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

(10) **DE 600 17 071 T2** 2005.12.15

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 119 148 B1**
(21) Deutsches Aktenzeichen: **600 17 071.3**
(96) Europäisches Aktenzeichen: **00 306 724.6**
(96) Europäischer Anmeldetag: **07.08.2000**
(97) Erstveröffentlichung durch das EPA: **25.07.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **29.12.2004**
(47) Veröffentlichungstag im Patentblatt: **15.12.2005**

(51) Int Cl.[7]: **H04L 29/06**

(30) Unionspriorität:
481951 **12.01.2000** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB

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

(74) Vertreter:
derzeit kein Vertreter bestellt

(72) Erfinder:
Aravamudan, Murali, Murray Hill, New Jersey 07974, US; Naqvi, Shamim A., Morristown, New Jersey 07960, US

(54) Bezeichnung: **Schutz der Integrität eines Kommunikationsnetzwerks**

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

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

Beschreibung

Erfindungsgebiet

[0001] Die vorliegende Erfindung betrifft Kommunikationsnetze und insbesondere das Schützen der Betriebsintegrität solcher Netze.

Stand der Technik

[0002] Ein wohlbekanntes Merkmal herkömmlicher Telekommunikationssysteme, die Telefondienst bieten, z.B. öffentliches Wählnetz (PSTN-Public Switched Telephone Network), Vermittlungsstellen (CO-Central Offices), Nebenstellenanlagen (PBX-Private Branch Exchange) und Internet-Telefonie-Server, ist, daß diese Systeme diskrete Inseln von Funktionalität sind und jede dieser Inseln ihre eigene bestimmte Syntax und Semantik besitzt. Durch die Verwendung der unterschiedlichen Syntaxen, Semantiken und Protokolle ist es schwierig, die verschiedenen Inseln leicht zusammenzuschalten und es ist praktisch unmöglich, Merkmale bereitzustellen, die nahtlos über die verschiedenen Inseln zusammenarbeiten.

[0003] Weiterhin wird die Einführung neuer Dienstmerkmale, d.h. Anwendungen in herkömmliche Telefonienetze durch den Betreiber des Netzes unter Verwendung interner Anwendungsprogrammierer und/oder einer begrenzten Anzahl von ausgewählten (und in den meisten Fällen zertifizierten) externen Softwarelieferanten bewirkt. Der Grund für eine derartig sorgfältige Einführung neuer Dienstmerkmale durch eine kleine Anzahl von Lieferanten steht im direkten Verhältnis zu der Besorgnis, ein Stück unzertifizierter Software in das Netz einzuführen, das größere Dienstunterbrechungen verursachen kann. Es gibt zahlreiche Beispiele von weitläufig bekannt gemachten Kommunikationsnetzausfällen, die größere Dienstunterbrechungen und bedeutende finanzielle Verluste für ihre Netzbetreiber und Kundenbasis verursacht haben.

[0004] Durch die gegenwärtige Entwicklung von Netzen der nächsten Generation, die auf die Konvergenz von Sprach- und Datennetzen fokussiert sind, wird die Situation noch komplizierter. Das heißt es erscheint hochwahrscheinlich, daß das Kommunikationsnetz der nächsten Generation eine Entwicklung der heutigen PSTN- und IP-Netze (Internet Protocol) sein wird. Die heutigen Diensteanbieter werden durch eine Anzahl von Faktoren bei der Entwicklung solcher Netze der nächsten Generation angetrieben, wie beispielsweise: (1) das wohlbekannte Internet wird zu einer bedeutenden Wahl eines Netzes zur Verteilung von Sprache und Daten; (2) IP-Nutzung steigt in einem drastischen Maß an und verursacht dadurch Bandbreitenprobleme auf bestehenden PSTN-Netzen, die bedeutenden Datenverkehr führen; (3) Konvergenz von PSTN- und Packetnetzen (z.B. IP-Netzen) ist erforderlich, um eine Ende-Ende-Zuführung von Kommunikationsdiensten zu ermöglichen; (4) die Erstellung von neuen, mit der steigenden Verwendung von Paketnetzen verbundenen Diensten; und (5) durch zunehmende Liberalisierung des Marktplatzes entstehen neue und alternative Telekommunikationsumgebungen für bestehende, neue und spezialisierte Diensteanbieter bei sowohl Sprach- als auch Datenverkehr.

[0005] Ein wesentliches zugrundeliegendes Merkmal bei der Fertigstellung solcher Kommunikationsnetze der nächsten Generation ist die Netzinteroperabilität. Das heißt, die Fähigkeit des Diensteanbieters, erweiterte Kommunikationsdienste über Leitungs- und Paketnetze anzubieten, ist direkt an die Fähigkeit zur Bereitstellung von Interoperabilität über eine Anzahl von heterogenen Netzen gebunden, die einen weiten Bereich an Zeichengabeprotokollen (z.B. SS7, IP, MGCP (Media Gateway Control Protocol), H.323, SIP (Session Initiation Protocol) und dergleichen) unterstützen.

[0006] Eine aufkommende Vermittlungsplattform, die zum Lösen solcher Netzinteroperabilitätsfragen nützlich ist, ist die sogenannte „Software-Vermittlung". Softwarevermittlungen (die in der Technik auch als „Softswitches" bekannt sind) sind eine Multi-Protokoll-Softwarelösung für Zeichengabe und Transport und bieten dadurch Interoperabilität über heterogene Netze, z.B. Leitungs- und Paketnetze. Dahingehend können PSTN- und Internet-Telefoniediensteanbieter nahtlose Interoperabiliät zwischen PSTN- und IP-Netzbereichen bereitstellen. Natürlich bleibt die oben aufgeworfene Frage hinsichtlich der Netzsicherheit und der Einführung neuer Dienstmerkmale durch die Implementierung von Softwarevermittlungen in Netzen der nächsten Generation unverändert.

[0007] Insbesondere gibt es zwei Haupt-Sicherheitseigenschaften, die bei Netzen der nächsten Generation kritisch sind, nämlich sogenannte „Rechen"-Sicherheit und „Netz"-Sicherheit. Rechen-Sicherheit richtet sich darauf, sicherzustellen, daß die Einführung eines bestimmten Stücks Softwarecode nicht andere Stücke von gegenwärtig im System ablaufendem Code, z.B. der Softwarevermittlung, verfälschen können. Rechen-Sicherheit kann durch die Auswahl der Programmierungssprache zum Codieren der Software bereitgestellt werden. Beispielsweise ist Java™ eine beliebte Progammiersprache, mit der Benutzer Anwendungen erstellen können, die ohne Sorgen über Plattformkompatibilität oder Netzsicherheit über das Internet hinweg benutzt und ausgeführt werden können. Das heißt, Java ist eine wohlbekannte plattformneutrale Sprache, was bedeutet, daß unter Verwendung von Java entwickelte Programme auf verschiedenen Computersystemen ohne Notwendigkeit irgendwelcher Abänderungen

ablaufen können. Diese Plattformunabhängigkeit stammt von der Verwendung eines Sonderformats kompilierter Java-Programme mit der Bezeichnung „Bytecodes", die ein Satz von Anweisungen sind, die herkömmlichem Maschinencode ähnlich aussehen, aber nicht für irgendeinen Prozessor spezifisch sind. So kann ein Java-Bytecode von jedem Computersystem gelesen und ausgeführt werden, das den wohlbekannten Java-Interpretierer besitzt. So wird durch Ausbilden des Java-Programms in Bytecodeform die Ausführung solcher Progamme über jede Plattform, jedes Betriebssystem oder Fensterbildungssystem ermöglicht, solange wie der Java-Interpretierer zur Verfügung steht. Die Fähigkeit, daß eine einzige Binärdatei, d.h. Java-Bytecode-Datei, über mehrere Plattformen ausführbar ist, ist damit ein Schlüsselmerkmal, mit dem Java-Bytecode, besonders in Form von Applets, zu einer gebräuchlichen Weise zur Ausführung von Programmen über das World Wide Web (WWW) wird.

[0008] Man wird erkennen, daß eine Bytecode-Datei typischerweise durch Kompilieren einer Java-Datei erhalten wird und ein Strom von Byte ist, der eine einzige Klasse in einer für die wohlbekannte Java Virtual Machine (JVM) geeigneten Form darstellt. Die Java Virtual Machine führt Bytecodes aus und stellt für Java gewisse Grundfähigkeiten wie beispielsweise Objekterstellung und Speicherbereinigung bereit. Bedeutsamerweise bietet Java als eine auf einer virtuellen Maschine basierende Sprache von sich aus Rechensicherheit, wodurch sichergestellt wird, daß ein Stück Java-Code kein anderes Stück Java-Code verfälschen kann, das in dem gleichen (oder unterschiedlichen) Prozeßraum abläuft.

[0009] Während jedoch die Bereitstellung von Rechensicherheit im Zusammenhang mit Netzen der nächsten Generation von Bedeutung ist, benutzen solche Netze robuste Verbindungsbearbeitungssysteme, für die Rechensicherheit allein unzureichend ist, um die Integrität des Netzes sicherzustellen. Das heißt, obwohl ein bestimmtes Stück Softwarecode, z.B. ein Dienstmerkmal, ein anderes Stück Softwarecode im Netz nicht verfälscht, kann das bestimmte Codestück das Netz immer noch bedeutend stören, z.B. durch Senden von willkürlichen Nachrichten durch das Netz, die wiederum Netzressourcen willkürlich benutzen. Die sogenannte Netzsicherheit ist die Sicherheitseigenschaft, die sicherstellt, daß keine einzelne Anwendung die Netzressourcen willkürlich mißbrauchen kann und dadurch das Netz schädigt oder den Netzwirkungsgrad verringert. Weiterhin bedeutet Netzsicherheit besonders auch für Verbindungsbearbeitungssysteme, daß jeglicher durch ein besonderes Merkmal verursachter Schaden auf dieses bestimmte Merkmal, z.B. eine Verbindung, lokalisiert bleibt und die übrigen Merkmale im Verbindungsbearbeitungssystem normal funktionieren.

[0010] Es besteht daher eine Notwendigkeit zur Bereitstellung von Netzsicherheit in Netzen der nächsten Generation.

[0011] In US-A 5 931 913 ist ein Verfahren offenbart, bei dem eine Sitzung zwischen einem Endgerät und einem Host hergestellt wird, die jeweils gemäß einem Kommunikationsprotokoll kommunizieren können. Zwischen dem Endgerät und dem Host wird ein Kommunikationskanal über einen Klienten und einen Server eines Kommunikationsnetzes hergestellt, wobei der Klient mit dem Endgerät und der Server mit dem Host verbunden ist. Endgeräteinformationen werden über den Kommunikationskanal vom Klienten zum Server übermittelt. Eine Anzeige der Bereitschaft zum Kommunizieren von Daten zwischen dem Endgerät und dem Host wird zwischen dem Server und dem Klienten über den Kommunikationskanal übermittelt. Nachrichten werden zwischen dem Klienten und dem Endgerät und dem Server und dem Host gemäß dem Kommunikationsprotokoll zum Emulieren von Übermittlung von Sitzungsherstellungsnachrichten zur Herstellung einer Sitzung zwischen dem Endgerät und dem Host gemäß dem Kommunikationsprotokoll übermittelt, ohne Übermittlung der Sitzungsherstellungsnachrichten über den Kommunikationskanal zu erfordern.

