gebotene Sicherheitsniveau nicht ansatzweise so stark ist wie das von einem öffentlichen Schlüsselsystem bereitgestellte. Jedoch werden bei Fehlen eines solchen Schlüsselverteilungsschemas im Wesentlichen nur solche Benutzer in der Lage sein, erfolgreich eine verschlüsselte Sitzung über die Verbindungsschicht auszuhandeln, die das private Netzwerk des Ressourcenanbieters nutzen und deren mobile Terminals bereits mit dem/den Schlüssel(n) für das/die WAP(s) dieses Netzwerks konfiguriert wurden, was nicht die bevorzugte Anordnung ist.

[0166] Sobald die Teilnehmer den/die Schüssel des/der WAP(s) haben, können sie ihre mobilen Terminals entsprechend konfigurieren. Wenn das mobile Terminal, das mit dem WAP verhandelt, mit einer oder mehreren verschlüsselten Challenges konfiguriert wurde, reagiert es auf die verschlüsselten Challenges des WAP, indem es

versucht, sie unter Verwendung seines/seiner intern gespeicherten Schlüssel(s) zu dechiffrieren, und auf den WAP zu reagieren. Wenn das mobile Terminal und der WAP sich dieselben Schlüssel teilen, wie in Schritt **114** gezeigt, und wenn das mobile Terminal die Challenges des WAP erfolgreich dechiffriert und auf diese erfolgreich reagiert, treten das mobile Terminal und der WAP in Schritt **116** in konventionelle Verhandlungen über eine verschlüsselte Sitzung über die Verbindungsschicht ein. Wenn die Verhandlung erfolgreich ist, wird in Schritt **119** eine verschlüsselte Funkverbindung eingerichtet.

[0167] Wenn jedoch das mobile Terminal und der WAP nicht den/dieselben Verschlüsselungsschlüssel teilen, wie in Schritt **115** gezeigt, so dass es nicht möglich ist, eine verschlüsselte Sitzung über die Verbindungsschicht herzustellen, oder wenn die Verbindung aus welchem anderen Grunde auch immer nicht hergestellt werden kann, so macht vorzugsweise entweder das mobile Terminal oder der WAP eine Anforderung, eine offene Sitzung in Schritt **104** auszuhandeln. Dieser sogenannte „Dual-Mode"-Ansatz zur Herstellung einer Kommunikationsverbindung umfasst die am meisten bevorzugte Ausführungsform dieses Aspekts der Erfindung. Vorausgesetzt, der WAP ist konfiguriert für und fähig zur Einrichtung einer „Offenen-Sitzungs-Verbindung" (Open Session Connection), so akzeptiert es in Schritt **112** die Anforderung einer offenen Sitzung und bietet an, eine Offene-Sitzungs-Verbindung mit dem mobilen Terminal in Schritt **117** herzustellen. Wenn jedoch aus irgendeinem Grunde der WAP nicht für das Kommunizieren in einer Offenen-Sitzungs-Umgebung konfiguriert ist oder dazu nicht in der Lage ist, wie in Schritt **113** gezeigt, und eine verschlüsselte Verbindung benötigt, was nicht bevorzugt ist, akzeptiert der WAP die Anforderung des Aushandelns einer offenen Sitzung von dem mobilen Terminal nicht und beendet die Sitzung in Schritt **124**. Als Folge hiervon wird dem mobilen Terminal der Zugang versagt, wie in **125** gezeigt. Auf die gleiche Art beendet der WAP in dem Fall, dass das mobile Terminal in Schritt **121** das Angebot des WAP der Einrichtung einer Offenen-Sitzungs-Verbindung ablehnt, die Sitzung in Schritt **124**. Bevorzugt ist der WAP dafür konfiguriert und in der Lage, SNMP-Ereignisse zu generieren, und generiert und speichert solch ein Ereignis, wenn die Herstellung einer Verbindung mit einem mobilen Terminal fehlschlägt, wie in **123** gezeigt. Vorzugsweise führt der NAS über seine SNMP-Komponente **41** periodische Abfragen nach SNMP-Ereignissen aus, wie in **FIG. 3** gezeigt, und teilt dem IODS den Fehlschlag mit, um zu ermöglichen, jedwede notwendige oder wünschenswerte Verarbeitung auszuführen.

[0168] Wenn jedoch das mobile Terminal das Angebot des WAP annimmt, eine Offene-Sitzungs-Verbindung mit dem mobilen Terminal in Schritt **120** einzurichten, dann handelt der WAP bei **120** eine Offene-Sitzungs-Verbindung mit dem mobilen Terminal aus und richtet diese gemäß den herkömmlichen Standards für drahtlose Netzwerkkommunikation ein, auf die hierin Bezug genommen wird. Der WAP beginnt dann mit dem Weiterleiten von Paketen von dem mobilen Terminal an den NAS, der die Authentifizierung des mobilen Terminals initiiert, wie bei **200** gezeigt.

[0169] Eine zweite Methode für die Verarbeitung der Anforderung einer verschlüsselten Verbindung seitens des mobilen Terminals existiert vorzugsweise dann, wenn der WAP eine API hat, die eine programmierte Steuerung durch den NAS ermöglicht, wie bei **106** gezeigt. Dies ist die am meisten bevorzugte Ausführungsform dieses Aspekts der Erfindung. In diesem Fall leitet der WAP, nach Empfang der Anfrage, falls keine nativen WAP-Schlüssel verfügbar sind, oder wenn keine nativen Schlüssel eine Übereinstimmung zeigen, die MAC-Adresse des mobilen Terminals oder eine andere eindeutige Gerätekennung in **109** an den NAS mit einer Anforderung, die Schlüssel zu aktualisieren. Ebenso versucht der NAS dann in **109**, die MAC-Adresse mit der MAC-Adresse eines registrierten Teilnehmers in seiner lokalen Datenbank abzugleichen. Wenn dort keine Übereinstimmung gefunden werden kann, kommuniziert er

vorzugsweise mit dem IODS und versucht, in der Adapter-Tabelle **3400** der IODS-Master-Datenbank **3000** eine Übereinstimmung zu finden. Wenn in keiner der Datenbanken eine Übereinstimmung gefunden wird, teilt der NAS dem WAP bei **130** mit, dass kein Verschlüsselungsschlüssel für das mobile Terminal vorhanden ist, und von dort aus wird die Anforderung des mobilen Terminals von Schritt **115** aus so verarbeitet, als ob der WAP und das mobile Terminal nicht in der Lage wären, eine verschlüsselte Sitzung einzurichten, wie oben beschrieben. Wenn jedoch entweder in der lokalen Datenbank des NAS oder in der IODS-Master-Datenbank eine Übereinstimmung gefunden wird, wie bei **129** gezeigt, ruft der NAS vorzugsweise die Chiffrierschlüssel, welche dem registrierten Teilnehmer und dem mobilen Terminal entsprechen, entweder von seiner lokalen Datenbank oder der Adapter-Tabelle **3400** der IODS-Master-Datenbank ab. Wenn entweder die lokale Datenbank oder die IODS-Datenbank eine Übereinstimmung für die MAC-Adresse enthält, jedoch kein(e) Schlüssel dem mobilen Terminal zugeordnet ist/sind, kann der NAS alternativ versuchen, den/die entsprechenden Schlüssel zu lokalisieren, indem er eine zuverlässige fremde Datenbank eines Dritten kontaktiert, wie etwa eine der bekannten Hinterlegungsstellen für öffentliche Schlüssel. Wo immer er den/die entsprechenden Schlüssel lokalisiert, setzt der NAS den neuen Schlüssel bei **131** in den WAP, und der WAP-Schlüsselspeicher wird mit dem/den entsprechenden Schlüssel(n) bei **114** aktualisiert. Der WAP sendet dann eine Challenge mit Verschlüsselung durch den/die Schlüssel des mobilen Terminals an das mobile Terminal. Wenn das mobile Terminal die verschlüsselte Aufforderung erfolgreich entschlüsselt und dem WAP antwortet, beginnen der WAP und das mobile Terminal in Schritt **116** mit dem konventionellen Aushandeln einer verschlüsselten Verbindung. Unter der Voraussetzung, dass die Verhandlung [im engl. Original steht ein falsches Wort für „**Verhandlung**", nämlich „**negation**" statt „negotiation"; Anm. d. Übers.] erfolgreich abgeschlossen wurde, wird in Schritt **119** eine verschlüsselte Funkverbindung eingerichtet. Sobald die Verbindung eingerichtet ist, verfügt der Host über einen Schicht-**2**-Zugang zum Netzwerk. Jede darauffolgende Netzwerkaktivität des mobilen Terminals hat die Übermittlung von Paketen über das Netzwerk zur Folge. Der WAP übermittelt diese Pakete von dem mobilen Terminal an den NAS, der die Anwesenheit einer neuen MAC-Adresse erkennt und in Schritt **200** Authentifizierungsverfahren in Bezug auf das mobile Terminal initiiert.

[0170] FIG. 8 veranschaulicht die detaillierten Operationen, welche vom NAS ausgeführt werden, um mobile Terminals zu authentifizieren, die sich mit dem Netzwerk verbinden. Damit ein mobiles, mit dem Netzwerk verbundenes Terminal Pakete an einen anderen Netzwerkknoten weiterleiten kann, muss das mobile Terminal die Netzwerkkonfiguration kennen. Herkömmliche Einrichtungen hierfür sind den Fachleuten allgemein bekannt und in verschiedenen IETF RCFs veröffentlicht. Typischerweise verwendet das mobile Terminal eine oder zwei herkömmliche Einrichtungen zur Bestimmung der Netzwerkkonfiguration. Das mobile Terminal kann eine Router-Discovery-Anfrage ausgeben, wofür es entweder seinen Mobile-IP-Stapel verwendet, wie bei **801** gezeigt, oder die Autokonfigurationseinrichtungen der IP-Version 6 benutzen, wie bei **803** gezeigt. Alternativ kann das mobile Terminal eine Dynamic-Host-Configuration-Protocol(DHCP)-Anfrage über das Netzwerk ausgeben, wie bei **802** gezeigt. Jede dieser Einrichtungen übermittelt ihrerseits eine Adressen-Auflösungs-Protokoll(ARP)-Anfrage über das Netzwerk, um die physische Hardware-(MAC oder Ethernet)Adresse des Knotens zu erhalten, an welchen das mobile Terminal Pakete übermittelt. Die ARP-Anfrage, welche per Definition die MAC-Adresse des mobilen Terminals enthält, wird vom ARP-Server des Netzwerks detektiert, in diesem Falle von der ARP-Komponente des Netzwerk-Stapels **25** des NAS, veranschaulicht in **FIG. 3**. Der ARP-Server speichert typischerweise einen ARP-Cache aufgelöster Adressen, d.h. die entsprechenden IP- und Hardware-Adressen. Der ARP-Server aktualisiert den Cache

mit den entsprechenden IP- und MAC-Adressen des mobilen Terminals, die er aus der ARP-Anfrage in Schritt **804** erhalten hat.

[0171] Vorzugsweise speichert der NAS in seiner lokalen Datenbank eine Replikation der IODS-Adapter-Tabelle **3400** mit den Adressen eines jeden registrierten mobilen Terminals. Ebenso bevorzugt wird der ARP-Server mit einer herkömmlichen Ereignis-Erzeuger-Einrichtung wie z.B. SNMP oder „Sockets" konfiguriert, so dass der Server bei jeder Aktualisierung des ARP-Cache mit einer neuen MAC-Adresse auf dem NAS-Downlink ein Ereignis für den Gatekeeper generiert, wie in Schritt **805** gezeigt. Der Gatekeeper-Prozess wird dann bei **806** aktiviert, und der Gatekeeper fragt dann die lokale Version der NAS-Adapter-Tabelle in Schritt **807** an. Alternativ kann der Gatekeeper-Prozess **24** periodisch den ARP-Cache auf einer festen wiederkehrenden Basis in ausgewählten Intervallen als Zeit-initiierten Prozess anfragen, um festzustellen, ob irgendwelche neuen mobilen Terminals Verbindung zum Netzwerk aufgenommen haben. Der Fachmann erkennt, dass in diesem Falle das Intervall, in welchem der Gatekeeper den ARP-Cache abfragt, kürzer bemessen sein sollte als das Intervall, in welchem der ARP-Cache, falls überhaupt, geleert wird.

[0172] Nach dem Vergleichen der MAC-Adressen im NAS-Cache mit den MAC-Adressen in der lokalen NAS-Datenbank findet der Gatekeeper entweder eine Übereinstimmung, welche anzeigt, das das mobile Terminal einem registrierten Teilnehmer gehört, wie bei **808** gezeigt, [oder er] findet eine Übereinstimmung, stellt aber fest, dass die MAC-Adresse auf der Schwarzen Liste (Blacklist) steht, wie bei **810** gezeigt, oder findet keine Übereinstimmung, wie in **809** gezeigt.

[0173] Wenn der Gatekeeper in der lokalen NAS-Datenbank keine Übereinstimmung findet, fragt er die Adapter-Tabelle **3400** der IODS-Master-Datenbank **3000** über den NAS-Uplink in Schritt **811** an. Infolge dieser Anfrage stellt der Gatekeeper in Schritt **813** entweder fest, dass es für den MAC in der IODS-Datenbank keine Übereinstimmung gibt, wodurch er anzeigt, dass das mobile Terminal keinem registrierten Teilnehmer gehört, oder dass es in Schritt **808** eine Übereinstimmung gibt, woraus hervorgeht, dass das mobile Terminal einem registrierten Teilnehmer gehört, oder dass es eine Übereinstimmung gibt, dass aber, in Schritt **810,** der MAC zu einem „Blacklist"-Konto gehört.

[0174] Falls der Gatekeeper weder in der lokalen NAS-Datenbank noch in der IODS-Master-Datenbank eine Übereinstimmung für die MAC-Adresse findet, initiiert er einen Registrierungsprozess. In Schritt **825** weist der Gatekeeper dem mobilen Terminal eine vorübergehende IP-Adresse zu, um zu ermöglichen, dass das mobile Terminal und der NAS kommunizieren. Vorzugsweise befindet sich die zugewiesene vorübergehende IP-Adresse im öffentlichen NAS-Subnetz und wird für eine relativ kurze Zeitdauer geleast, z.B. fünf Minuten. Auch werden jegliche Versuche des nichtregistrierten mobilen Terminals, Zugang zum Internet zu erhalten, über die NAS-HTTP/HTTPS-Server **37** an eine Registrierungs-Webseite auf dem NAS umgeleitet, wie in **FIG. 3** veranschaulicht. Falls nach dem Zugriff auf die Registrierungsseite in **826** der Benutzer bestimmt, als Teilnehmer registriert zu werden, präsentieren die HTTP/HTTPS-Server eine Registrierungsseite, welche ein Registrierungsformular enthält, das bestimmte Informationen vom Benutzer verlangt. Die HTTP/HTTPS-Server können auch ein spezielles Kennzeichen in die Adapter-Tabelle **3400** setzen, welches anzeigt, dass das mobile Terminal zum ersten Mal mit dem Netzwerk verbunden ist. Das Setzen dieses Kennzeichens stellt sicher, dass der neu registrierte Teilnehmer Zugang zum Netzwerk haben wird, ungeachtet des Status des Regelwerks des Ressourcenanbieters für den Zugang zum Netzwerk.

[0175] Der Registrierungsprozess umfasst das Überprüfen der auf dem Registrierungsformular gegebenen Informationen des angehenden Teilnehmers, d.h. die Gültigkeitsprüfung des Registrierungsformulars. Die Gültigkeitsprüfung des Registrierungsformulars hat zwei Komponenten: (1) syntaktische Gültigkeitsprüfung, und (2) Prüfung der Gültigkeit der Informationen. Die Gültigkeitsprüfung des Registrierungsformulars wird bevorzugt vom NAS verarbeitet. In der Komponente der syntaktischen Gültigkeitsprüfung überprüft der NAS, ob der Satz an Feldern, den der Benutzer in dem Registrierungsformular befüllt hat, den einfachen html-Form-Regeln entspricht, wie z.B., dass der eingetragene Nachname zumindest einen Buchstaben enthalten muss. Wenn das Formular die syntaktische Gültigkeitsprüfung besteht, leitet der NAS die Daten vorzugsweise an den IODS zur Gültigkeitsprüfung der Informationen weiter. Um die Informationen für gültig zu erklären, versucht der IODS bevorzugt, eindeutige Einträge betreffend den Neu-Teilnehmer, Teilnehmer-Dienstplan und Mobile-Terminal-Netzwerk-Adapter zu erzeugen, indem er die Daten verwendet, die der angehende Teilnehmer eingegeben hat. Wenn der IODS in der Lage ist, diese Einträge eindeutig zu erzeugen, leitet er die Kreditkarteninformationen des angehenden Teilnehmers zur Verarbeitung an den Kreditkartenprozessor weiter. Wenn die Kreditkarteninformationen erfolgreich verarbeitet worden sind, erzeugt der IODS die neuen Einträge in der IODS-Datenbank zusammen mit einem dazugehörigen SLA (Dienstleistungsstufen-Vereinbarung, „Service Level Agreement"). Sodann übermittelt der IODS die Daten, die während der Benutzeranmeldung vom NAS normal abgerufen wurden, an den NAS zurück, womit der Registrierungsvorgang bei **827** abgeschlossen ist.

[0176] Falls nach dem Zugriff auf die Registrierungsseite der nichtregistrierte Benutzer nicht in der Lage ist, den Registrierungsvorgang erfolgreich abzuschließen, oder falls der nichtregistrierte Benutzer nicht auf die Registrierungsseite zugreift, erstreckt sich der Netzwerkzugang des nichtregistrierten Benutzers nur bis zum NAS oder bis zum Gateway des privaten lokalen Netzwerks, das vom NAS gesteuert wird, wie bei **829** gezeigt. Darüber hinaus sendet der Gatekeeper, wenn der WAP mittels Programmierung durch den NAS steuerbar ist, bei **828** einen De-Authentifizierungsbefehl an der WAP, welcher der WAP anweist, die Kommunikationsverbindung mit dem nichtregistrierten mobilen Terminal zu beenden.

[0177] Wenn der Gatekeeper eine Übereinstimmung für die MAC-Adresse des mobilen Terminals entweder in der lokalen NAS-Datenbank oder in der IODS-Master-Datenbank findet, aber feststellt, dass die MAC-Adresse zu einem „Blacklist"-Konto gehört, initiiert der Gatekeeper vorzugsweise Sicherheitsvorkehrungen, wie bei **815** gezeigt. Einzelheiten dieser Vorkehrungen sind in Bezug auf **FIG. 12** veranschaulicht und beschrieben. Eine „Blacklist"-Mac-Adresse kann durch den Status des „verlorenen oder gestohlenen Kennzeichens" angezeigt werden, der in der Adapter-Tabelle **3400** der IODS-Master-Datenbank **3000** gespeichert ist, welche vorzugsweise wenigstens zum Teil auf der lokalen NAS-Datenbank repliziert ist, wie vorher beschrieben. Sie kann auch durch ein Kennzeichen oder einen anderen Hinweis angezeigt werden, der mit der MAC-Adresse in Zusammenhang steht und angibt, dass das Konto des Teilnehmers, der der Eigentümer des mobilen Terminals ist, nicht verstoßfrei ist, oder bei dem festgestellt worden ist, dass er schon früher ohne Berechtigung Zugang zum Netzwerk hatte, z.B. ein Hacker oder dergleichen.

[0178] Wenn der Teilnehmer bei **827** eine Registrierung erfolgreich abschließt, oder wenn der Gatekeeper eine Übereinstimmung für die MAC-Adresse des mobilen Terminals entweder in der lokalen NAS-Datenbank oder in der IODS-Master-Datenbank findet, und wenn der Gatekeeper feststellt, dass die MAC-Adresse sich nicht auf der „Blacklist" befindet, dann betrachtet er das Konto als ein registriertes Konto mit einwandfreier Konto-Historie, wie bei **808** gezeigt. Der Gatekeeper fährt dann fort und verarbeitet den Dienstplan des Teilnehmers bei **821**. Bei der

Verarbeitung des Dienstplans des Teilnehmers ruft der Gatekeeper die Informationen des Dienstplans des Teilnehmers und das Zugangs-Regelwerk des Ressourcenanbieters für besuchende mobile Terminals von den lokalen Versionen der Regelwerk-Tabelle **3500** und der Tabelle **3650** des Zugangs-Regelwerks für die Bandbreite in der NAS-Datenbank ab, oder, falls dort nicht existent, von der IODS-Master-Datenbank. Der Gatekeeper erhält auch Informationen über die verfügbaren Netzwerk-Ressourcen vom BAM. Der Gatekeeper führt dann einen Vergleich durch, um zu bestimmen, ob der im Dienstplan des Teilnehmers bereitgestellte Netzwerkzugang sich im Rahmen des Netzwerkzugangs befindet, welcher nach dem Zugangs-Regelwerk des Ressourcenanbieters den besuchenden mobilen Terminals gewährt wird, und ob ausreichende Netzwerk-Ressourcen zur Verfügung stehen, um das besuchende mobile Terminal aufzunehmen. Wenn der Gatekeeper bestimmt, dass der im Plan des Teilnehmers dargelegte Zugang autorisiert ist, und wenn ausreichende Netzwerk-Ressourcen, z.B. Bandbreite, verfügbar sind, um den besuchenden Teilnehmer aufzunehmen, wie bei **822** gezeigt, initiiert der Gatekeeper die drei Operationen **816, 817** und **818**.