[0012] In EP-A-0 963 096 ist ein Telefondienst offenbart, der eine verteilte Architektur mit einer Sammlung von Ressourcen benutzt, die jeweils einen hierarchischen Namensraum freilegen. Die Architektur enthält zwei Grundressourcenarten, den Vorrichtungsserver und den Rufkoordinator, die durch ein Netz mit einem gemeinsamen Protokoll, z.B. TCP/IP, zusammengeschaltet sind. Die Wechselwirkung zwischen den verschiedenen Ressourcen folgt „Klient-Server"-Grundsätzen zur Implementierung von Ende-Ende-Kommunikation. Vorrichtungsserver stellen physikalische/logische Telefonvorrichtungen dar, die a) Endpunkt-Vorrichtungsserver und b) Gateway-Vorrichtungsserver umfassen. Endpunkt-Vorrichtungsserver 1) stellen Steuerungselemente für Kommunikation wie beispielsweise Tastaturen, Anzeigelampen und Anzeigen dar und 2) führen Medienwiedergabe, z.B. Sprachdigitalisierung, -transportierung und -wiederherstellung durch. Gateway-Vorrichtungsserver weisen zwei „Seiten" auf. Eine Seite ist so implentiert, daß sie einem Rufkoordinator erscheint, als wenn sie ein Vorrichtungsserver wäre, die andere Seite besitzt eine Schnittstelle zum Zusammenarbeiten mit einer bereits bestehenden Insel des Telefondienstes. In dem Begriff „Vorrichtungsserver" wird Server auf die herkömmliche Weise der „Klient-Server"-Architektur benutzt, wo der Server Anforderungen von den Klienten bedient und keine Handlung unternimmt, es sei denn als Antwort auf eine Klientenanforderung. Ein Rufkoordinator funktioniert in der Rolle des „Klienten". Die Vorrichtungsserver sind sich nicht des Kommunikationszustandes bewußt,

der vom Rufkoordinator aufrechterhalten und als ein hierarchischer Namensraum freigelegt wird. Vom Rufkoordinator wird die Bearbeitung eines Rufs als Folge von Schritten behandelt, die jeweils auf einem kleinen Stück von auf einem Computer ausführbaren Code mit der Bezeichnung „Merkmals-Applet" implementiert werden können.

Kurze Beschreibung der Erfindung

[0013] Ein Verfahren und Kommunikationssystem gemäß der Erfindung entsprechen den unabhängigen Ansprüchen. Bevorzugte Ausführungsformen entsprechen den abhängigen Ansprüchen.

[0014] Ein Aspekt der vorliegenden Erfindung richtet sich auf ein Verfahren und eine Vorrichtung zum Schutz gegen Netzschädigung in Verbindungsbearbeitungssystemen der nächsten Generation. Insbesondere wird gemäß einem Aspekt der Erfindung Netzsicherheit unter Verwendung einer semantischen Einschränkung von höheren Verbindungsbearbeitungsprotokollgrundelementen in Verbindung mit dynamischer Programmierung der verschiedenen Netzwegeleitungselemente zum Erzwingen von sowohl sogenannter Verbindungssteuerung als auch Ratensteuerung erreicht. Gemäß der bevorzugten Ausführungsform der Erfindung wird durch eine solche semantische Einschränkung die Beschaffenheit der Nachrichten eingeschränkt, die zwischen den verschiedenen Komponenten eines Softswitch ausgetauscht werden können. Weiterhin wird durch Verbindungssteuerung die Anzahl von Verbindungen zwischen verschiedenen Komponenten des Softswitch begrenzt und durch Ratensteuerung wird die Rate festgelegt, mit der diese Verbindungen hergestellt werden. Gemäß einer Ausführungsform der Erfindung wird eine solche Verbindungssteuerung und Ratensteuerung durch dynamisches Umprogrammieren verschiedener Netzwegeleitungselemente erreicht. Beispielsweise wird gemäß einem Aspekt der Erfindung Verbindungssteuerung zum Einschränken der Anzahl von Verbindungen, z.B. TCP-Verbindungen benutzt, die ein bestimmtes Merkmal herstellen darf, und Ratensteuerung wird zum Einschränken der Anzahl von Nachrichten, d.h. der effektiven Bandbreite, von dem bestimmten Merkmal benutzt.

[0015] Gemäß der bevorzugten Ausführungsform der Erfindung wird eine verteilte Architektur definiert, die sich einer Ansammlung von Ressourcen bedient, die jeweils einen hierarchischen Namensraum freilegen. Insbesondere ist die verteilte Architektur der bevorzugten Ausführungsform die des sogenannten (hiernach als „LT Softswitch") bezeichneten „Lucent Technologies Softswitch", der von Lucent Technologies Inc. erhältlich ist. Die Architektur der bevorzugten Ausführungsform richtet sich auf die Bereitstellung von Telefoniediensten in Netzen der nächsten Generation und enthält zwei Grundressourcenarten, nämlich i) den Vorrichtungsserver und ii) den Rufkoordinator, die durch ein Netz mit einem gemeinsamen Protokoll, z.B. TCP/IP (Transmission Control Protocol/Internet Protocol) zusammengeschaltet sind. Jede Ressource kann an mehr als einer Verbindung teilnehmen, d.h. jede Ressource wirkt als ein verteiltes Dateisystem, das verschiedene ihm gebotene Anforderungen entscheiden kann. Die Wechselwirkung zwischen den verschiedenen, zur Verfügung stehenden Ressourcen, die im wesentlichen unabhängig sind, folgt herkömmlichen Grundsätzen der „Klient-Server"-Architektur zum Implementieren von Ende-Ende-Kommunikation.

[0016] Gemäß den Grundsätzen der Erfindung wird Netzsicherheit durch Anwenden der semantischen Einschränkung durch Isolieren und Einschränken des bestimmten, benutzten Protokolls durch einen sogenannten Verbindungsbearbeitungskomplex und das bestimmte Merkmal, z.B. ein Merkmals-Applet bereitgestellt. Zusätzlich werden die direkten Kommunikationen des Merkmals auf den Verbindungsbearbeitungskomplex eingeschränkt, der gemäß der bevorzugten Ausführungsform unter anderem mindestens einen Softswitch enthält. Beispielsweise dürfen willkürliche Komponenten des Verbindungssteuerungskomplexes nicht miteinander kommunizieren. So dürfen Vorrichtungsserver nur auf Rufkoordinatoren reagieren und insbesondere nur auf diejenigen Rufkoordinatoren, die für diese Vorrichtungsserver vorgesehen worden sind. Weiterhin werden gemäß der bevorzugten Ausführungsform der Erfindung die Einschränkungen dynamisch über eine externe Instanz, nämlich einen sogenannten „Policy-Server" programmiert. Der Policy-Server überwacht alle Verwaltungsereignisse in dem Verbindungsbearbeitungskomplex und behält Kontrolle über alle seine Elemente. Als solches überwacht der Policy-Server den Betriebszustand der Komponenten des Komplexes und unterhält Konfigurationsinformationen hinsichtlich dieser Komponenten, wodurch der Policy-Server zu einer strategischen Instanz wird, indem er die Herstellung von Netzsicherheit gemäß den Grundsätzen der Erfindung erleichtert.

[0017] Vorteilhafterweise wird gemäß den Aspekten der Erfindung Schutz gegen Netzschädigung in Verbindungsbearbeitungssystemen der nächsten Generation durch Benutzung einer semantischen Einschränkung von höheren Verbindungsbearbeitungsprotokollgrundelementen im Zusammenhang mit dynamischer Programmierung der verschiedenen Netzwegeleitungselemente zum Erzwingen von sowohl Verbindungssteuerung als auch Ratensteuerung realisiert.

Kurze Beschreibung der Zeichnungen

[0018] Fig. 1 zeigt eine beispielhafte Architektur für

ein PSTN/IP-Netz, die Netzsicherheit gemäß den Grundsätzen der Erfindung implementiert;

[0019] Fig. 2 zeigt einen beispielhaften Namensraumbaum für einen Vorrichtungsserver, z.B. nach der Darstellung in Fig. 1;

[0020] Fig. 3 zeigt einen beispielhaften Namensraum eines Rufkoordinators, z.B. nach der Darstellung in Fig. 1;

[0021] Fig. 4 ist ein Flußdiagramm von beispielhaften Operationen **400** zur Herstellung von Netzsicherheit in Kommunikationsnetzen gemäß den Grundsätzen der Erfindung; und

[0022] Fig. 5 zeigt ein beispielhaftes Netzmanagementszenario mit Netzsicherheitsmerkmalen, die gemäß den Grundsätzen der Erfindung hergestellt werden.

[0023] In dieser gesamten Beschreibung werden sofern nicht anderweitig angemerkt gleiche Elemente, Blöcke, Komponenten und Abschnitte in den Figuren durch die gleichen Bezugsbezeichnungen bezeichnet.

Ausführliche Beschreibung

[0024] In der nachfolgenden Beschreibung werden die verschiedenen Aspekte der Erfindung unter Verwendung eines beispielhaften Telefoniedienstbeispiels ausführlich beschrieben und dargestellt. Es versteht sich jedoch, daß die Erfindung nicht auf die Verwendung mit irgendeiner bestimmten Systemkonfiguration begrenzt ist. Stattdessen sind die Grundsätze der Erfindung allgemeiner auf ein beliebiges Kommunikationsnetz anwendbar, wo die Herstellung von Netzsicherheitseigenschaften kritisch ist.

[0025] Gemäß der bevorzugten Ausführungsform der Erfindung kann nahtlose Telefonie über die verschiedenen Inseln mit Telefoniefunktionalität durch zur Verfügungstellung von Telefondienst mit einer verteilten Architektur bereitgestellt werden, die eine Sammlung von Ressourcen nutzt, die jeweils einen hierarchischen Namensraum für mindestens eine andere Ressource freilegen. So wie er hier benutzt wird, ist ein hierarchischer Namensraum analog einem auf einer Computerfestplatte basierenden hierarchischen Dateisystem, das als eine Baumstruktur dargestellt werden kann, nur könnte das, was in den Knoten und Ästen der Hierarchie erscheint, keine eigentlichen Datenverzeichnisse und Dateien sein, sondern stattdessen andere Datenstrukturen im Speicher sein, die in der Form eines Dateisystems dargestellt sind. So ist ein hierarchischer Namensraum vergleichbar mit einer sogenannten „RAM-Disk", jedoch kann der Namensraum an ein Plattendateisystem gebunden sein. Eine ausführlichere Beschreibung eines solchen verteilten Verbindungs-bearbeitungssystemes ist in der gleichzeitig anhängigen gemeinsam erteilten, am 5. Juni 1998 eingereichten US-Patentanmeldung Serien-Nr. 09/092,495 mit dem Titel „Distributed Call System" (verteiltes Verbindungsbearbeitungssystem) enthalten, die hiermit durch Bezugnahme für alle Zwecke hier aufgenommen wird.