[0179] Bei **816** kopiert der Gatekeeper bestimmte Benutzerprofilinformationen aus der IODS-Datenbank auf die lokale NAS-Datenbank. Die Benutzerprofilinformationen beinhalten vorzugsweise die Identifikationsinformationen des Teilnehmers aus der Teilnehmer-Tabelle **3100** und die Informationen über den mobilen Teilnehmer aus der Adapter-Tabelle **3400**.

[0180] Bei **817** kann der IODS wahlweise mit jedem vorhergehenden NAS kommunizieren, mit welchem der Teilnehmer eine Sitzung eröffnet hat, und den vorigen NAS diese Sitzung zugunsten der neuen Sitzung schließen lassen, welche mit dem neuen NAS eröffnet wird.

[0181] Bei **818** modifiziert der Gatekeeper den Status der MAC-Adresse in seinem IP-Filter **26** von „nicht weiterleiten" auf „Weiterleiten erlaubt". An dieser Stelle aktualisiert der Gatekeeper lediglich den IP-Filter, der mit einem eigenen Uplink-Anschluss in Verbindung steht, um dem besuchenden Teilnehmer den Zugriff auf den Uplink-Anschluss und somit auf das Internet zu ermöglichen. Der Gatekeeper aktualisiert den mit seinem privaten Netzwerk verbundenen IP-Filter nicht. Dies wird getrennt behandelt, wenn die Sicherheitsregelwerke des Teilnehmers in Verbindung mit der Host-Ressourcen-Zuteilungsverarbeitung in Schritt **820** verarbeitet werden.

[0182] An dieser Stelle wird das besuchende Terminal authentifiziert und hat Basisberechtigung zum Zugriff auf das Internet über den NAS, wie in **819** gezeigt. Vorzugsweise wird das besuchende mobile Terminal für zumindest den Basiszugriff auf das NAS-Uplink autorisiert, bevor eine vollständige Zuteilung von Netzwerk-Ressourcen durchgeführt wird. Dies geschieht deshalb, um Fehler und exzessive erneute Übertragungen zu vermeiden, wenn das besuchende mobile Terminal wichtige Netzwerkdienste während der Zeit benötigt, in der der Ressourcen-Zuteilungsprozess ausgeführt wird. Sobald das besuchende mobile Terminal authentifiziert ist, beginnt der Gatekeeper den Host-Ressourcen-Zuteilungsprozess in Schritt **820**.

[0183] Wenn jedoch der Gatekeeper in **824** bestimmt, dass der im Dienstplan des Providers zur Verfügung gestellte Zugang mit dem Regelwerk des Ressourcenanbieters betreffend den Zugang eines besuchenden Teilnehmers nicht kompatibel ist, oder dass ungenügende Netzwerk-Ressourcen zur Verfügung stehen, um den besuchenden Teilnehmer aufzunehmen, oder wenn das Regelwerk des Ressourcenanbieters oder des Teilnehmers es erforderlich macht, dass sich der Benutzer im Netzwerk anmeldet, dann leitet der Gatekeeper den besuchenden Teilnehmer zum

Registrierungsprozess zurück. Die Registrierungsseite enthält vorzugsweise Fehlermeldungen, welche dem besuchenden Teilnehmer den Grund für das Fehlschlagen des Zugriffs, wenn überhaupt, anzeigen. Darüber hinaus kann die Registrierungsseite dem besuchenden Teilnehmer helfen, die Situation zu korrigieren. Zum Beispiel kann das Netzwerkzugangs-Regelwerk des Ressourcenanbieters für besuchende Teilnehmer bestimmen, dass nur solchen Teilnehmern, die Prioritätsdienstpläne haben, Zugang gewährt wird. Das könnte z.B. der Fall sein, wenn der Ressourcenanbieter eine hohe Last an privaten Netzwerk-Clients hat, die Zugang zu einem öffentlichen Netzwerk benötigen. Der Ressourcenanbieter kann daher bestimmen, dass in Anbetracht der begrenzten Verfügbarkeit der Bandbreiten-Ressourcen des Netzwerks für besuchende Teilnehmer das Netzwerk nur jene besuchenden Teilnehmer aufnehmen kann, die über Prioritätsdienstvereinbarungen verfügen. In diesem Falle kann die Registrierungsseite dem besuchenden Teilnehmer die Möglichkeit anbieten, seinen Dienstplan von einem Nicht-Prioritätsplan auf einen Prioritätsplan heraufzustufen. Noch weitergehend kann die Registrierungsseite dem besuchenden Teilnehmer Informationen über die Verfügbarkeit von Netzwerk-Ressourcen für besuchende Teilnehmer hinsichtlich der vergangenen Tage oder Wochen liefern, um dem besuchenden Teilnehmer einen Hinweis zu geben, sofern und wann Netzwerk-Ressourcen verfügbar werden könnten. Die Informationen können z.B. dem besuchenden Teilnehmer anzeigen, dass routinemäßig zusätzliche Netzwerk-Ressourcen nach 18 Uhr verfügbar werden, wenn der Netzwerkverkehr aufgrund lokaler privater Netzwerk-Clients abnimmt. Wenn der besuchende Teilnehmer bestimmt, seine Dienstvereinbarung nicht heraufzustufen, oder falls dies nicht möglich ist, veranlasst der Gatekeeper die De-Authentifizierung und Beendigung der Verbindung mit dem besuchenden mobilen Terminal wie bei **828** gezeigt. Wenn der Teilnehmer zur Registrierungsseite zurückgeleitet wird, weil eine Anmeldung erforderlich ist, so erledigt die Registrierungsseite vorzugsweise die Authentifizierung des Benutzers und die Anmeldungsverarbeitung bei **840** und **841**, z.B. indem sie den Teilnehmer auffordert, den Anmeldenamen und das Passwort korrekt einzugeben. Wenn die Anmeldung nach einer vorher festgelegten Anzahl von Versuchen fehlschlägt, wie bei **843** gezeigt, wird der Teilnehmer erneut zur Registrierungsseite geleitet. Wenn die Anmeldung bei **842** erfolgreich abgeschlossen ist, geht der Prozess weiter, um die Arbeitsgänge **816, 817** und **818** auszuführen und den Authentifizierungsvorgang bei **819** abzuschließen.

[0184] **FIG. 9** veranschaulicht die Einzelheiten des Host-Ressourcen-Zuteilungs-Prozesses. In diesem Prozess teilt der Gatekeeper dem besuchenden Teilnehmer Netzwerk-Ressourcen zu und aktualisiert einige der Teilnehmer-Einträge. In **910** ruft der Gatekeeper das Benutzerprofil und die Dienstplaninformationen des besuchenden Teilnehmers, vorzugsweise von der lokalen Datenbank des NAS, wenn aber nicht dort, von der IODS-Master-Datenbank. Der Gatekeeper initiiert dann vier Threads bei **902, 903, 904** und **905**.

[0185] In **902** analysiert der Gatekeeper die Dienstvereinbarung des besuchenden Teilnehmers aus dem Benutzerprofil und bestimmt die Dienststufe, welche durch die Vereinbarung festgelegt wird. Unter Anwendung des BAM-Prozesses **28** und auf der Grundlage der in der Vereinbarung festgelegten Dienststufe bestimmt der Gatekeeper eine entsprechende Stufe der Baseline-QoS für den besuchenden mobilen Terminal und teilt eine Baseline-Bandbreite zu, wie im Einzelnen im Zusammenhang mit den **FIG. 17** und **18** beschrieben. Vorzugsweise leitet der Gatekeeper diese Parameter an den vorhandenen QoS-Dienst, z.B. RSVP („Resource ReSerVation Protocol"), zur Umsetzung bei den verwendbaren Anschlüssen des NAS. Wenn der NAS nicht selbst der Router zwischen den WAPs und dem Rest des Netzwerks ist, z.B. bei der in **FIG. 13** veranschaulichten, alternativen Ausführungsform, muss der NAS diese Parameter auf dem Router aktualisieren.

[0186] Bei **905** assoziiert der Gatekeeper eine IP-Adresse mit dem besuchenden mobilen Terminal. Dies erfolgt typischerweise auf herkömmliche Art und Weise durch den DHCP oder die DHCP-Relay-Komponente **31** im Falle, dass Netzwerke bei den IRTF IP-Version-4-Standards bleiben. Bei Netzwerken, die an den IETF IP-Version-6-Standards festhalten, werden die herkömmliche Router Discovery und Autokonfiguration verwendet. Weitere Einzelheiten dieses Prozesses werden mit Bezug auf **FIG. 11** veranschaulicht und beschrieben.

[0187] Bei **904** aktualisiert der Gatekeeper den Standort des besuchenden mobilen Terminals in der Adapter-Status-Tabelle **3700** der IODS-Master-Datenbank **3000**. Dies geschieht, um das mobile Terminal zwecks Weiterleitung von Echtzeit-Protokollen und des eingehenden Telefonverkehrs an das mobile Terminal leichter zu lokalisieren, wie bei **907** gezeigt.

[0188] Bei **903** verarbeitet der Gatekeeper die Sicherheitsregelwerke des Teilnehmers. Vorzugsweise fragt der Gatekeeper die Sicherheitsregelwerke des Teilnehmers bei der lokalen Version der Adapter-Tabelle **3400** in der Datenbank des NAS ab und bestimmt, ob die Sicherheitsregelwerke des Teilnehmers den Zugang zu dem privaten Netzwerk erlauben, was normalerweise der Fall ist, wenn der Teilnehmer auch ein autorisierter Client des privaten Netzwerks ist. Wenn der Zugang erlaubt wird, wie bei **908** gezeigt, aktualisiert der Gatekeeper den IP-Filter **26**, der mit dem privaten Netzwerkanschluss des NAS bei **910** verbunden ist, um dem mobilen Terminal Zugang zu dem privaten Netzwerk zu erlauben. Wenn der Zugang nicht erlaubt wird, wie bei **909** gezeigt, aktualisiert der Gatekeeper den IP-Filter nicht, und dem mobilen Terminal ist es dann nicht gestattet, Pakete in das lokale private Netzwerk weiterzuleiten.

[0189] Damit ist die Verarbeitung des Benutzerprofils durch den Gatekeeper abgeschlossen, wie bei **911** gezeigt. Als nächstes wendet sich der Gatekeeper seinen Abrechnungs- und Sitzungs-Management-Prozessen zu, wie bei **1000** gezeigt.

[0190] FIG. 10 veranschaulicht die Einzelheiten der Abrechnungs- und Sitzungs-Management-Prozessen. In diesen Prozessen initialisiert und aktualisiert der Gatekeeper die Sitzungseinträge des Teilnehmers, initialisiert und aktualisiert die Abrechnungsaufzeichnungen des Teilnehmers und überwacht die Nutzung des Netzwerks durch den Benutzer. Bei **1001** initialisiert der Gatekeeper die Sitzungseinträge des Teilnehmers, indem er eine lokale Version der Sitzungsaufzeichnungstabelle **3750** in der lokalen Datenbank des NAS erzeugt. Der Gatekeeper initialisiert die Sitzungseinträge mit der MAC-Adresse des mobilen Terminals mit der Zeit, zu welcher die Sitzung begann, und den Standort des mobilen Terminals. Wenn die lokale Datenbank des NAS gerade benutzt wird, um DHCP-Parameter für den mobilen Terminal in Verbindung mit der DHCP/DHCP-Relay-Komponente **31** zu speichern, speichert der Gatekeeper bei **1002** auch das DHCP IP-Adressen-Lease auf der lokalen Datenbank.

[0191] Bei **1003** überprüft der Netzwerkmessungs- oder Statistikerfassungsagent **29** des NAS, welcher in Bezug auf **FIG. 2** gezeigt und beschrieben ist, periodisch die Netzwerkaktivität des Teilnehmers. Dies geschieht entweder durch Abfrage des API des Netzwerks des Betriebssystems, wie vorher beschrieben, oder über SNMP. Vorzugsweise bestimmt der Agent jedes Mal, wenn er die Aktivität des Teilnehmers überprüft, welche Netzwerk-Webseiten der Teilnehmer besucht hat und wie viele Bits er gesendet und empfangen hat. Der Agent **29** kann für diese Zwecke herkömmliche Betriebssystemeinrichtungen verwenden. Z.B. kann im Fall von Windows 2000 und Windows NT über ein API auf einen besonderen Treiber, der als Netzwerk-Überwachungs-Agent bezeichnet wird, zugegriffen werden,

um den Sitzungsstatus abzufragen und diese Informationen an die lokale Datenbank des NAS zu übertragen. Vorzugsweise überprüft der Agent weiterhin periodisch die Netzwerkaktivität des Teilnehmers, bis sich der Teilnehmer mit Bestätigung vom Netzwerk trennt oder er beschlossen hat, inaktiv zu werden.

[0192] Wenn der WAP von der bevorzugten Art ist, welche eine API aufweist und auf die der NAS mittels Programmierung zugreifen kann, ist er vorzugsweise so konfiguriert, dass er den NAS informiert, wenn er eine Trennung des mobilen Terminals vom Netzwerk detektiert, wie bei **1006** und **1008** gezeigt. Das kann einfach bewerkstelligt werden, wenn der WAP SNMP unterstützt, indem er dieses so konfiguriert, dass es die Trennung als ein Ereignis erkennt und dem NAS nach dem Detektieren der Trennung eine Netzwerk-Benachrichtigung zukommen lässt. Wenn der WAP dem NAS meldet, dass das mobile Terminal sich vom Netzwerk getrennt hat, ändert der NAS bei **1012** den Status des mobilen Terminals in der lokalen Version der Adapter-Status-Tabelle **3700** auf „Knoten nicht mehr aktiv" ab, und geht zur Beendigung der Sitzung über.

[0193] Wenn dem NAS nicht anderweitig gemeldet wurde, dass das mobile Terminal sich vom Netzwerk getrennt hat, überprüft der Agent **29** vorzugsweise jedes Mal, wenn er die Netzwerkaktivität des mobilen Terminals überprüft, ob das mobile Terminal inaktiv geworden ist. Bei **1005** bestimmt der Agent **29**, ob es seit der letzten Überprüfung irgendeine Netzwerkaktivität seitens des mobilen Terminals gegeben hat. Dies kann dadurch geschehen, dass die Anzahl der Bits, die das mobile Terminal während der Sitzung bei dieser Überprüfung versendet und empfangen hat, mit der bei der letzten Überprüfung aufgezeichneten Anzahl derselben verglichen wird. Wenn seit der letzten Überprüfung keine Aktivität erfolgt ist, inkrementiert der Agent einen Knoteninaktivitätszähler bei **1007** und prüft nach, ob der Zähler bei **1009** einen vorgegebenen Schwellwert überstiegen hat. Wenn der Schwellwert überstiegen wurde, sendet der Agent ein ICMP-Paket an den mobilen Terminal bei **1010** und wartet auf eine Antwort. Wenn innerhalb einer vorgegebenen Zeit keine angemessene Antwort von dem mobilen Terminal ausgehend empfangen wird, stellt der Agent fest, dass das mobile Terminal im Netzwerk bei **1012** nicht mehr aktiv ist und geht zur Beendigung der Sitzung über. Wenn jedoch innerhalb einer vorgegebenen Zeit eine angemessene Reaktion von dem mobilen Terminal empfangen wurde, bestimmt der Agent bei **1011**, dass das mobile Terminal weiterhin aktiv ist, setzt den Inaktivitätszähler bei **1013** auf Null und kehrt zur periodischen Überprüfung der Netzwerkaktivität des mobilen Terminals zurück, wie bei **1003** gezeigt.

[0194] Bevorzugt aktualisiert der Agent jedes Mal, wenn er die Netzwerkaktivität des Teilnehmers überprüft, auch die Sitzungseinträge in der lokalen Datenbank des NAS mit der Anzahl von versendeten und empfangenen Bits, und den Webseiten, die der Teilnehmer besucht hat. Letztere Informationen sind vorzugsweise mit dem öffentlichen Schlüssel des Teilnehmers verschlüsselt, falls vorhanden, um nichtautorisierten Zugang zu verhindern.

[0195] Um eine Sitzung zu beenden, kennzeichnet der Gatekeeper die Sitzungseinträge in der lokalen Datenbank des NAS bei **1016** als geschlossen und repliziert die lokalen Sitzungseinträge in der Sitzungsaufzeichnungstabelle **3750** der IODS-Master-Datenbank **3000**, die in **FIG. 2** gezeigt ist. Bevorzugt werden die Sitzungseinträge mit dem öffentlichen Schlüssel des Integrationsbetreibers verschlüsselt, bevor sie repliziert werden, um nichtautorisierten Zugang zu verhindern. Ebenso bevorzugt wird vor der verschlüsselten Übertragung eine geeignete X.509 Zertifikatssperrliste („Certificate Revocation List" - CRL) konsultiert, um sicherzugehen, dass der öffentliche Schlüssel des Integrationsbetreibers noch korrekt ist. Bei **1015** aktualisiert der Gatekeeper auch die IP-Filter **26** für die geeigneten Anschlüsse, d.h. die Anschlüsse für den Downlink-, den Uplink- und das private Netzwerk, wie

erforderlich, um alle Berechtigungen für das mobile Terminal zum Weiterleiten oder Empfangen von Paketen über das Netzwerk zu entfernen. Hiermit ist die Sitzung beendet, wie bei **1017** gezeigt.

[0196] Der Fachmann weiß, dass viele andere Prozesse neben den beschriebenen Prozessen des Gatekeepers im Netzwerk gleichzeitig nebeneinander laufen können. Alt-AAA und Remote-Client-Anwendungs-Prozesse, Mobile-IP-Heim- und Foreign-Agent-Aktivitäten, IPSec, DHCP, und Router-Discovery-Prozesse z.B. können alle weiterlaufen. Da diese Prozesse alle von herkömmlicher Art sind und von den Gatekeeper-Prozessen nicht verändert werden, sofern hierin nicht anders beschrieben, ist es nicht erforderlich, sie hier im Detail zu beschreiben, und deshalb wird auf eine solche Beschreibung verzichtet.

[0197] FIG. 11 veranschaulicht die Einzelheiten der Verfahren, mit welchen der Gatekeeper einem mobilen Terminal eine IP-Adresse zuteilt, wie an der Stelle **905** der **FIG. 9** ausgewiesen. Ein mobiles Terminal erhält seine Netzwerk-Konfigurationsparameter einschließlich einer IP-Adresse auf eine von drei Arten. Das mobile Terminal kann seine Parameter entweder manuell oder automatisch selbst konfigurieren, wie bei **1101** gezeigt, das mobile Terminal kann das Dynamic-Host-Configuration-Protocol-(DHCP)Verfahren anwenden, wie bei **1102** gezeigt, oder das mobile Terminal kann seine Konfigurationsparameter über seinen Mobile-IP-Stapel erhalten, wie bei **1103** gezeigt.

[0198] Wie bei **1101** gezeigt, sendet das mobile Terminal bei Netzwerken, die den Standards der IETF IP Version 6 entsprechen, eine Router-Discovery-Anfrage, um die Netzwerk-Konfiguration zu bestimmen, und konfiguriert dann automatisch seine Netzwerkparameter selbst. Dies kann auch manuell geschehen. In diesem Falle ist der Gatekeeper nicht an der Zuteilung einer IP-Adresse an das mobile Terminal beteiligt, und er geht sofort zu den Host-Sitzungsabrechnungs- und Verwaltungsfunktionen weiter, die in Verbindung mit **FIG. 10** veranschaulicht und beschrieben werden.