[0026] Um Zusammenhang zu bieten und ein vollständiges Verständnis der vorliegenden Erfindung zu erleichtern, werden gewisse Merkmale des oben beschriebenen verteilten Verbindungsbearbeitungssystems im Zusammenhang mit der bevorzugten Ausführungsform der Erfindung besprochen. Die Architektur der bevorzugten Ausführungsform enthält zwei Grundressourcenarten, nämlich i) den Vorrichtungsserver und ii) den Rufkoordinator, die durch ein Netz mit einem gemeinsamen Protokoll, z.B. TCP/IP, zusammengeschaltet sind. Jede Ressource kann an mehr als einem Ruf teilnehmen, d.h. jede Ressource wirkt als ein verteiltes Dateisystem, das zwischen verschiedenen ihm dargebotenen Anforderungen entscheiden kann. Die Wechselwirkung zwischen den verschiedenen verfügbaren Ressourcen, die im wesentlichen unabhängig sind, folgt herkömmlichen Grundsätzen der „Klient-Server"-Architektur zum Implementieren einer Ende-Ende-Kommunikation. Dahingehend erscheinen durch die Verwendung des hierarchischen Namensraums alle Kommunikationen zwischen den Ressourcen der verteilten Architektur als Dateisystemkommunikationen.

[0027] Insbesondere wird im Begriff „Vorrichtungsserver" „Server" auf die herkömmliche Weise der „Klient-Server"-Architektur benutzt, wo der Server Anforderungen von Klienten bearbeitet und keine Handlung unternimmt, es sei den als Reaktion auf eine Klientenanforderung. Vom Vorrichtungsserver werden Protokollzustandsinformationen für das Protokoll unterhalten, das er zum Kommunizieren mit dem Rufkoordinator benutzt. Jeder Vorrichtungsserver legt sich selbst als ein hierarchischer Namensraum frei, so daß jeder Klient, der die durch den Vorrichtungsserver bereitgestellten Dienste benutzen will, auf den Vorrichtungsserver zugreift, als wenn er auf ein verteiltes Dateisystem zugreift. Typische Vorrichtungsserver sind physikalische/logische Telefonvorrichtungen, die a) Endpunkt-Vorrichtungsserver und b) Gateway-Vorrichtungsserver umfassen.

[0028] Endpunkt-Vorrichtungsserver 1) stellen Steuerelemente für die Kommunikation wie beispielsweise Tastaturen, Anzeigelampen und Anzeigen dar, und 2) führen Medienwiedergabe, z.B. Sprachdigitalisierung, -transport und -wiederherstellung durch. Endpunkt-Vorrichtungsserver können Telefonvorrichtungsserver; einen Anrufbeantwortungsserver (z.B. Sprachspeicherdienst); Server für intelligente persönliche Kommunikationen, sogenannte intelligente

Agenten und dergleichen umfassen. Ein Beispiel eines Endpunkt-Vorrichtungsservers ist ein Telefonvorrichtungsserver. Ein Telefonvorrichtungsserver modelliert typischerweise ein Telefongerät, das aus Folgendem besteht: a) einer Bedienungsoberfläche, die von einem Benutzer zur Rufeinleitung, Beendigung, und Steuerungsoperationen benutzt wird, und b) einer Medienwiedergabemaschine, z.B. einem Lautsprecher und/oder einem Mikrofon für Tonanwendungen, ein Anzeigeschirm für Videoanwendungen und dergleichen.

[0029] Die eigentliche Bedienungsoberfläche und Medienwiedergabeeinzelheiten können sich für verschiedene bestimmte Ausführungsformen unterscheiden, d.h. für unterschiedliche Telefongeräte oder Kommunikationsvorrichtungen. Beispielsweise weist ein standarmäßiges Telefongerät des herkömmlichen Telefondienstes (POTS-plain old telephone service) keine Anzeige auf und viele Aspekte seiner Bedienungsoberfläche sind unter Verwendung der Medien des POTS-Telefongeräts selbst für Inbandzeichengabe implementiert. Dem gegenüber benutzt ein virtuelles Telefon eines sogenannten Personal Computers (PC) Menüs/Fenster als Bedienungsoberfläche, wobei die Tonwiedergabe über die Soundkarte des PC stattfindet. Eine andere Art von Telefonvorrichtung ist ein PC, auf dem ein standardmäßiger H.323-Klient abläuft. Für eine derartige Telefonvorrichtung läuft ein Proxy für den H.323-Klienten typischerweise im gemeinsamen Protokollnetzwerk ab und legt eine Namensraumschnittstelle, z.B. eine Dateisystemschnittstelle frei. All diese und andere Telefonvorrichtungen können an zutreffende Telefonvorrichtungsserver angeschlossen werden.

[0030] Man beachte, daß standardmäßige Telefoniekonzepte wie beispielsweise Wählton, Rufton und dergleichen der bestimmten Telefonvorrichtung zugeordnete Einzelheiten sind. So würde ein Telefonvorrichtungsserver, der ein POTS-Telefon unterstützt, wahrscheinlich Wählton liefern, während die PC-Benutzeroberfläche kein direktes Analog eines Wähltons haben könnte und der ein PC-Telefon unterstützende Telefonvorrichtungsserver ihn daher nicht bereitstellen würden. Von Bedeutung ist, daß jeder andere Klient wie beispielsweise der Rufkoordinator, der einen Telefonvorrichtungsserver benutzt, sich nicht der einzelnen/örtlichen Einzelheiten der Endpunktvorrichtung bewußt ist.

[0031] Für ein POTS-Telefongerät könnte ein Telefonvorrichtungsserver in der Form eines PC mit einer POTS-Schnittstellenkarte zur Verbindung mit einem POTS-Telefongerät und einer Netzkarte für TCP/IP-Konnektivität implementiert sein. Bei Verwendung mit TCP/IP kann die Netzkarte eine beliebige Art von Kommunikationsvorrichtung sein, die zum Erhalten von TCP/IP-Konnektivität benutzt werden kann, wie beispielsweise Netzschnittstellenkarten (NIC-Network Interface Cards), herkömmliche Analogmodems, Glasfaserschnittstellenkarten, ISDN-Modems (Integrated Services Digital Network), jede beliebige Form von DSL-Technik (Digital Subscriber Loop) oder dergleichen. Der Telefonvorrichtungsserver kann in der Form eines Teilnehmermultiplexsystems oder einer Nebenstellenanlage (PBX-Private Branch Exchange) implementiert sein, die mit einer Schnittstelle wie beispielsweise einer TCP/IP-Schnittstellenkarte zum Anschalten an das vom Rufkoordinator und anderen Vorrichtungsservern benutzte Netz ausgerüstet worden sind.

[0032] Gateway-Vorrichtungsserver besitzen zwei sogenannte „Seiten". Eine Seite ist so implementiert, daß sie einem Rufkoordinator als ein Vorrichtungsserver erscheint und dient zum Verbinden des Gateway-Vorrichtungsservers mit dem vom Rufkoordinator und anderen Vorrichtungsservern benutzten Netz. Die andere Seite des Gateway-Vorrichtungsservers besitzt eine Schnittstelle zum Anschalten sowie Steuern und Bedienen von Elementen einer vorher bestehenden Telefondienstinsel. Ein beispielhafter Gateway-Vorrichtungsserver ist ein Leitungsvorrichtungsserver. Beispielhafterweise modelliert ein Leitungsvorrichtungsserver typischerweise eine Vorläufer-Netzschnittstelle, die eine oder mehrere Telefonverbindungen über eine vorher bestehende Telefondienstinsel, wie beispielsweise das wohlbekannte PSTN unterstützen kann.

[0033] Eine Hauptfunktion eines Gateway-Vorrichtungsservers besteht darin, als ein Gateway zwischen dem die Vorrichtungsserver und Rufkoordinatoren verbindendem Netz und einem anderen externen Netz, z.B. einem Netz, das eines der Telefonieinseln ist, zu wirken. Dahingehend ist der Gateway-Vorrichtungsserver eine gültige Instanz im Netz und bedient sich des zutreffenden Protokolls dieses Netzes. Durch Freilegen eines Namensraums für seine Klienten, nämlich den Rufkoordinator, wird durch die einzelnen Gateway-Vorrichtungsserver der Rufkoordinator gegen bestimmte Zeichengabeprotokolle des Netzes abgeschirmt. Dies wird durch Aufrechterhaltung eines protokollspezifischen Zustandes im Gateway-Vorrichtungsserver erreicht. Vorrichtungsserver können mehrere Verbindungen von einem einzigen Rufkoordinator handhaben, sowie auch mehrere solche Rufkoordinatoren handhaben. Um solche mehrfachen Wechselwirkungen und Multiplexen handzuhaben, wird von Vorrichtungsservern ein lokaler Zustand aufrechterhalten.

[0034] Ein Rufkoordinator stellt Kommunikationen zwischen verschiedenen Vorrichtungsservern her. Der Rufkoordinator kann als ein Softwaremodul implementiert werden, das von einem Computer ausgeführt wird, der mit dem Netz verbunden ist, an das die Vorrichtungsserver angeschaltet sind. Der den Rufkoordinator ausführende Computer kann getrennt

von dem Computer oder den Computern der Vorrichtungsserver sein oder er kann die Verarbeitungsleistung mit einem oder mehreren der Vorrichtungsservercomputer oder anderen, an das Netz angeschalteten Computern teilen. Als Alternative kann die Funktionalität des Rufkoordinators über mehrere Computer verteilt sein, die in beliebiger Kombination von den Computern der Vorrichtungsserver getrennt sein, oder mit diesen geteilt sein können. Weiterhin kann an ein einzelnes Netz mehr als ein Rufkoordinator angeschaltet sein.

[0035] Ein Ruf/eine Kommunikation und alle zugehörigen Verwaltungsaufgaben werden vollständig vom Rufkoordinator gehandhabt. Der Rufkoordinator funktioniert in der Rolle des „Klienten" der herkömmlichen „Klienten-Server-"Architektur, z.B. er leitet Anforderungen von Diensten an die verschiedenen Vorrichtungsserver ein. Typischerweise finden solche Anforderungen als Reaktion auf ein sogenanntes „Ereignis" statt, das vom Rufkoordinator erkannt wird. Da der Rufkoordinator der Klient ist, kann er einen Dienst von verschiedenen der Server, d.h. Vorrichtungsservern oder Gateway-Servern entsprechend dem an einer bestimmten Verbindung bereitgestellten Dienst und den gespeicherten Regeln oder Registrierungen anfordern.

[0036] Die Vorrichtungsserver sind sich nicht des Kommunikationszustandes, der die Wechselwirkung zwischen mehreren Vorrichtungsservern ist, bewußt. Stattdessen wird ein Kommunikationszustand vom Rufkoordinator aufrechterhalten, der den Kommunikationszustand als einen hierarchischen Namensraum freilegt. Als ein Klient der Vorrichtungsserver manipuliert der Rufkoordinator die Vorrichtungsserver, um Kommunikationen herzustellen. Weiterhin wird vom Rufkoordinator eine solche, als „Rufsitzung" bekannte Wechselwirkung erfasst und als hierarchischer Namensraum exportiert.

[0037] Vom Rufkoordinator wird die Bearbeitung einer Verbindung als eine Folge von Schritten behandelt, von denen jeder durch ein kleines Stück von auf einem Computer ausführbarem Code mit der Bezeichnung „Merkmals-Applet" implementiert werden kann. Merkmals-Applets führen einen bestimmten Schritt bei der Rufbearbeitung durch und manipulieren typischerweise den Rufbaum des vom Rufkoordinator freigelegten Namensraums. Das heißt, abgesehen vom Herunterladen der Merkmals-Applets kommunizieren der Rufkoordinator und die Merkmals-Applets vollkommen durch den Rufbaum. Merkmals-Applets können vom Rufkoordinator dynamisch heruntergeladen und ausgeführt werden. Gemäß einem Aspekt der Erfindung kann sich der Merkmals-Applet-Code an beliebiger Stelle im Netz befinden und kann fliegend aus dem Netz oder von einem unabhängigen Softwarelieferanten (ISV – Independent Software Vendor) heruntergeladen werden, oder das Merkmals-Applet selbst kann irgendwo anders im Netz ausgeführt werden. Da der Sitzungszustand unter Verwendung des Rufbaums manipuliert wird, der vom Rufkoordinator als ein hierarchischer Namensraum freigelegt wird, ist der Ort des Merkmals-Applets selbst oder seine Ausführung als Teil der Bearbeitung der gegenwärtigen Verbindung/Sitzung bedeutungslos.

[0038] Wie aus der obigen Besprechung ersichtlich ist, ist eindeutig die Fähigkeit, Netzinteroperabilität unter und zwischen heterogenen Kommunikationsnetzen bereitzustellen, bei der Herstellung von Kommunikationsnetzen der nächsten Generation kritisch. Die verschiedenen Aspekte der vorliegenden Erfindung richten sich auf die Herstellung einer solchen Netzsicherheit in solchen Kommunikationsnetzen.

[0039] Insbesondere zeigt die Fig. 1 eine beispielhafte Architektur für ein PSTN/IP-Kommunikationsnetz **100**, die Netzsicherheit gemäß den Grundsätzen der Erfindung implementiert. In der Darstellung enthält die bespielhafte Architektur **100** folgendes: POTS-Telefone **105** und **110**, IP-Telefon **115**, SS7-Netze **120** und **125** (die Teil des PSTN bilden), IP-Netz **130**, Verbindungsleitungs-Gateways **140** und **145**, Zugangs-Gateway **150**, Verzeichnisse **135** und Verbindungsbearbeitungskomplex **155**. Gemäß der bevorzugten Ausführungsform enthält der Verbindungsverarbeitungskomplex einen Softswitch und insbesondere den von Lucent Technologies Inc., 600 Mountain Ave., Murray Hill, NJ 07974 erhältlichen oben erwähnten LT Softswitch.

[0040] In der Darstellung in Fig. 1 umfaßt der Rufbearbeitungskomplex **155** den Rufkoordinator **160**, Vorrichtungsserver **170**, **170-1**, **170-2** und **170-3**, Benutzermerkmals-Applet **175**, Diensteanbieter-Servlet **180**, Verzeichniskoordinator **185** und Policy-Server **165**. Der Rufkoordinator **160** ist wie oben besprochen ein Objekt, das den gesamten Fluß von Ereignissen verwaltet, die an einer oder mehreren Kommunikationssitzungen, z.B. Rufbearbeitungssitzungen beteiligt sind, und unterhält Informationen für jede von ihm verwaltete Verbindung. Beispielhafterweise umfassen die vom Rufkoordinator **160** unterhaltenen Informationen verbindungsspezifische Elemente wie beispielsweise: Benutzermerkmals-Applet(s), ein Diensteanbieter-Servlet und Vorrichtungsserver, die in der Rufbearbeitungsanforderung benutzt werden. Wie ausführlicher unten besprochen wird, werden die vom Rufkoordinator **160** unterhaltenen Informationen als ein gemeinsamer Namensraum dargestellt, so daß jede interessierte Instanz im System auf die Informationen zugreifen kann.

[0041] Die Vorrichtungsserver, d.h. Vorrichtungsserver **170**, **170-1**, **170-2** und **170-3** im Rufbearbeitungskomplex **155** ermöglichen Kommunikationen zwischen verschiedenen Netzelementen, die unter-

schiedliche Protokolle benutzen. Beispielsweise ist der Vorrichtungsserver **170** beispielhafterweise als ein SS7-Vorrichtungsserver zum Erleichtern von Kommunikationen im wohlbekannten SS7-Zeichengabeprotokoll über ein leitungsvermitteltes Netz, z.B. SS7-Netz **120** und das Verbindungsleitungs-Gateway **140** dargestellt. In ähnlicher Weise ist der Vorrichtungsserver **170-3** beispielhafterweise als ein SIP-Vorrichtungsserver zum Erleichtern von Kommunikationen in dem wohlbekannten SIP-Zeichengabeprotokoll über ein Paketnetz, z.B. das IP-Netz **130** dargestellt. Vorteilhafterweise nutzt der Verbindungsbearbeitungskomplex **155** einen oder mehrere Vorrichtungsserver für jede unterschiedliche Protokoll/Gateway-Konfiguration, für die Kommunikationen gewünscht werden. Weiterhin ist die Kommunikation zu und von diesen Gateways vollständig im Verbindungsbearbeitungskomplex **155** verkapselt, wodurch sich erübrigt, daß andere Komponenten im Kommunikationssystem sich des benutzten Protokolls bewußt sind. Damit wird die Herstellung neuer Gateways zum Kommunikationssystem, z.B. der beispielhaften Architektur **100** einfach durch Zufügen eines entsprechenden Device-Servers für diese Gateway-Art bewirkt, ohne irgendeinen anderen Teil des Verbindungsverarbeitungskomplexes **155** zu beinflussen.

[0042] Fig. 2 zeigt den beispielhaften Namensraumbaum **200** für einen Vorrichtungsserver. Wie bei Dateisystemen gebräuchlich, ist der Wurzelknoten **210** des Namensraumbaums **200** als „#“ bezeichnet. Ereignissteuerung **220** ist die Datei, in die Ereignisse, die dem Rufkoordinator anzuzeigen sind, eingeschrieben werden, und die Dienstanforderungen vom Rufkoordinator eingeschrieben werden. Somit ein Anzeiger, daß eine Verbindung einzuleiten ist und die gewählten Ziffern in die Ereignisssteuerung **220** eingegeben werden. Die Knotendaten **230** werden zur Aushandlung von Medien benutzt, sobald eine Verbindung hergestellt ist. Der Knotenbenutzer **240** enthält Anzeigen darüber, welche Merkmals-Applets vom Rufkoordinator bei der Bearbeitung einer Verbindung für den Vorrichtungsserver, wie ausführlicher unten beschrieben wird, zu fahren sind.

[0043] Weiterhin zeigt die Fig. 3 einen beispielhaften Namensraum **300** eines Rufkoordinators. Wie beim Namensraum **300** ist der Wurzelknoten **310** des Namensraums „#/“. Unter dem Wurzelknoten **310** befindet sich die globale Ereignisssterungsdatei **320**. Die globale Ereignissteuerungsdatei **320** hält alle Ereignisse die sich auf alle Verbindungen beziehen, z.B. global bezogene Gebühreninformationen wie beispielsweise eine Änderung des Gebührenratenplans aufgrund einer Zeitänderung. Zusätzlich kann die globale Ereignissteuerungsdatei **320** durch Programme geöffnet und gelesen werden, wie beispielsweise Ereigniseinzelheitenaufzeichnung die über alle Verbindungsbearbeitungsereignisse erfahren möchten, die in einem bestimmten Rufkoordinator stattfinden.

[0044] Der Rufbaumknoten **330**, ebenfalls unter dem Wuzelknoten **310**, enthält alle gegenwärtig unter der Kontrolle des aktiven Rufkoordinators, z.B. Rufkoordinators **160**, aktiven Verbindungen. So gibt es für jede aktive Verbindung einen aktiven Verbindungsknoten **340**. In der Fig. 3 ist der Deutlichkeit der Besprechung halber nur eine aktive Verbindung dargestellt, aber es ist zu bemerken, daß mehrere Rufkoordinatoren und aktive Verbindungen gemäß den Grundsätzen der Erfindung bestehen können. Unter jedem aktiven Verbindungsknoten **340** gibt es eine verbindungsweite Ereignissteuerungsdatei **350** und einen Nummernknoten **360** für jede Vorrichtung einer Verbindung. Verbindungsweite Ereignissteuerungsdatei **350** wird für Ereignisse benutzt, die sich auf die Verbindung als Ganze beziehen. Verbindungsweite Ereignissteuerungsdatei **350** stellt alle Verbindungsbearbeitungsereignisse bereit, die für diese bestimmte Verbindung relevant sind. Der Rufkoordinator und die Merkmals-Applets können über die verbindungsweite Ereignissteuerungsdatei **350** kommunizieren. Jeder Nummernknoten **360** wird durch die netzwegeleitbare Adresse der von ihr vertretenen Vorrichtung identifiziert. Der Nummernknoten stellt eigentlich den durch die identifizierte Vorrichtung freigelegten gesamten Namensraum dar. So ist der Nummernknoten nicht wirklich ein einziger Knoten, sondern stattdessen selbst ein Baum des Namensraums eines Vorrichtungsservers, wobei sich der Wurzelknoten des Baums am Ort des Nummernknotens **360** befindet.

[0045] Sich wieder der Fig. 1 zuwendend ist das Benutzermerkmals-Applet **175** ein Objekt, das einen Teilnehmer an einer Verbindung darstellt, d.h. Ausführung des Benutzermerkmals-Applets **175** implementiert die diesem Sitzungsteilnehmer zugeordnete erforderliche Dienstlogik. Beispielsweise stellt das Benutzermerkmals-Applet **175** vom Anrufer angeforderte Merkmals-Applets/-Dienste wie beispielsweise den wohlbekannten Anklopfdienst her. Vorteilhafterweise ermöglicht dies Dienstanbietern und/oder dritten Dienstlieferanten, Dienste zu erstellen und sie über die Dienstreihe eines bestimmten Diensteanbieters anzubieten. Als solches ist das Diensteanbieter-Servlet **180** ein Objekt, das vom Diensteanbieter benutzt wird, um seine Dienstangebote kundenspezifisch auszulegen. Beispielsweise kann der Diensteanbieter unter Verwendung des Diensteanbieter-Servlet **180** das Verhalten des Verbindungsbearbeitungskomplexes **155** zum Durchleiten von Verkehr durch verschiedene Telekommunikationsbetreiber zu unterschiedlichen Tageszeiten kundenspezifisch auslegen, um niedrigere Ferngebühren auszunutzen.

[0046] Weiterhin kommuniziert der Verzeichniskoor-

dinator **185** mit Verzeichnissen **135**, die für gewisse Dienstangebote über sowohl PSTN- als auch IP-Netze erforderlich sind. Beispielsweise könnten die Verzeichnisse **135** wohlbekannte SCP-Datenbänke (Service Control Point) oder LDAP-basierte Datenbänke (Lightweight Directory Access Protocol) oder SIP-aktive Verzeichnisse umfassen. Als solches werden durch direkte Aufnahme des Verzeichniskoordinators **185** in den Verbindungsbearbeitungskomplex **155** andere Komponenten im System von der Aufgabe befreit, sich für die zur Herstellung eines bestimmten Merkmals erforderlichen Informationen an Verzeichnisse **135** einschalten zu müssen.