[0199] Beim zweiten Ansatz, der bei **1102** gezeigt ist, sendet herkömmliche DHCP-Agent-Software auf dem mobilen Terminal eine DHCP-Discovery-Anfrage über das Netzwerk, welche vom NAS bei **1104** empfangen wird. Wenn der NAS einen DHCP-Relay-Agent **31** implementiert, anstatt einem DHCP-Server selbst, leitet der NAS die Anfrage bei **1105** und **1106** an den DHCP-Server weiter. Wenn der DHCP-Server die DHCP-Server-Ermittlungsanfrage empfängt, geht der DHCP-Server bei **1107** daran, ein DHCP-Konfigurationsangebot zu erstellen. Das Konfigurationsangebot enthält Informationen, welche durch Abfrage eines Profils der NAS-Ressourcen bei **1108** erhalten wurden, wobei die IP-Adresse des NAS die Anfrage bei **1109**, die MAC-Adresse des mobilen Terminals bei **1110** und die Abrechnungseinzelheiten des Teilnehmers bei **1111** erledigt. Die NAS-Ressourcen umfassen die Identifizierung von IP-Subnetzen, die für den NAS spezifisch sind (wie z.B. privates LAN-Subnetz und öffentliches Netzwerk-Subnetz) sowie andere IP-Ressourcen, welche der NAS den Clients zur Verfügung stellt, wie z.B. Telefon-Gateways und verschiedene Anschlüsse. Diese Informationen sind zusammen mit der NAS-IP-Adresse und der MAC-Adresse des mobilen Terminals einfach erhältlich über die DHCP-Ermittlungsanfrage. Die Abrechnungsinformationen des Teilnehmers sind vorzugsweise von dem NAS über dessen lokale Datenbank erhältlich, oder mittelbar von der IODS-Datenbank über den NAS. Diese Abrechnungsinformationen werden vorzugsweise dazu benutzt, zu identifizieren, zu welchen Subnetzen dem Teilnehmer der Zugang erlaubt ist.

[0200] Als nächstes generiert der Server bei **1112** und **1113** ein herkömmliches DHCP-Angebot einschließlich einer IP-Adresse und sendet dies an das mobile Terminal. Das mobile Terminal akzeptiert das Angebot, wie bei **1114**

gezeigt, indem es eine Empfangsbestätigung (ACK) ausstellt. Wenn ein ACK empfangen wird, ist die IP-Adresse zugeteilt worden, und der Gatekeeper geht weiter zu den Sitzungsabrechnungs- und Verwaltungsverfahren, wie hinsichtlich **FIG. 10** gezeigt und beschrieben. Wenn jedoch das mobile Terminal das Angebot ablehnt, wie bei **1115** gezeigt, generiert der DHCP-Server vorzugsweise ein Ereignis, welches auf dem SNMP oder einer geeigneten Ereignisverwaltungs- und Aufzeichnungsanwendung bei **1116** aufgezeichnet wird. Der Gatekeeper geht dann weiter zu den Sitzungsabrechnungs- und Verwaltungsverfahren von **FIG. 10**. Wenn die Übersendung eines ACK (NACK) fehlschlägt, so wird dies als Ablehnung angesehen.

[0201] Der dritte Ansatz, der bei **1103** gezeigt wird, setzt das Vorhandensein der bevorzugten Mobile-IP-Unterstützungskomponente **33** des NAS voraus, wie in **FIG. 3** gezeigt. In diesem Ansatz gibt das mobile Terminal eine Mobile-IP-Konfigurationsanfrage aus, welche vom NAS bei **1117** empfangen wird. Daraufhin führt der NAS die bei **1108-1111** ausgewiesenen Funktionen durch und erhält die erforderlichen Mobile-IP-Konfigurationsparameter. Dann sendet der NAS die Konfigurationsparameter bei **1118** zurück zu dem mobilen Terminal. Nach Empfang bei **1113** akzeptiert das mobile Terminal die Parameter oder lehnt diese bei **1114** und **1115** ab. Nach Akzeptierung geht der Gatekeeper weiter zu den Sitzungsabrechnungs- und Verwaltungsverfahren von **FIG. 10**. Jede Ablehnung löst bevorzugt ein Ereignis aus, welches durch SNMP oder einer geeigneten Ereignisverwaltungs- und Aufzeichnungsanwendung bei dem DHCP-Server aufgezeichnet wird. Der Gatekeeper geht dann weiter zu den Sitzungsabrechnungs- und Verwaltungsverfahren von **FIG. 10**.

[0202] **FIG. 12** veranschaulicht die Einzelheiten der Sicherheitsverfahren, die im Allgemeinen an der Stelle **815** von **FIG. 8** ausgewiesen sind. Zusätzlich veranschaulicht **FIG. 12** die Einzelheiten von Verfahren zur Verhütung von betrügerischen Eingriffen bei den Abrechnungscodes. Die Sicherheitsverfahren werden durch das Auftreten einer jeden von sieben Sicherheitssituationen ausgelöst.

[0203] Die erste Situation besteht im Empfangen von Ressourcenanbieter-Rechnungen, welche nicht mit einem vorbestimmten Profil übereinstimmen. Dies wird bei **1224** gezeigt. Die IODS-Master-Datenbank hat genügend Informationen über Ressourcenanbieter, um ein Profil für jeden Anbieter auf der Grundlage solcher Faktoren, wie z.B. dem Standort des Ressourcenanbieters, die Zellengröße und die Uplink-Kapazität, zu erstellen. Des Weiteren ermöglicht es der Standort des Ressourcenanbieters, das Profil um Informationen zu erweitern, welche die Bevölkerung und das allgemeine Wohlstandsniveau der Bevölkerung betreffen. Aus diesen Profilinformationen kann der Integrationsbetreiber ganz einfach Algorithmen erstellen, so dass, wenn Rechnungen von Ressourcenanbietern empfangen werden, detektiert werden kann, ob die Rechnungen mit dem Profil unvereinbar sind. Zum Beispiel könnte ein Ressourcenanbieter mit einer 56K-Verbindung im ländlichen Raum in Idaho Verdacht erregen, wenn er plötzlich anfangen würde, Rechnungen an den IODS zu senden, welche sehr hohe Netzwerkverkehrsniveaus angeben.

[0204] Außerdem werden Ressourcenanbieter vorzugsweise vom Erstellen falscher Rechnungs-Einträge über nicht vorhandenen (virtuellen) Netzwerkverkehr oder von Eingriffen in die lokale NAS-Datenbank abgehalten. Vorzugsweise verschlüsselt der Gatekeeper die Abrechnungseinträge, die in der lokalen NAS-Datenbank gespeichert sind, mit dem öffentlichen Schlüssel des Integrationsbetreibers, wie vorher beschrieben, wodurch einem skrupellosen Ressourcenanbieter der Zugang verwehrt bleibt. Da der Gatekeeper durch einen Ressourcenanbieter nicht modifiziert werden kann, besteht der einzige Weg für einen Ressourcenanbieter, Verkehr durch seine Netzwerkanbindung

herzustellen, darin, den Verkehr tatsächlich von einem drahtlosen mobilen Terminal aus durch den lokalen Uplink-Anschluss weiterzuleiten.

[0205] Die zweite Situation ist das Detektieren eines mobilen Terminals, das mit einem NAS an einem Standort Verbindung hat, der weiter als eine vorgegebene Entfernung von dem letzten NAS weg ist, mit dem es verbunden ist, und dies in weniger als einer vorher festgelegten Zeit. Dies wird in **1202** gezeigt. Die dritte Situation ist das Detektieren von mobilen Terminals, welche dieselbe MAC-Adresse haben und gleichzeitig an zwei verschiedenen Standorten Verbindung zum Netzwerk zu bekommen versuchen oder mit diesem verbunden sind. Dies wird in **1203** gezeigt. Jede dieser Situationen deutet darauf hin, dass zumindest eines der mobilen Terminals eine falsche MAC-Adresse benutzt. Der Standort und die MAC-Adresse eines mobilen Terminals, das Verbindung mit dem Netzwerk hat, werden in der IODS-Master-Datenbank zum Zeitpunkt der Verbindung gespeichert, wie vorher beschrieben. Somit ist es relativ einfach, zu detektieren, wann „dasselbe" mobile Terminal behauptet, zur selben Zeit an zwei verschiedenen Standorten zu sein, oder an einem Standort zu einem Zeitpunkt und an einem anderen Standort in gewisser Entfernung davon, und dies in weniger als einem Minimum an Zeit, das erforderlich ist, um dorthin zu gelangen. Der Fachmann erkennt, dass beim Ermitteln der Wegzeit für diesen Zweck der Standort des WAP zu berücksichtigen ist, über den das mobile Terminal verbunden ist. Zum Beispiel könnte die geschätzte Mindestzeit für den Weg zwischen zwei WAPs, die sich an zwei verschiedenen Flughäfen befinden, weit weniger betragen als die geschätzte Mindestzeit für den Weg über dieselbe Distanz zwischen zwei Punkten, die nicht durch gewerblichen Luftverkehr verbunden sind. Das Einstellen der Zeitparameter müsste deshalb sorgfältig überlegt werden, um das Auftreten von Fehlalarmen gering zu halten.

[0206] Die vierte Situation besteht im Feststellen, dass der gegenwärtige Abrechnungsbetrag für einen Teilnehmer ein vorgegebenes Mehrfaches des Abrechnungsbetrages für die gesamte letzte Abrechnungsperiode überstiegen hat, wie bei 1**204** gezeigt. Diese Situation ist leicht zu ermitteln, indem man die gegenwärtigen und die vorhergehenden Kosten mit denen eines Teilnehmers in der IODS-Teilnehmerkonto-Status-Tabelle **3800** vergleicht. Diese Situation tritt normalerweise aufgrund einer nichtautorisierten Benutzung des mobilen Terminals des Teilnehmers durch eine andere Person ein, z.B. aufgrund von Diebstahl oder dergleichen.

[0207] Die fünfte Situation ist das Detektieren mehrfacher fehlgeschlagener Anmeldeversuche, wie bei 1**205** gezeigt. Diese Situation tritt typischerweise bei Geräten mit interaktiven Anmeldemöglichkeiten zur Verbindung mit Firmennetzwerken oder dergleichen auf. Solche Geräte versuchen automatisch, sich bei verschiedenen Netzwerkverbindungen anzumelden, in deren Nähe sie kommen, haben aber typischerweise keinen Erfolg, weil sie lediglich für die Anmeldung beim Firmennetzwerk konfiguriert sind. Da erfolglose Anmeldeversuche aufgezeichnet und gespeichert werden, wie vorher beschrieben, ist dies eine relativ leicht festzustellende Situation.