[0047] Gemäß einem Aspekt der Erfindung wird Netzsicherheit durch Verwendung semantischer Einschränkung von höheren Verbindungsbearbeitungsprotokollgrundelementen im Zusammenhang mit dynamischer Programmierung der verschiedenen Netzwegeleitelemente zum Erzwingen von sowohl Verbindungssteuerung als auch Ratensteuerung erreicht. Gemäß den Grundsätzen der Erfindung wird Netzsicherheit durch Anwenden der semantischen Einschränkung durch Isolieren des bestimmten, vom Verbindungsbearbeitungskomplex **155** benutzten Protokolls und des bestimmten Merkmals, z.B. Benutzermerkmals-Applet **175**, bereitgestellt. Zusätzlich werden die direkten Kommunikationen des Merkmals auf den Verbindungsbearbeitungskomplex **155** beschränkt. Weiterhin werden gemäß der bevorzugten Ausführungsform der Erfindung die Einschränkungen dynamisch über den Policy-Server **165** programmiert. Vom Policy-Server **165** werden alle Verwaltungsereignisse im Verbindungsbearbeitungskomplex **155** überwacht und die Kontrolle über alle seine Elemente aufrechterhalten. Dahingehend überwacht der Policy-Server den Gesundheitszustand der Komponenten des Softswitch und unterhält Konfigurationsinformationen hinsichtlich dieser Komponenten, wodurch der Policy-Server **165** zu einer strategischen Instanz bei der Erleichterung der Herstellung von Netzsicherheit gemäß den Grundsätzen der Erfindung wird. Es versteht sich weiterhin, daß während der Policy-Server in der Ausführungsform der Erfindung nach der Darstellung in Fig. 1 als Teil des Verbindungsbearbeitungskomplexes dargestellt ist, der Policy-Server auch getrennt und außerhalb des Verbindungsbearbeitungskomplexes gemäß den Grundsätzen der Erfindung implementiert sein kann.

[0048] Vorteilhafterweise wird gemäß einem Aspekt der Erfindung der Schutz gegen Netzschädigung in Verbindungsbearbeitungssystemen der nächsten Generation durch Verwendung einer semantischen Einschränkung von höheren Verbindungsbearbeitungsprotokollgrundelementen zusammen mit der dynamischen Programmierung der verschiedenen Netzwegeleitelemente zum Erzwingen von sowohl Verbindungssteuerung als auch Ratensteuerung realisiert, wie leicht aus der nachfolgenden beispielhaften Folge von Funktionen ersichtlich ist, die während einer beispielhaften Kommunikationssitzung auftreten, wobei eine Telefonverbindung zwischen dem POTS-Telefon **105** und IP-Telefon **115** hergestellt wird.

[0049] Beispielhafterweise ist das POTS-Telefon **105** herkömmlich mit dem SS7-Netz **120** und über eine POTS-Schnittstelle mit dem SS7-Vorrichtungsserver **170** verbunden. Der SS7-Vorrichtungsserver **170**, Rufkoordinator **160** und SIP-Vorrichtungsserver **170-3** sind über Datenverbindungen und mit dem IP-Netz **130** verbunden, das beispielsweise ein Internet-ähnliches Netz oder ein sogenanntes Intranet ist. Als solches ist der SIP-Vorrichtungsserver **170-3** über das IP-Netz **130** mit dem IP-Telefon **115** verbunden, z.B. über eine herkömmliche TCP-Verbindung. Um eine Telefonverbindung zwischen dem POTS-Telefon **105** und dem IP-Telefon **115** zu erreichen, treten folgende beispielhafte Funktionen ein.

[0050] Wenn die Telefonverbindung durch das POTS-Telefon **105** eingeleitet wird, wird das POTS-Telefon **105**, z.B. durch einen anrufenden Teilnehmer wie gewöhnlich abgehoben. Dadurch wird ein Zeichen zum SS7-Vorrichtungsserver **170** gesendet, der dem POTS-Telefon **105** Wählton zuführt oder dessen Zuführung bewirkt. Als Reaktion auf stattfindendes Wählen am POTS-Telefon **105** wird vom SS7-Vorrichtungsserver **170** der Wählton entfernt oder dessen Entfernung bewirkt und die gewählten Ziffern erhalten. Danach wird vom SS7-Vorrichtungsserver **170** ein Ereignis ausgelöst, das durch Beschreiben der Ereignissteuerungsdatei des den hierarchischen Namensraum des SS7-Vorrichtungsservers **170** darstellenden Baums erreicht werden kann. Wie schon bemerkt, kann der hierarchische Namensraum des Vorrichtungsservers **170** als eine Baum-Datenstruktur dargestellt werden.

[0051] Danach untersucht der aktive Rufkoordinator, z.B. Rufkoordinator **160** die Ereignissteuerungsdateien der Namensraumbäume aller von ihm unterstützten Vorrichtungsserver. Dahingehend ist sich der Rufkoordinator **160** der Konfiguration bzw. Topologie des IP-Netzes **130** einschließlich des Standorts, z.B. der Adressen der Vorrichtungsserver sowie der bestimmten Vorrichtungen hinter diesen Servern bewußt. So können beispielsweise beim Rufkoordinator **160** die Identitäten der Eigentümer von durch Telefonvorrichtungsserver bedienten Telefonen, gegebenenfalls die Telefonnummern solcher Telefone und die direkt durch Leitungsvorrichtungsserver bedienten Leitungen oder durch diese erreichbaren Telefone gespeichert sein. Die Informationen, die dafür notwendig sind, dem Rufkoordinator **160** diese Kenntnis zu vermitteln, können in den Rufkoordinator **160** vorprammiert sein, können vom Rufkoordinator **160** dynamisch unter Verwendung bekannter Prozesse entdeckt werden, oder können unter Verwendung einer

Kombination der obigen erreicht werden.

[0052] Als Reaktion auf das Lesen der Ereignissteuerungsdatei wie schon beschrieben wird vom Rufkoordinator **160** unternommen, zu bestimmen, welches Ereignis stattgefunden hat und welche Handlung erforderlich ist, wenn überhaupt. In dem oben beschriebenen bestimmten Beispiel bestimmt der Rufkoordinator **160**, daß ein Benutzer am POTS-Telefon **105** wünscht, die durch die gewählten Ziffern angezeigte Telefonnummer anzurufen. Um dies auf die vom Anrufer gewünschte Weise zu erreichen, veranlaßt der Rufkoordinator **160** die Ausführung der notwendigen Applets, z.B. Benutzermerkmals-Applet **175**.

[0053] Gemäß Ausführungsformen der Erfindung können die bestimmten, zur Herstellung einer Verbindung ausgeführten Applets folgende sein: ein einziges, auf den anrufenden Teilnehmer zugeschnittenes Applet; ein generisches Applet für den rufenden Teilnehmer; eine Folge von Applets, die auf den rufenden Teilnehmer zugeschnitten sind; eine generische Folge von Applets für den rufenden Teilnehmer; ein einziges Applet, das auf den gerufenen Teilnehmer zugeschnitten ist; ein generisches Applet für den gerufenen Teilnehmer; eine Folge von Applets die auf den gerufenen Teilnehmer zugeschnitten sind; eine generische Folge von Applets für den gerufenen Teilnehmer; eine beliebige Kombination der obigen; und/oder andere Applets die z.B. durch ISV für solche Anwendungen geschrieben sein können. Die Applets können sich alle im Rufkoordinator **160**, außerhalb des Rufkoordinators **160** (z.B. im Verbindungsbearbeitungskomplex **155**) oder einer Kombination beider befinden. Auch können die Applets alle vom Rufkoordinator **160** ausgeführt oder durch andere Ressourcen, z.B. Server oder Rufkoordinatoren ausgeführt werden, die an das IP-Netz **130** und/oder die SS7-Netze **120** bzw. **125** angeschlossen sind.

[0054] Beispielsweise kann der Anrufer ein Merkmal angegeben haben, das dem Anrufer erlaubt, eine mehrfache Telefonnummernfolge zur Kontaktaufnahme mit angegebenen gerufenen Teilnehmern als Funktion der gewählten Telefonnummer zu identifizieren. Wenn dies der Fall ist, wird vom Rufkoordinator **160** das Applet für dieses Merkmal ausgeführt, das bestimmen würde, ob die gewählte Nummer einer mehrfachen Telefonnummernfolge zugeordnet war. Sollte die gewählte Telefonnummer keiner mehrfachen Telefonnummernfolge zugeordnet sein, wird vom Rufkoordinator **160** das Vorgabe-Rufeinleitungs-Applet ausgeführt. Sollte die gewählte Telefonnummer einer mehrfachen Telefonnummernfolge zugeordnet sein, wird vom Rufkoordinator **160** die erste Telefonnummer der Folge besorgt und als Vorgabe-Rufeinleitungs-Applet ausgeführt. Wenn die Verbindung nicht hergestellt wurde, kehrt die Steuerung zum Folgen-Applet zurück, das gegebenenfalls die nächste Nummer besorgt und wieder das Vorgabe-Rufeinleitungs-Applet ausführt. Wenn es nicht möglich war, eine Verbindung zu irgendeiner der Telefonnummern in der Folge herzustellen, so wird vom Folgen-Applet die Steuerung zum Rufkoordinator **160** rückübertragen, der ein anderes Applet ausführt, z.B. eine Nachricht abspielt, um den rufenden Teilnehmer darüber zu informieren, daß der gerufene Teilnehmer nicht erreicht werden konnte.

[0055] Angenommen, es wird gewünscht, eine IP-Sprachverbindung für eine einzige Telefonnummer zu versuchen, wird vom Rufkoordinator **160** für das IP-Netz **130** die netzleitfähige Adresse des gerufenen Teilnehmers bestimmt, die den erhaltenen Ziffern entspricht. Dies wird durch einen Umcodierer durchgeführt, der sich im Rufkoordinator **160** befindet, oder diesem zugeordnet ist. Der Umcodierer ist im wesentlichen eine Wegeleitmaschine. Die Funktion des Umcodierers besteht darin, einem Applet, z.B. dem gegenwärtig ablaufenden Applet eine beschränkte Liste von Adressen für Gateway-Vorrichtungsserver oder Telefonvorrichtungsserver zuzuführen, die die Verbindung möglicherweise herstellen können.

[0056] Bei der gegenwärtigen beispielhaften Ausführungsform, bei der eine IP-Verbindung gewünscht wird, sendet der Umcodierer die Adresse des SIP-Vorrichtungsservers **170-3** zurück. Vom Rufkoordinator **160** wird als Klient Dienst vom SIP-Vorrichtungsserver **170-3** angefordert. Insbesondere fordert der Rufkoordinator **160** an, daß der SIP-Vorrichtungsserver **170-3** eine Verbindung zu der vom POTS-Telefon **105** erhaltenen Telefonnummer herstelle. Dies wird durch Einschreiben eines zutreffenden Befehls, z.B. eines Befehls Verbindung herstellen, in die Ereignissteuerungsdatei des Namensraum-Baums des SIP-Vorrichtungsservers **170-3** erreicht.

[0057] Als Reaktion auf die Dienstanforderung vom Rufkoordinator **160**, z.B. über seine herkömmliche TCP/IP-Schnittstelle, beginnt der SIP-Vorrichtungsserver **170-3** das Verfahren zur Herstellung der angeforderten Verbindung von sich zum IP-Netz **130** und letztendlich zum IP-Telefon **115**. Dies wird durch Verwendung herkömmlich verfügbarer Protokolle des SS7-Netzes **120** und IP-Netzes **130** bewirkt und ist gemäß einem Aspekt der Erfindung vollständig transparent für den Rufkoordinator **160**. Bei Erreichen einer Verbindung zum IP-Telefon **115** veranlaßt der Rufkoordinator **160** die Herstellung eines Medienweges zwischen dem SS7-Vorrichtungsserver **170** und SIP-Vorrichtungsserver **170-3**. Dies wird durch vom Rufkoordinator **160** durch Einschreiben von Dienstanforderungen von Medienkonnektivität in die Ereignissteuerungsdatei des Namensraumbaums des jeweiligen SS7-Vorrichtungsservers **170** bzw. SIP-Vorrichtungsservers **170-3** erreicht.

[0058] Bei erfolgreichem Anschluß und Herstellung der Verbindung wird die Verbindung vom Rufkoordinator **160** überwacht, sollte weiterer Dienst auf der Verbindung erforderlich sein. Beispielsweise kann als Reaktion darauf, daß eine der Kommunikationsvorrichtungen „auflegt", ein Verbindungsabbau angefordert werden. Als Alternative kann zusätzlich Merkmalsbearbeitung wie beispielsweise Anklopfen, Rufumlegung oder Gebührenübernahme angefordert werden. Wie bei dem Verbindungsaufbau wird die Notwendigkeit, einen solchen Dienst bereitzustellen, durch an die Ereignissteuerungsdatei des Namensraumbaums des jeweiligen SS7-Vorrichtungsservers **170** und/oder SIP-Vorrichtungsservers **170-3** eingeschriebene Anforderungen angezeigt. Vom Rufkoordinator **160** wird die Ereignissteuerungsdatei gelesen, die entsprechenden Applets gefahren und als Klient Dienstanforderungen an die zutreffenden Vorrichtungsserver ausgegeben.

[0059] Zum Abschließen der Verbindung wird beispielsweise das POTS-Telefon **105** aufgelegt. Dieses Ereignis wird in die Ereignissteuerungsdatei des Namensraumbaums des SS7-Vorrichtungsservers **170** eingeschrieben und der Rufkoordinator **160** erkennt das Ereignis. Als Reaktion auf das Ereignis wird vom Rufkoordinator **160** ein Applet gefahren. Bei einer Ausführungsform der Erfindung kann das Applet Auslösedienst vom SS7-Vorrichtungsserver **170** und SIP-Vorrichtungsserver **170-3** durch Einschreiben eines Auslösebefehls in jede ihrer Ereignissteuerungsdateien zusammen mit der Angabe der jeweiligen auszulösenden Telefonnummer anfordern.

[0060] Auf ähnliche Weise wird, wenn das IP-Telefon die Verbindung abschließt, eine Anzeige dieses Ereignisses in die Ereignissteuerungsdatei des Namensraum-Baums des SIP-Vorrichtungsservers **170-3** eingeschrieben. Bei Erkennung dieses Ereignisses in der Ereignissteuerungsdatei des SIP-Vorrichtungsservers **170-3** wird vom Rufkoordinator **160** das zugehörige Applet ausgeführt. In einer zweiten Ausführungsform der Erfindung kann das Applet Auslösedienst vom SS7-Vorrichtungsserver 17770 und SIP-Vorrichtungsserver **170-3** durch Einschreiben eines Auslösebefehls in jede ihrer Ereignissteuerungsdateien zusammen mit der Angabe der auszulösenden Telefonnummer anfordern.

[0061] Wie aus der Beschreibung der obigen bevorzugten Ausführungsform ersichtlich, bedeutet die Herstellung des beispielhaften Telefoniedienstes die Ausführung von mehreren Verfahren bzw. Prozeßsträngen, z.B. den Rufkoordinatoren, den Vorrichtungsservern und den Merkmals-Applets, und die Verwendung mehrerer Protokolle über heterogene Netze hinweg. Weiterhin wird wie oben angeführt die bevorzugte Ausführungsform unter Verwendung von Systemen ausgeführt, die virtuelle Maschinen, z.B. die Java Virtual Machine benutzen. Als solches ist die Herstellung von Netzsicherheit von wesentlicher Bedeutung, um sicherzustellen, daß keine einzelne Anwendung Netzressourcen willkürlich mißbrauchen kann und dadurch das Netz schädigen oder den Netzwirkungsgrad vermindern kann. Weiterhin und insbesondere für Verbindungsbearbeitungssysteme wird durch die Herstellung von Netzsicherheit sichergestellt, daß irgendein durch ein bestimmtes Merkmal verursachter Schaden auf dieses bestimmte Merkmal, z.B. eine Verbindung, lokalisiert ist und die übrigen Merkmale im Verbindungsbearbeitungssystem normal funktionieren.

[0062] Wie schon erwähnt, wird gemäß den Grundsätzen der Erfindung Netzsicherheit unter Verwendung semantischer Einschränkung von höheren Verbindungsbearbeitungsprotokollgrundelementen zusammen mit dynamischer Programmierung der verschiedenen Netzwegeleitelemente zum Erzwingen von sowohl Verbindungs- als auch Ratensteuerung erreicht. Beispielhafterweise wird durch eine solche semantische Einschränkung die Beschaffenheit der Nachrichten eingeschränkt, die zwischen den verschiedenen Komponenten eines Softswitch ausgetauscht werden können. Weiterhin wird durch Verbindungssteuerung die Anzahl von Verbindungen zwischen verschiedenen Komponenten des Softswitch begrenzt und durch Ratensteuerung wird die Rate festgelegt, mit der diese Verbindungen hergestellt werden. Gemäß einer Ausführungsform der Erfindung wird eine solche Verbindungssteuerung und Ratensteuerung durch dynamisches Umprogrammieren verschiedener Netzwegeleitelemente erreicht. Gemäß den Grundsätzen der Erfindung wird Netzsicherheit durch Anwenden der semantischen Einschränkung durch Isolieren des bestimmten, durch den Verbindungsbearbeitungskomplex, z.B. den Verbindungsbearbeitungskomplex **155**, und das bestimmte Merkmal, z.B. Benutzermerkmals-Applet **175** eingesetzten Protokolls bereitgestellt. Zusätzlich sind die direkten Kommunikationen des Merkmals auf den Verbindungsbearbeitungskomplex **155** beschränkt. Weiterhin werden gemäß der bevorzugten Ausführungsform der Erfindung die Einschränkungen dynamisch über den Policy-Server **165** programmiert. Vom Policy-Server **165** werden alle Verwaltungsereignisse im Verbindungsbearbeitungskomplex **155** überwacht und die Kontrolle über alle seine Elemente aufrechterhalten. Dahingehend wird vom Policy-Server der Gesundheitszustand der Komponenten des Softswitch überwacht und Konfigurationsinformationen hinsichtlich dieser Komponenten unterhalten, wodurch der Policy-Server zu einer strategischen Instanz wird, indem er die Herstellung von Netzsicherheit gemäß den Grundsätzen der Erfindung erleichtert.

[0063] Insbesondere ist die Fig. 4 ein Flußdiagramm von beispielhaften Operationen **400** zur Herstellung von Netzsicherheit in Kommunikationsnet-

zen gemäß den Grundsätzen der Erfindung. Insbesondere wird eine Kommunikationssitzung, z.B. eine Verbindungsbearbeitungsanforderung eingeleitet (Block **410**). Es wird (werden) das (die) zutreffende(n) Merkmals-Applet(s) für die bestimmte Kommunikationssitzung ausgewählt (Block **420**). Gemäß verschiedenen Ausführungsformen der Erfindung können die Merkmals-Applets (i) direkt innerhalb des Verbindungsbearbeitungskomplexes, (ii) direkt vom Softswitch, (iii) von einem Benutzer; (iv) von einem unabhängigen Softwarelieferanten (ISV-Independent Software Vendor); (v) vom Diensteanbieter oder (vi) einer beliebigen Kombination der obigen ausgewählt oder geliefert werden. Als Funktion der ausgewählten Merkmals-Applets und der Kommunikationssitzung werden gemäß einem Aspekt der Erfindung vom Policy-Server (siehe, z.B. Policy-Server **165** in Fig. 1) gewisse Ratensteuerungs- und Verbindungssteuerungsmerkmale eingeleitet und dynamisch in ausgewählte Instanzen des Netzes einprogrammiert (Block **430**).

[0064] Insbesondere wird vom Policy-Server bestimmt, wo das Merkmals-Applet gespeichert ist und der Weg vom gespeicherten Merkmals-Applet zum Verbindungssteuerungskomplex, d.h. dem Softswitch, bestimmt. Danach bestimmt der Policy-Server die Netzelemente entlang dem oben erwähnten Weg. Insbesondere buchen sich die Netzelemente im Softswitch-gesteuerten Netz gemäß der bevorzugten Ausführungsform der Erfindung bei einem Verzeichnisserver ein und erleichtern damit die Herstellung eines sogenannten verzeichnisfähigen Netzes (directory enabled network). In einem solchen verzeichnisfähigen Netz kann der Policy-Server den Verzeichnisserver abfragen, um sicherzustellen, welches der registrierten Netzelemente sich entlang dem entsprechenden Weg im Netz befinden, und die verschiedenen registrierten Fähigkeiten und Eigenschaften solcher Netzelemente. Gemäß der bevorzugten Ausführungsform werden diese Netzelemente durch Einleiten und Implementieren einer neuen Ratensteuerungs- und Verbindungssteuerungs-Policy umprogrammiert.

[0065] Insbesondere wird durch eine solche Ratensteuerungs- und Verbindungssteuerungs-Policy beispielhafterweise die Art von Netzinstanzen angegeben, die durch ein Merkmals-Applet kontaktiert werden können, und die Anzahl von Nachrichten pro Zeitperiode, die für jede bestimmte Kommunikation zulässig sein wird. So wird eine gegebene Policy gemäß der bevorzugten Ausführungsform durch Übertragen der Policy in einem wohlbekannten Kommunikationsprotokoll zu den Netzelementen auf dem identifizierten Weg implementiert. Weiterhin werden solche Übertragungen von besonderen Codefragmenten, sogenannten PEP-Punkten (Policy Enforcement Points-Policy-Zwangsdurchführungs-Punkten) empfangen. PEP sind wohlbekannte Softwarefragmente, die zwei sogenannte „Seiten" aufweisen. Eine PEP-Fragmentseite nimmt übertragene Policies in einem wohlbekannten Kommunikationsprotokoll an. Die andere PEP-Fragmentseite sendet Steuersignale zu besonderen Vorrichtungen in ihrem Zuständigkeitsbereich.

[0066] Beispielsweise wird ein beispielhafter PEP für ein wohlbekanntes paketvermitteltes Sprach-Gateway (Packet Voice Gateway-PVG) oder einen Router Policies vom Policy-Server empfangen, die Policies in eine Folge von Befehlen umsetzen, die für die jeweilige Vorrichtung spezifisch sind, und diese Befehle zu den Vorrichtungen übertragen. Es versteht sich, daß die Übertragung solcher Befehle auf verschiedene Weise erreicht werden kann: (a) der PEP kann auf der Vorrichtung selbst ablaufen, so daß die Übertragung die Form von Prozeß-Prozeß-Kommunikation (IPC-inter-process communication) annehmen kann; oder (b) der PEP kann auf einer Hostmaschine im Netz ablaufen und die Befehlsfolgen über ein Befehlsprotokoll, z.B. das wohlbekannte SNMP-Protokoll (Simple Network Management Protocol) senden, das von der Vorrichtung, d.h. dem Netzelement, unterstützt wird, oder (c) der PEP kann auf einer bestimmten Hostmaschine auf dem Netz ablaufen, eine Fernanmeldungssitzung auf dem Netzelement öffnen und die wohlbekannte CLI-Schnittstelle (Command Line Interface) zum Senden von Befehlsfolgen zum Netzelement benutzen.