[0208] Die sechste und die siebente Situation bestehen im Empfangen von Informationen aus einer externen Quelle, wie bei 1**206** gezeigt, und dem Empfangen einer Beschwerde von einem Ressourcenanbieter oder einem Teilnehmer wegen einer Abrechnung, wie bei **1225** gezeigt.

[0209] Vorzugsweise ist das Verwaltungsnetzwerksystem, z.B. SNMP, so konfiguriert, dass das Auftreten irgendeiner der oben aufgeführten Situationen bei **1206** als ein Ereignis identifiziert wird. Ebenfalls bevorzugt ist das Netzwerkmanagementsystem konfiguriert, um einem ausgewählten Personal des Integrationsbetreibers als Reaktion auf das Ereignis bei **1208** Meldung zu machen.

[0210] Als nächstes wird ein Prozess zur Identifizierung des Eindringlings bei **1209** initiiert. Der ausgewählte Sicherheitsdienst des Integrationsbetreibers analysiert die verfügbaren Informationen und versucht zu ermitteln, ob er zwischen dem Teilnehmer, dem Ressourcenanbieter und dem mutmaßlichen Eindringling bei **1210** und **1212** unterscheiden kann, oder ob, bei **1211**, das Vorkommnis ein falscher Alarm ist. Vorausgesetzt, das Vorkommnis wird nicht als ein falscher Alarm eingestuft und das Personal ist imstande, zwischen den drei Entitäten zu unterscheiden, so meldet das Personal vorzugsweise dem Teilnehmer und dem Ressourcenanbieter bei **1207** und **1212** das Vorkommnis, kontaktiert den mutmaßlichen Eindringling über das Netzwerk und fordert ihn bei **1214** auf, seine Identität nachzuweisen. Dies kann z.B. dadurch geschehen, dass von registrierten Teilnehmern verlangt wird, einige persönliche Informationen, die nur ihnen bekannt sind, als Teil des Registrierungsprozesses zu liefern. Informationen wie z.B. der Mädchenname der Mutter sind ein geeignetes Beispiel.

[0211] An diesem Punkt kann die Ergreifung des Eindringlings bei **1215** versucht werden, indem die Netzwerkaktivität des Eindringlings überwacht wird und der Versuch gemacht wird, den Eindringling zu lokalisieren. Bei **1217** können auch Strafverfolgungsbehörden benachrichtigt werden. An dieser Stelle kann eine von drei Situationen auftreten: Der Eindringling wird bei **1221** erfolgreich lokalisiert und ergriffen, der Eindringling bemerkt die Entdeckung und entkommt der Ergreifung bei **1218**, oder der Eindringling kann nicht lokalisiert werden und bemerkt den Entdeckungs- und Ergreifungsversuch bei **1219** nicht.

[0212] Falls der Eindringling den Entdeckungsversuch bemerkt und der Ergreifung entgeht, werden vorzugsweise die Zugangsparameter des Teilnehmers bei **1220** geändert, um dem Eindringling den weiteren unautorisierten Zugang zum Netzwerk zu verwehren. Falls der Eindringling ergriffen wird, kann bei **1222** und **1223** ermittelt werden, ob der Eindringling ein betrügerischer Ressourcenanbieter oder ein Übertreter, wie z.B. ein Hacker ist, und geeignete Maßnahmen können ergriffen werden. Darüber hinaus werden in jeder Situation, in der durch den Sicherheitsdienst ermittelt wird, dass es einen Eindringling gibt, vorzugsweise die oben beschriebenen Betrugsaufdeckungsparameter modifiziert, um an dem Standort restriktiver zu werden, wo der Eindringling sich Zugang zum Netzwerk verschafft hat, sowie über einen vorher festgelegten nachfolgenden Zeitraum. Nach diesem Zeitpunkt, oder wenn der Eindringling letztendlich detektiert und erfolgreich ergriffen worden ist, werden die Betrugsaufdeckungsparameter vorzugsweise wieder auf ihre ursprünglichen Werte zurückgesetzt.

[0213] FIG. 14 stellt eine zusammenfassende Darstellung von bevorzugten Sicherheitsvorkehrungen bereit, um die Vertraulichkeit und Authentizität von Kommunikationen in der vorliegenden Erfindung zu gewährleisten. Im Allgemeinen wird die Sicherheit vorzugsweise durch eine Verschlüsselungskombination von Verbindungsschicht, Netzwerkschicht und Anwendungsschicht gewährleistet. **FIG. 14** benennt eine Anzahl von möglichen kryptographischen Endpunkten im Netzwerk, d.h., das mobile Terminal **1**, die WAPs **3**, **4**, NAS **7**, der lokale Loop-Router **14**, IODS **18**, und ein möglicher Korrespondenz-Knoten **1057** sowie sein assoziierter Heim-Netzwerk-Router oder -Agent **1506**. Vorzugsweise verwendet jeder der Endpunkte eine herkömmliche Infrastrukturtechnologie mit hinterlegtem öffentlichen Schlüssel („Public Key Infrastructure" – PKI), um in der Lage zu sein, sichere Kommunikationskanäle auszuhandeln, ohne notwendigerweise vorher voneinander Kenntnis haben zu müssen. Diese Funktion wird durch eine herkömmliche Zertifizierungsautorität **1516** bereitgestellt, die öffentliche Schlüssel für jede der Komponenten verwaltet und zur Verfügung stellt, und die vorzugsweise für jede der Komponenten entweder direkt oder eventuell indirekt über den IODS zugänglich ist.

[0214] Es gibt im Wesentlichen fünf Netzwerkkommunikationssegmente, die gesichert werden müssen. Sobald diese durch die Anwendung von geeigneter Verschlüsselung gesichert sind, werden sie als „verschlüsselte Transporte" bezeichnet. Das erste Netzwerkkommunikationssegment **1508** befindet sich zwischen dem mobilen Terminal und dem WAP. Dieses Segment wird bevorzugt zu einem verschlüsselten Transport gemacht, indem eine verschlüsselte Sitzung über die Verbindungsschicht zwischen dem mobilen Terminal und dem WAP hergestellt wird, falls möglich. Wie vorher beschrieben, gibt es mindestens zwei Wege, um dies zu erreichen. Erstens, wenn das mobile Terminal und der WAP verschlüsselungskompatibel sind, können sie eine verschlüsselte Sitzung über die Verbindungsschicht aushandeln, die einen oder mehrere native Schlüssel verwendet, die lokal auf dem WAP gespeichert sind. Alternativ kann, falls der WAP mittels Programmierung durch den NAS **7** steuerbar ist, der NAS dem WAP einen oder mehrere Schlüssel von der Zertifizierungsautorität zur Verfügung stellen, und das mobile Terminal kann die geeigneten Schlüssel vom IODS erhalten, um die Einrichtung einer verschlüsselten Sitzung über die Verbindungsschicht zu ermöglichen. Schlimmstenfalls kann dieses Segment, wenn keiner der Ansätze verfügbar oder anwendbar ist, ungesichert bleiben, damit das mobile Terminal Verbindung zum Netzwerk bekommt.

[0215] Das zweite Segment **1509** befindet sich zwischen dem mobilen Terminal und dem NAS. Dieses Segment wird vorzugsweise zu einem verschlüsselten Transport gemacht, indem das mobile Terminal mit einem geeigneten Security-Client wie z.B. IPSec, ESP oder AH, oder einem Legacy-Remote-Client oder AAA-Client, wie z.B. Radius oder Diameter, versehen wird. In diesem Falle wird die Verschlüsselung auf der Netzwerkschicht **3** durchgeführt.

[0216] Das dritte Segment **1510** befindet sich zwischen dem Host und dem IODS. Dieses Segment wird ebenfalls vorzugsweise ähnlich wie das zweite Segment zu einem verschlüsselten Transport gemacht, indem das mobile Terminal mit einem geeigneten Security-Client wie z.B. IPSec, falls verfügbar, ausgestattet wird, und die Verschlüsselung auf der Netzwerkschicht **3** stattfindet.

[0217] Das vierte Segment **1511** befindet sich potentiell zwischen dem mobilen Terminal und dem Heim-Netzwerk-Router oder -Agent **1506** eines Korrespondenz-Knotens **1507**. Dieses Segment wird vorzugsweise zu einem verschlüsselten Transport gemacht, indem die Einrichtung der IETF Mobile-IP Standard's Security Association verwendet wird. Alternativ kann, wie bei den Segmenten **2** und **3**, ein sicherer Fernzugangs-Client auf dem mobilen Terminal zur Verfügung gestellt werden, wie z.B. Radius, Diameter, PPTP oder IPSec, falls verfügbar.

[0218] Das fünfte Segment **1512** befindet sich zwischen dem mobilen Terminal und einem potentiellen mobilen, entfernten Korrespondenz-Knoten **1507**. Wie das dritte und das vierte Segment wird dieses Segment bevorzugt zu einem verschlüsselten Transport gemacht, indem ein IPSec oder ähnlicher Sicherheits-/Verschlüsselungs-Client auf dem mobilen Internet-Terminal verwendet wird, falls verfügbar.

[0219] Zusätzlich oder als Alternative zu den vorerwähnten Ansätzen, von denen einige es vielleicht erfordern, dass das mobile Terminal einen zusätzlichen Sicherheits-Client hat, stellen die auf dem Netzwerk laufenden Anwendungen vorzugsweise die Verschlüsselung auf der Anwendungsebene bereit, z.B. unter Verwendung des Secure Sockets Layer-(SSL)Protokolls.