[0067] Während sich die obige Besprechung auf Kommunikationen zwischen dem Policy-Server und den PEP und zwischen den PEP und den Netzelementen konzentrierte, die im wesentlichen „Einweg"-Kommunikationen waren, d.h. vom Policy-Server zu den PEP und von den PEP zu den Netzelementen, versteht es sich, daß Informationen auf andere Weisen fließen können. Das heißt, gemäß weiteren Ausührungsformen der Erfindung können Kommunikationen vom Netzelement zum PEP und dem Policy-Server fließen. Solche Informationen werden als ein „Ereignis" gekennzeichnet. So kann ein Netzelement ein oder mehrere Ereignisse erzeugen, die für einen PEP freigelegt werden. Beispielhafterweise kann der PEP ein Netzelement auf solche Ereignisse überwachen oder periodisch gewisse durch die Vorrichtung gespeicherte und aktualisierte Informationen lesen oder solche Ereignisse unter Verwendung eines wohlbekannten Protokolls vom Netzelement empfangen. Als solches werden vom PEP wiederum diese Ereignisse für den Policy-Server freigelegt, wobei diese Ereignisse eine oder mehrere Handlungen auslösen können. Diese Handlungen können die Übertragung von einer oder mehreren Policies zu den PEP ergeben, die gemäß der bevorzugten Ausführungsform der Erfindung eine Umprogrammierung der Netzelemente anfordern. So können an einem Netzelement erzeugte Ereignisse die Umprogrammierung des Netzelements entsprechend einer neu-

en Policy ergeben und dadurch das Verhalten des Elements ändern.

[0068] Wenn beispielsweise zwei Ereignisse A und B an Netzelementen 1 bzw. 2 erzeugt und für den Policy-Server freigelegt werden, wird der Policy-Server gemäß der bevorzugten Ausführungsform die zwei Ereignisse korrelieren und neue Policies zum Umprogrammieren der Netzelemente ausgeben. Die vom Policy-Server unterstützte Korrelation wird folgendes umfassen: (a) UND-Verknüpfung eines oder mehrerer Ereignisse; (b) ODER-Verknüpfung eines oder mehrerer Ereignisse; (c) Folgen von Ereignissen mit Wiederholung; (d) Folgen von Ereignissen mit sogenannten „Platzhaltern" und gewissen spezifischen Ereignissen; oder (e) die Abwesenheit eines oder mehrerer Ereignisse. So sind gemäß der bevorzugten Ausführungsform Ereignisausdrücke erlaubt, die (a) bis (e) wie oben aufgeführt in jeder logischen Reihenfolge verbinden. So kann wie ersichtlich eine äußerst komplexe Menge von Ereignissen durch solche Ereignisausdrücke erfaßt oder beschrieben werden, die zum Identifizieren einer verschiedenartigen Menge von Zuständen benutzt werden kann, die an verschiedenen Netzelementen auftreten. Der Policy-Server ist daher gemäß den Grundsätzen der Erfindung in der Lage, die verschiedenen Zustände zu verstehen und durch Übertragen von spezifischen neuen Policies zum Auswählen von Netzelementen Korrektur- oder Präventivmaßnahme(n) zu ergreifen.

[0069] Beispielsweise wird, wie in der Ausführungsform unten besprochen, der Policy-Server in gewissen Netzen, z.B. SS7-Netz **120** der Fig. 1, eine Firewall programmieren, um sicherzustellen, daß ratengesteuerter Zugang zu diesem Netz implementiert ist. Wie wohlbekannt ist, werden Firewalls zur Herstellung verschiedener Sicherheitsmaßnahmen zum Schützen von Netzen gegen externe Sicherheitsverstöße, wie beispielsweise die Einführung von Computerviren, benutzt. Durch diese Sicherheitsanordnung wird im wesentlichen ein getrenntes Computersystem, d.h. die Firewall, zwischen das Privatnetz und das öffentliche Netz, z.B. das Internet, plaziert. Diese Firewalls sind Software basierte Gateways, die typischerweise zum Schutz von Computern an einem LAN-Netz (local area network) gegen Angriffe von Außenseitern, d.h. unberechtigten Benutzern, installiert sind. Die Firewall unterhält Kontrolle über Kommunikationen von und zu dem Privatnetz. Im Wesentlichen werden durch die Firewall allen das Privatnetz nutzenden Benutzern gewisse Sicherheitsmaßnahmen auferlegt. Beispielsweise können Firewalls Zugang zu neuen Internet-Diensten oder Angeboten auf dem World Wide Web (WWW) blockieren, da die Sicherheitsfolgen unbekannt sind oder durch die gegenwärtige Firewallkonfiguration nicht berücksichtigt werden.

[0070] So wird gemäß den Grundsätzen der Erfindung der Policy-Server die entsprechenden Firewalls programmieren, um unter anderem sicherzustellen, daß ISV ratengesteuerten Zugang zur Hostinstanz besitzen, z.B. einem als Host für das Merkmals-Applet dienenden Server, oder daß ein sich gastweise in einem Netz (z.B. SS7-Netz) aufhaltendes Merkmals-Applet ratengesteuerten Zugang zu einer vorbestimmten Menge von Netzressourcen besitzt, oder daß ein gastweises Applet Zugang zum Rufkoordinator hat. Nach der dynamischen Programmierung der Ratensteuerung und Verbindungssteuerung durch den Policy-Server gemäß der oben angeführten Erfindung wird vom Verbindungsbearbeitungskomplex **155** eine sitzungsweite Zugangssteuerung ausgeübt und werden Verbindungssteuerungsgrundelemente von allen Netzressourcen angenommen, die an der Verbindungsbearbeitunganforderung teilnehmen (siehe Fig. 4, Block **440**). Gemäß der bevorzugten Ausführungsform wird die durch den Softswitch ausgeübte sitzungsweite Steuerung solange fortgeführt bis die Verbindungsbearbeitung vollendet ist (siehe Fig. 4, Block **450**) und bei Verbindungsvollendung wird die Kommunikationssitzung abgeschlossen (siehe Fig. 4, Block **460**).

[0071] Als weitere Darstellung der oben beschriebenen Einzelheiten und Grundsätze der Erfindung zeigt Fig. 5 ein beispielhaftes Netzverwaltungsszenario **500** mit gemäß den Grundsätzen der Erfindung hergestellten Netzsicherheitsmerkmalen. Das beispielhafte Szenario **500** beginnt damit, daß das gastweise auf dem Host-Server **510** befindliche Merkmals-Applet **505** versucht, sich an den im Verbindungsbearbeitungskomplex **515** residenten Vorrichtungsserver **530** anzuschließen. Wie schon ausgeführt wird das gastweise Applet in der bestimmten Verbindungssitzung benutzt und stellt gewisse Verbindungsbearbeitungsmerkmale her, die von dieser Verbindungssitzung erfordert werden. Gemäß den Grundsätzen der Erfindung wird die Verbindung des Merkmals-Applets **505** mit dem Vorrichtungsserver **530** durch den Policy-Server **535** gesteuert. Gemäß der vorliegenden Ausführungsform der Erfindung ist der Policy-Server **535** eine getrennte Instanz im Kommunikationssystem. Weiterhin wird vom Rufkoordinator **520** gesteuert, welche durch das Merkmals-Applet **505** eingeleiteten Ereignisse zum Vorrichtungsserver **530** und/oder Vorrichtungsserver **525** gemultiplext werden, um irgendwelche durch das Merkmals-Applet **505** verursachte Verfälschung im Rufkoordinator **520** zu lindern. Zusätzlich wird wie oben beschrieben vom Rufkoordinator **520** eine sitzungsweite Zugangssteuerung ausgeübt und werden Verbindungssteuerungsgrundelemente von allen Netzressourcen, z.B. dem Amtsverbindungsnetz (IXC-inter-exchange network) **555** angenommen, die an der Kommunikationssitzung teilnehmen.

[0072] Gemäß dem beispielhaften Szenario **500** kann das Merkmals-Applet **505** auch versuchen, sich

böswillig an den im ISV **540** residenten Vorrichtungsserver **545** anzuschließen, z.B. um den Vorrichtungsserver anzuweisen, seinem zugehörigen Vorrichtungs-Gateway Dienst zu verweigern. Wie oben aufgeführt, wird der Policy-Server **535** gemäß einem Aspekt der Erfindung eine dem ISV **540** zugeordnete Firewall programmieren, um unter anderem sicherzustellen, daß der ISV **540** einen ratengesteuerten Zugang zur Hostinstanz (z.B. dem Host-Server **510**) besitzt, der als Host für das Merkmals-Applet dient, oder daß das Merkmals-Applet einen ratengesteuerten Zugang zu einer vorbestimmten Menge von notwendigen Ressourcen besitzt. Weiterhin kann der Vorrichtungsserver **545** gemäß dem beispielhaften Szenario **500** versuchen, sich an den Rufkoordinator **520** anzuschalten, um die gewünschte Wegeleitung des Rufs zu leiten. Wie zuvor wird der Policy-Server **535** gemäß einem Aspekt der Erfindung eine im ISV **540**, dem Verbindungsbearbeitungskomplex **515** und/oder dem IXC-Netz **555** residente Firewall programmieren, um unter anderem sicherzustellen, daß in der Kommunikationssitzung ratengesteuerter Zugang und Verbindungssteuerung, d.h. Netzsicherheit bereitgestellt wird. Weiterhin kann das Merkmals-Applet **550**, wie durch die bestimmte Verbindungsbearbeitungsanforderung der Sitzung erforderlich, Zugang zum Rufkoordinator **520** erfordern. Wie beim Merkmals-Applet **505** ist die Verbindung des Merkmals-Applet **550** mit dem Rufkoordinator **520** durch den Policy-Server **535** gesteuert. Weiterhin wird vom Rufkoordinator **520** gesteuert, welche durch Merkmals-Applet **550** eingeleiteten Ereignisse zum Vorrichtungsserver **530** und/oder Vorrichtungsserver **535** gemultiplext werden, um irgendeine durch die Ausführung des Merkmals-Applets **550** verursachte Verfälschung im Rufkoordinator **520** zu lindern.

[0073] Vorteilhafterweise wird gemäß der Erfindung der Schutz gegen Netzschädigung in Verbindungsbearbeitungssystemen der nächsten Generation durch Verwendung einer semantischen Einschränkung von höheren Verbindungsbearbeitungsprotokollgrundelementen zusammen mit dynamischer Programmierung der verschiedenen Netzwegeleitelemente zum Erzwingen von sowohl Verbindungs- als auch Ratensteuerung realisiert.

[0074] Wie oben aufgeführt, kann die vorliegende Erfindung in der Form von Verfahren und Vorrichtungen zum Ausüben dieser Verfahren verwirklicht sein. Auch kann die Erfindung in der Form von Programmcode verwirklicht sein, der in physikalischen Medien wie beispielsweise Disketten, CD-ROM, Festplattenlaufwerken oder einem beliebig anderen durch Maschinen lesbaren Speichermedium verwirklicht ist, wobei, wenn der Programmcode in eine Maschine wie beispielsweise einen Computer eingeladen und von ihr ausgeführt wird, die Maschine zu einer Vorrichtung zur Ausübung der Erfindung wird. Auch kann die Erfindung in der Form von Programmcode, beispielsweise in einem Speichermedium verwirklicht sein, der in eine Maschine eingeladen und/oder von ihr ausgeführt oder über irgendein Übertragungsmedium wie beispielsweise über elektrische Verdrahtung oder Verkabelung, über Glasfasern oder über elektromagnetische Strahlung übertragen wird, wobei, wenn der Programmcode in eine Maschine wie beispielsweise einen Computer eingeladen und von ihr ausgeführt wird, die Maschine zu einer Vorrichtung zur Ausübung der Erfindung wird. Wenn sie auf einem Universalprozessor implementiert sind, kombinieren sich die Programmcodesegmente mit dem Prozessor zur Bereitstellung einer einmaligen Vorrichtung, die wie bestimmte Logikschaltungen fungiert.