[0220] Zusätzlich zu den vorstehenden Ansätzen, von denen bei jedem das mobile Terminal einer der End-Knoten ist, kann die Verschlüsselung auch zwischen Zwischen-Knoten bereitgestellt werden, die als Sicherheits-Gateways fungieren. Dieser Ansatz erfordert nicht, dass das mobile Terminal über einen Security-Client wie z.B. IPSec verfügt,

um die Verschlüsselung zur Verfügung zu stellen. Es ist jedoch weiterhin bevorzugt, dass, falls überhaupt möglich, das mobile Terminal eine verschlüsselte Sitzung über die Verbindungsschicht mit dem WAP und vorzugsweise mit dem NAS herstellt, so dass Kommunikationen mit dem mobilen Terminal von Ende zu Ende sicher sind. Bei diesem Ansatz verwendet der NAS bevorzugt IPSec, um einen sicheren Kommunikationstunnel **1513, 1514, 1515** zu dem am weitesten entfernten Knoten herzustellen, welcher in der Lage ist, eine Sicherheitsverknüpfung mit dem NAS auszuhandeln. Dieser Ansatz hat den zusätzlichen Vorteil, dass er es dem NAS ermöglicht, dieselbe Datenbank für Anwendungsklassifizierung zu verwenden, die hinsichtlich des QoS-Systems beschrieben ist, um zu bestimmen, ob der Verkehr durch den Tunnel geleitet werden soll, was langsamer geht, oder ob Daten unverschlüsselt zu übermitteln sind. Wenn z.B. die Tunnel-Umlaufzeit 150 ms übersteigt, die Standard-Route aber nicht, so könnte die Standard-Route für zeitsensible Datenklassen, z.B. Sprache, verwendet werden, während der Tunnel für Daten genutzt werden könnte, welche relativ wenig zeitsensibel sind, wie z.B. E-Mail. Des Weiteren ist es bei diesem Ansatz so, dass sogar dann, wenn das mobile Terminal nicht imstande ist, eine verschlüsselte Sitzung über die Verbindungsschicht mit dem WAP herzustellen und keinen geeigneten Security-Agent hat, die Sicherheit immer noch zwischen dem NAS und anderen Remote-Netzwerk-Knoten gewährleistet ist.

[0221] Der Fachmann wird erkennen, dass die Verschlüsselung des gesamten im Netzwerk fließenden Verkehrs Auswirkungen in Bezug auf das Funktionieren der BAM- und QoS-Funktionen des Systems hat. Deshalb sollen QoS-Informationen bevorzugt in nicht-verschlüsseltem Zustand übermittelt werden. Dies ermöglicht es dem NAS, dem Verkehr, welcher z.B. RSVP oder DIFFSERV verwendet, gemäß den vorher beschriebenen QoS-Methoden und Regelwerken den Vorrang zu geben.

[0222] Im Vorstehenden werden gegenwärtig bevorzugte Ausführungsformen der Erfindung beschrieben. Der Fachmann wird feststellen, dass zahlreiche Hinzufügungen und Änderungen bei den beschriebenen Ausführungsformen vorgenommen werden können, und zwar unter Beibehaltung der Merkmale und Vorteile, welche die Erfindung charakterisieren, und ohne vom Geist derselben abzuweichen. Die vorstehenden Beschreibungen sollen deshalb von beispielhafter und nicht von beschränkender Art sein, und der Geltungsbereich der Erfindung wird lediglich durch die angefügten Ansprüche in ihrer ordnungsgemäßen Auslegung definiert.

Ansprüche:

1. System zur Bereitstellung eines kontrollierten Zugangs zu einem öffentlichen Netzwerk für Terminals unter Benutzung der öffentlichen Netzwerkverbindung eines privaten Netzwerks, umfassend:

einen Netzwerkzugangspunkt zur Einrichtung einer Netzwerkverbindung mit einem Terminal;

einen Netzwerk-Zugangs-Server;

eine erste Netzwerkschnittstelle zwischen dem Netzwerk-Zugangs-Server und dem Netzwerkzugangspunkt;

eine zweite Netzwerkschnittstelle zwischen dem Netzwerk-Zugangs-Server und der öffentlichen Netzwerkverbindung des privaten Netzwerks;

wobei der Netzwerk-Zugangs-Server konfiguriert ist, um eine Netzwerkverbindung zwischen einem Terminal herzustellen und zu steuern, der eine Netzwerkverbindung mit dem Netzwerkzugangspunkt und dem öffentlichen Netzwerk durch die öffentliche Netzwerkverbindung des privaten Netzwerks hat, ohne dass eine Netzwerkverbindung zwischen dem Terminal und dem privaten Netzwerk hergestellt wird.

2. System nach Anspruch 1, wobei der Netzwerkzugangspunkt eine drahtlose Netzwerkschnittstelle zur Herstellung einer drahtlosen Netzwerkverbindung mit einem Terminal aufweist.

3. System nach Anspruch 1, wobei das Terminal eine drahtlose Netzwerkschnittstelle zur Herstellung einer Netzwerkverbindung mit dem Netzwerkzugangspunkt aufweist.

4. System nach Anspruch 3, wobei das Terminal ein mobiles Terminal ist.

5. System nach Anspruch 4, wobei das Terminal und der Netzwerkzugangspunkt über das Bluetooth-Protokoll kommunizieren.

6. System nach Anspruch 4, wobei das Terminal und der Netzwerkzugangspunkt über das IEEE 802.11X Drahtlos-LAN-Protokoll kommunizieren.

7. System nach Anspruch 1, umfassend eine dritte Netzwerkschnittstelle zwischen dem Netzwerk-Zugangs-Server und dem privaten Netzwerk, um die Netzwerkkommunikation zwischen dem Netzwerk-Zugangs-Server und dem privaten Netzwerk zu ermöglichen.

8. System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server an dem Netzwerkzugangspunkt untergebracht ist.

9. System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server und der Netzwerkzugangspunkt in einem Computer nebeneinander untergebracht sind.

10. System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server in einem Computer untergebracht ist und wobei der Computer eine Schnittstelle zwischen dem Netzwerkzugangspunkt und dem privaten Netzwerk umfasst.

11. System nach Anspruch 7, wobei der Netzwerk-Zugangs-Server in der dritten Netzwerkschnittstelle untergebracht ist.

12. System nach Anspruch 11, wobei die dritte Netzwerkschnittstelle einen lokalen Netzwerk-Adapter (Local Area Adapter, LAN) umfasst.

13. System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server Software zum Registrieren von Terminals und Software zur Beschränkung des Zugangs für registrierte Terminals zum öffentlichen Netzwerk umfasst.

14. System nach Anspruch 7, wobei der Netzwerk-Zugangs-Server Einrichtungen enthält, die den Terminals den Zugang zum privaten Netzwerk unmöglich machen.

15. System nach Anspruch 14, wobei die Einrichtungen Funktionen zum Konfigurieren eines separaten öffentlichen Zugangs und privater Zugangs-Subnetze aufweisen.

16. System nach Anspruch 14, wobei diese Einrichtungen einen IP-Adressfilter beinhalten.

17. System nach Anspruch 7, wobei der Netzwerk-Zugangs-Server Software enthält, die das Verschlüsseln und Entschlüsseln von Daten ermöglicht, die von dem mobilen Terminal über das öffentliche Netzwerk gesendet und empfangen wurden.

18. System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server Einrichtungen zum dynamischen Bereitstellen von Netzwerkkonfigurationsdaten an die Terminals umfasst.

19. System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server Einrichtungen umfasst, um Daten weiterzuleiten, die zu und von dem mobilen Terminal über das öffentliche Netzwerk kommuniziert wurden.

20. System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server Software zur Steuerung der Bandbreitennutzung durch die Terminals umfasst.

21. System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server Software für die Überwachung und Aufzeichnung der Netzwerknutzung durch die Terminals umfasst.

22. System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server Software zur Bereitstellung mobiler IP-Unterstützung für die drahtlosen, mobilen Terminals umfasst.

23. System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server eine Datenbank zur Speicherung von ausgewählten Informationen umfasst, die registrierte Terminals betreffen.

24. Das System nach Anspruch 1, wobei der Netzwerk-Zugangs-Server Einrichtungen zur Bereitstellung von Telefondiensten an die mobilen Terminals umfasst.

25. System nach Anspruch 1, welches ein Integrationsbetreibernetz enthält, welches angepasst ist, mit dem Netzwerk-Zugangs-Server über das öffentliche Netzwerk zu kommunizieren, wobei das Integrationsbetreibernetz Einrichtungen zur Verwaltung des Zugangs zum öffentlichen Netzwerk durch das mobile Terminal über den Netzwerk-Zugangs-Server umfasst.

26. System nach Anspruch 25, wobei das Integrationsbetreibernetz eine zentrale Datenbank zur Speicherung ausgewählter Informationen über die Netzwerk-Zugangs-Server und die registrierten Terminals sowie Regelwerke für ausgewählten Netzwerkzugang und Nutzung umfasst.

27. System nach Anspruch 25, wobei die ausgewählten Informationen über die Netzwerk-Zugangs-Server zumindest eines von Provideridentifizierung, Informationen zur Netzwerkkonfiguration, Datenverschlüsselungsinformationen, Informationen zum Regelwerk für Netzwerknutzung und Informationen zur Anbieterabrechnung enthalten.

28. System nach Anspruch 25, wobei die ausgewählten Informationen über die registrierten Terminals zumindest eines von autorisierter Benutzeridentität, Terminaladresse, Regelwerk zur Terminalsicherheit, Identifizierung des Terminal-Dienstplans, Informationen über Datenverschlüsselung, Terminalstatus im Netzwerk, Informationen über die Abrechnung der Netzwerknutzung enthalten.

29. System nach Anspruch 25, wobei die ausgewählten Netzwerkzugangs- und Nutzungsregelwerke zumindest eines von Informationen zum Regelwerk über den Zugang zum öffentlichen Netzwerk, Informationen zum Regelwerk über die Bandbreitennutzung und Informationen zum Regelwerk über die Netzwerkverkehrspriorität enthalten.

30. Verfahren zur Bereitstellung von kontrolliertem Zugang für Terminals zu einem öffentlichen Netzwerk unter Verwendung der öffentlichen Netzwerkanbindung eines privaten Netzwerks, umfassend:

Bereitstellung eines Netzwerkzugangspunktes zur Herstellung einer Netzwerkverbindung mit dem Terminal;

Bereitstellung eines Netzwerk-Zugangs-Servers;

Bereitstellung einer ersten Netzwerkschnittstelle zwischen dem Netzwerk-Zugangs-Server und dem Netzwerkzugangspunkt;

Bereitstellung einer zweiten Netzwerkschnittstelle zwischen dem Netzwerk-Zugangs-Server und der öffentlichen Netzwerkanbindung des privaten Netzwerks;

Konfiguration des Netzwerk-Zugangs-Servers, um eine Netzwerkverbindung zwischen dem Terminal, welches eine Netzwerkverbindung zu dem Netzwerkzugangspunkt hat, und dem öffentlichen Netzwerk über die öffentliche Netzwerkverbindung des privaten Netzwerks einzurichten, ohne dass eine Netzwerkverbindung zwischen dem Terminal und dem privaten Netzwerk eingerichtet wird.

31. Verfahren nach Anspruch 30 einschließlich der Bereitstellung des Netzwerkzugangspunkts mit einer drahtlosen Netzwerkschnittstelle zum Einrichten einer drahtlosen Netzwerkverbindung mit dem Terminal.

32. Verfahren nach Anspruch 31 einschließlich der Bereitstellung an das Terminal einer drahtlosen Netzwerkschnittstelle zum Einrichten einer drahtlosen Netzwerkverbindung mit dem Netzwerkzugangspunkt.

33. Verfahren nach Anspruch 32, wobei das Terminal ein mobiles Terminal ist.

34. Verfahren nach Anspruch 33, wobei das Terminal und der Netzwerkzugangspunkt über das Bluetooth-Protokoll kommunizieren.

35. Verfahren nach Anspruch 33, wobei das Terminal und der Netzwerkzugangspunkt über das IEEE 802.11X Drahtlos-LAN-Protokoll kommunizieren.

36. Verfahren nach Anspruch 30 einschließlich der Bereitstellung einer dritten Netzwerkschnittstelle zwischen dem Netzwerk-Zugangs-Server und dem privaten Netzwerk, um die Netzwerkkommunikation zwischen dem Netzwerk-Zugangs-Server und dem privaten Netzwerk zu ermöglichen.

37. Verfahren nach Anspruch 30 einschließlich der Anbindung des Netzwerk-Zugangs-Servers an den Netzwerkzugangspunkt.

38. Verfahren nach Anspruch 30 einschließlich der Integrierung des Netzwerk-Zugangs-Servers in den Netzwerkzugangspunkt.

39. Verfahren nach Anspruch 30 einschließlich der Integrierung des Netzwerk-Zugangs-Servers in einen Computer, welcher eine Schnittstelle zwischen dem Netzwerkzugangspunkt und dem privaten Netzwerk aufweist.

40. Verfahren nach Anspruch 36 einschließlich der Integrierung des Netzwerk-Zugangs-Servers in die dritte Netzwerkschnittstelle.

41. Verfahren nach Anspruch 40, wobei die dritte Netzwerkschnittstelle einen lokalen Netzwerkadapter umfasst.

42. Verfahren nach Anspruch 30 einschließlich der Bereitstellung, bei dem Netzwerk-Zugangs-Server, von Software zur Registrierung von Terminals und Software zur Beschränkung des Zugangs zum öffentlichen Netzwerk für registrierte Terminals.

43. Verfahren nach Anspruch 42, wobei die Software zur Registrierung von Terminals funktionsfähig ist, um automatisch einen Registrierungsprozess in Bezug auf das Terminal zu starten, wenn sich das Terminal innerhalb der Kommunikationsreichweite des Netzwerkzugangspunkts befindet.

44. Verfahren nach Anspruch 36 einschließlich der Bereitstellung, bei dem Netzwerk-Zugangs-Server, von Einrichtungen zur Verhinderung des Zugangs zu dem privaten Netzwerk durch die Terminals.

45. Verfahren nach Anspruch 44, wobei die Einrichtungen Funktionen zur Konfigurierung eines separaten öffentlichen Zugangs und privater Zugangs-Subnetze umfassen.

46. Verfahren nach Anspruch 44, wobei die Einrichtungen einen IP-Adressfilter beinhalten.

47. Verfahren nach Anspruch 30 einschließlich der Bereitstellung, bei dem Netzwerk-Zugangs-Server, von Software, die das Verschlüsseln und Entschlüsseln von Daten ermöglicht, die von dem mobilen Terminal über das öffentliche Netzwerk gesendet und empfangen wurden.

48. Verfahren nach Anspruch 30 einschließlich der Bereitstellung, bei dem Netzwerk-Zugangs-Server, von Einrichtungen zur dynamischen Bereitstellung von Netzwerkkonfigurationsdaten an die Terminals.

49. Verfahren nach Anspruch 30 einschließlich der Bereitstellung, bei dem Netzwerk-Zugangs-Server, von Einrichtungen zur Weiterleitung von Daten, die an den und von dem mobilen Terminal über das öffentliche Netzwerk kommuniziert wurden.

50. Verfahren nach Anspruch 30 einschließlich der Bereitstellung von Software bei dem Netzwerk-Zugangs-Server zur Steuerung der Nutzung der Bandbreite durch die Terminals.

51. Verfahren nach Anspruch 30 einschließlich der Bereitstellung von Software bei dem Netzwerk-Zugangs-Server zur Überwachung und Aufzeichnung der Netzwerknutzung durch die Terminals.

52. Verfahren nach Anspruch 33 einschließlich der Bereitstellung von Software bei dem Netzwerk-Zugangs-Server zur Bereitstellung von mobiler IP-Unterstützung für die drahtlosen, mobilen Terminals.

53. Verfahren nach Anspruch 30 einschließlich der Bereitstellung einer Datenbank zur Speicherung ausgewählter Informationen, welche registrierte Terminals betreffen, bei dem Netzwerk-Zugangs-Server.

54. Verfahren nach Anspruch 30 einschließlich der Bereitstellung von Einrichtungen zur Bereitstellung von Telefondiensten für die Terminals bei dem Netzwerk-Zugangs-Server.

55. Verfahren nach Anspruch 30 einschließlich der Bereitstellung eines Integrationsbetreibernetzwerks, welches angepasst ist, um mit dem Netzwerk-Zugangs-Server über das öffentliche Netzwerk zu kommunizieren, wobei das Integrationsbetreibernetzwerk Einrichtungen für die Verwaltung des öffentlichen Netzzugangs durch das mobile Terminal über den Netzwerk-Zugangs-Server umfasst.

56. Verfahren nach Anspruch 55, welche die Bereitstellung einer zentralen Datenbank zur Speicherung ausgewählter Informationen über die Netzwerk-Zugangs-Server und die registrierten Terminals sowie von Regelwerken über Zugang zu ausgewählten Netzwerken und deren Nutzung an das Integrationsbetreibernetzwerk einschließt.

57. Verfahren nach Anspruch 55, wobei die ausgewählten Informationen über die Netzwerk-Zugangs-Server zumindest eines von Anbieteridentifizierung, Informationen über Netzwerkkonfiguration, Informationen über Datenverschlüsselung, Informationen über das Regelwerk zur Netzwerknutzung sowie Informationen über die Abrechnung von Anbietern enthalten.

58. Verfahren nach Anspruch 55, wobei die ausgewählten Informationen über die registrierten Terminals zumindest eines von Identität des autorisierten Benutzers, Terminaladresse, Regelwerk über die Sicherheit von Terminals, Identifizierung des Terminal-Dienstplans, Informationen über Datenverschlüsselung, Terminalstatus im Netzwerk, Informationen über Netzwerknutzung, Informationen über die Abrechnung der Netzwerknutzung enthalten.

59. Verfahren nach Anspruch 55, wobei die Regelwerke über ausgewählten Netzwerkzugang und Nutzung zumindest eines von Informationen über das Regelwerk zum öffentlichen Netzwerkzugang, Informationen über das Regelwerk zur Nutzung der Bandbreite und Informationen über das Regelwerk zur Netzwerkverkehrspriorität enthalten.

60. Vorrichtung zur Bereitstellung von kontrolliertem Zugang zu einem öffentlichen Netzwerk an mobile Terminals unter Anwendung der Ressourcen eines privaten Netzwerks, welches einen Netzwerkzugangspunkt zur Verbindung mit den mobilen Terminals sowie eine öffentliche Netzwerkverbindung zur Verbindung mit dem öffentlichen Netzwerk aufweist, umfassend:

einen Netzwerk-Zugangs-Server mit einer Netzwerkschnittstelle zur Einrichtung einer Netzwerkverbindung mit dem Zugangspunkt und einer Netzwerkschnittstelle zur Einrichtung einer Netzwerkverbindung mit der öffentlichen Netzwerkverbindung;

wobei der Netzwerk-Zugangs-Server die Verbindung zwischen den mobilen Terminals und dem öffentlichen Netzwerk über die öffentliche Netzwerkverbindung des privaten Netzwerks operativ steuern kann, ohne den mobilen Terminals den Zugang zu dem privaten Netzwerk zu gewähren.

61. Verteiltes System zur Bereitstellung eines kontrollierten Zugangs zu einem öffentlichen Netzwerk an mobile Terminals unter Verwendung der öffentlichen Netzwerkverbindungen einer Mehrzahl privater Netzwerke, umfassend:

eine Mehrzahl von geografisch verteilten Netzwerkzugangspunkten zur Einrichtung von Netzwerkverbindungen mit einem oder mehreren der mobilen Terminals;

eine Mehrzahl von geografisch verteilten Netzwerk-Zugangs-Servern;

eine Mehrzahl erster Netzwerkschnittstellen, wobei jede erste Netzwerkschnittstelle zur Verbindung des Netzwerk-Zugangs-Servers mit einer ausgewählten Gruppe der Netzwerkzugangspunkte dient;

eine Mehrzahl zweiter Netzwerkschnittstellen, wobei jede zweite Netzwerkschnittstelle zur Verbindung des Netzwerk-Zugangs-Servers mit der öffentlichen Netzwerkzugangsverbindung eines privaten Netzwerks dient;

wobei jeder Netzwerk-Zugangs-Server konfiguriert ist, um eine Netzwerkverbindung zwischen einem mobilen Terminal einzurichten und zu steuern, welcher eine Netzwerkverbindung zu dem Netzwerkzugangspunkt und dem öffentlichen Netzwerk über die öffentliche Netzwerkanbindung eines privaten Netzwerks hat, ohne dass eine Netzwerkverbindung zwischen dem Terminal und dem privaten Netzwerk eingerichtet wird; und

ein Integrationsbetreibernetzwerk, welches von zumindest einigen aus der Mehrzahl von Netzwerk-Zugangs-Servern entfernt ist und das angepasst ist, um mit jedem der Netzwerk-Zugangs-Server über das öffentliche Netzwerk zu kommunizieren, wobei das Integrationsbetreibernetzwerk Einrichtungen umfasst, um die Netzwerk-Zugangs-Server zu einem verteilten Netzwerk für öffentlichen Netzwerkzugang zu formen.

* * * * *