[0075] Weiterhin sollen grundsätzlich alle hier aufgeführten Beispiele und bedingten sprachlichen Aufführungen ausdrücklich nur Lehrzwecken dienen, um dem Leser bei dem Verständnis der Grundsätze der Erfindung und der durch die Anmelderin beigetragenen Konzepte zur Weiterentwicklung der Technik behilflich zu sein und sind so auszulegen, daß sie keine Begrenzung dieser besonders angeführten Beispiele und Zustände darstellen. Weiterhin sollen alle hiesigen Aussagen über Grundsätze, Aspekte und Ausführungsformen der Erfindung wie auch bestimmte Beispiele derselben sowohl strukturelle als funktionelle Äquivalente derselben umfassen. Zusätzlich ist beabsichtigt, daß diese Äquivalente sowohl gegenwärtig bekannte Äquivalente wie auch zukünftig entwickelte Äquivalente, d.h. alle entwickelten Elemente, die ungeachtet der Struktur die gleiche Funktion durchführen, einschließen.

[0076] So wird beispielsweise der Fachmann erkennen, daß die hiesigen Blockschaltbilder konzeptionelle Ansichten beispielhafter Schaltungen darstellen, die die Grundsätze der Erfindung verwirklichen. Auf ähnliche Weise versteht es sich, daß alle Flußdiagramme, Zustandsübergangsdiagramme, Pseudocode, Programmcode und dergleichen verschiedene Prozesse darstellen, die im wesentlichen in einem von einem Computer lesbaren Medium dargestellt und so durch einen Computer, eine Maschine oder einen Prozessor ausgeführt werden können, egal ob ein solcher Computer, eine solche Maschine oder ein solcher Prozessor ausdrücklich dargestellt sind oder nicht.

[0077] Das obige stellt nur die Grundsätze der vorliegenden Erfindung dar. Es versteht sich daher, daß der Fachmann in der Lage sein wird, verschienene Anordnungen auszuarbeiten, die obwohl sie hier nicht ausdrücklich beschrieben oder dargestellt sind, die Grundsätze der Erfindung verwirklichen und in ihrem Rahmen enthalten sind.

Patentansprüche

1. Verfahren zum Bereitstellen von Diensten in einem Kommunikationsnetz (**100**), mit folgenden Schritten:
Einleiten einer Kommunikationssitzung in dem Kommunikationsnetz;
als Reaktion auf das Einleiten der Kommunikationssitzung Ausführen eines ersten Verfahrens in einem Hostserver (**510**) zum Erbringen mindestens eines Dienstes in dem Kommunikationsnetz;
als Reaktion auf das Einleiten der Kommunikationssitzung Ausführen eines zweiten Verfahrens in einem Vorrichtungsserver (**170**, **170-1**, **170-2** oder **170-3**) zum Erbringen des mindestens einen Dienstes in dem Kommunikationsnetz; gekennzeichnet durch Ausführen einen dritten Verfahrens in einem Rufkoordinator (**160**) zum Empfangen und Bearbeiten von Anforderungen von dem Vorrichtungsserver und dem Hostserver bei dem Erbringen des mindestens einen Dienstes; und
Herstellen von Ratensteuerung und Verbindungssteuerung zwischen dem Hostserver, dem Vorrichtungsserver und dem Rufkoordinator, wobei die Verbindungssteuerung die Anzahl von Verbindungen für die Kommunikationssitzung begrenzt und die Ratensteuerung die Raten dieser Verbindungen festlegt.

2. Verfahren nach Anspruch 1, wobei das Herstellen der Ratensteuerung und der Verbindungssteuerung durch einen Policy-Server (**165**) durchgeführt wird.

3. Verfahren nach Anspruch 2, wobei die Operation des Herstellens der Ratensteuerung und der Verbindungssteuerung weiterhin folgendes umfaßt:
dynamisches Programmieren von mindestens einer Firewall in dem Kommunikationsnetz zum Beschränken des Zugriffs des ersten Verfahrens auf eine vorbestimmte Menge von Netzressourcen.

4. Verfahren nach Anspruch 3, wobei das Kommunikationssystem bei der Ausführung von mindestens einem des ersten Verfahrens, des zweiten Verfahrens oder des dritten Verfahrens eine Java Virtual Machine benutzt.

5. Verfahren nach Anspruch 4, wobei der Vorrichtungsserver und der Rufkoordinator in einer Klienten-Server-Anordnung verkoppelt sind.

6. Verfahren nach Anspruch 5, wobei der Vorrichtungsserver und mindestens einer der Rufkoordinatoren einen hierarchischen Namensraum (**300**) freilegt.

7. Verfahren nach Anspruch 4, wobei das erste Verfahren ein Merkmals-Applet ist.

8. Verfahren nach Anspruch 6, wobei der Vorrichtungsserver und der Rufkoordinator durch ein SS7-Zeichengabenetz (**120**) zusammengekoppelt sind.

9. Verfahren nach Anspruch 3, wobei der Policy-Server weiterhin folgende Operationen durchführt:
Überwachen der Kommunikationssitzung;
Unterhalten der Kontrolle über die Menge von Netzressourcen; und
Überwachen eines Betriebszustands des Hostservers, des Vorrichtungsservers und des Rufkoordinators.

10. Verfahren nach Anspruch 7, wobei das Merkmals-Applet über eine Verbindung zwischen dem Kommunikationsnetz und dem Server eines unabhängigen Softwarelieferanten heruntergeladen wird.

11. Verfahren nach Anspruch 2, wobei der Policy-Server bei der Herstellung der Ratensteuerung und der Verbindungssteuerung mindestens einen PEP (Policy Enforcement Point – Policy-Zwangsdurchführungspunkt) einsetzt.

12. Verfahren nach Anspruch 3, wobei der Vorrichtungsserver und der Rufkoordinator Teil eines Softswitch sind.

13. Verfahren nach Anspruch 12, wobei das Kommunikationsnetz mindestens ein PSTN (**120**, **125**) und mindestens ein IP-Netz (**130**) einschließt.

14. Verfahren nach Anspruch 13, wobei die hergestellte Ratensteuerung eine Verkehrsbandbreite herstellt, die mit dem Kommunikationsnetz geteilt wird.

15. Verfahren nach Anspruch 13, wobei die hergestellte Verbindungssteuerung eine Anzahl von in dem Kommunikationsnetz hergestellten Kommunikationsverbindungen beschränkt.

16. Kommunikationssytem (**100**) mit Mitteln zum Ausführen der Schritte eines Verfahrens gemäß einem beliebigen der vorhergehenden Ansprüche.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

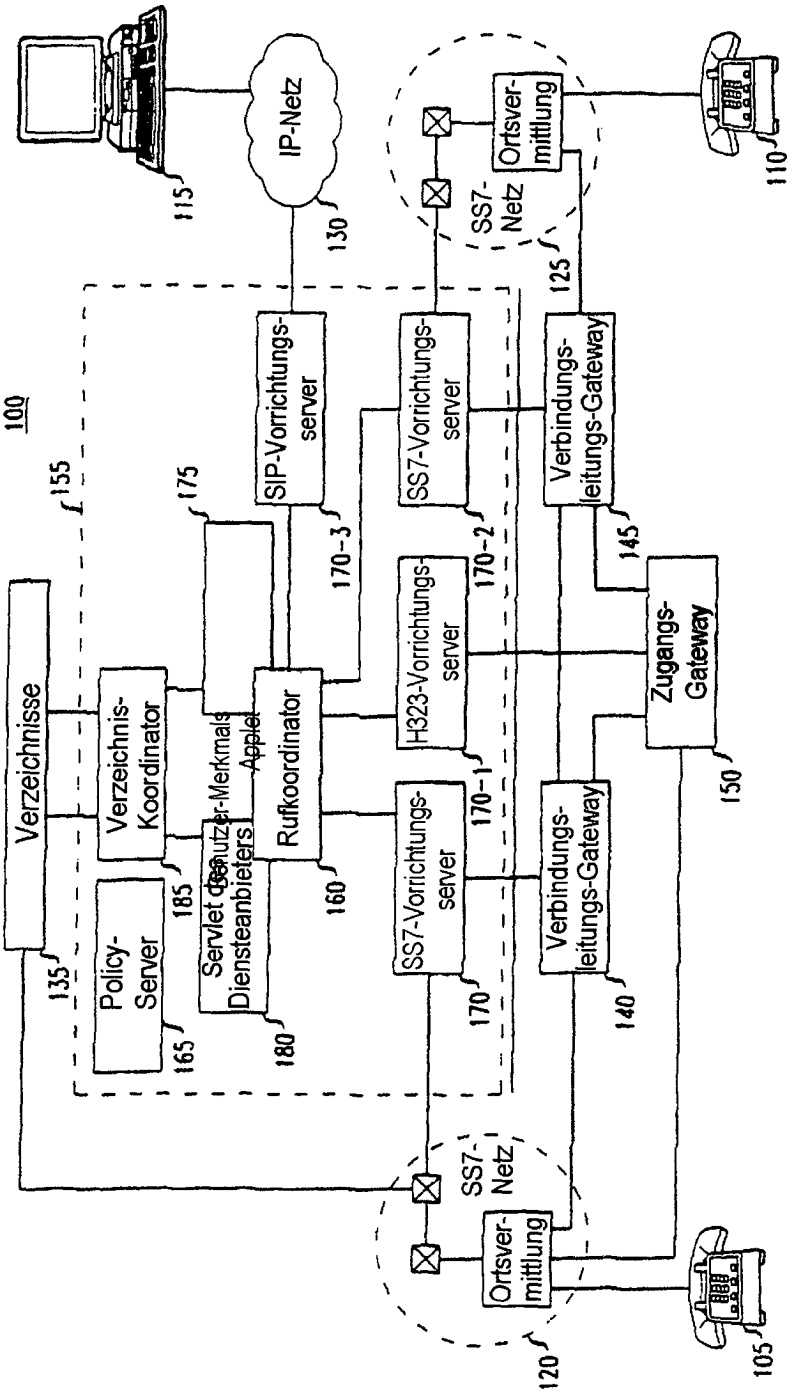


FIG. 2

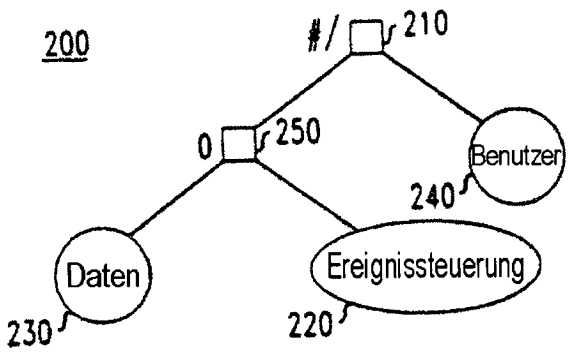

200
#/
210
0
250
Benutzer
240
Daten
230
Ereignissteuerung
220

FIG. 3

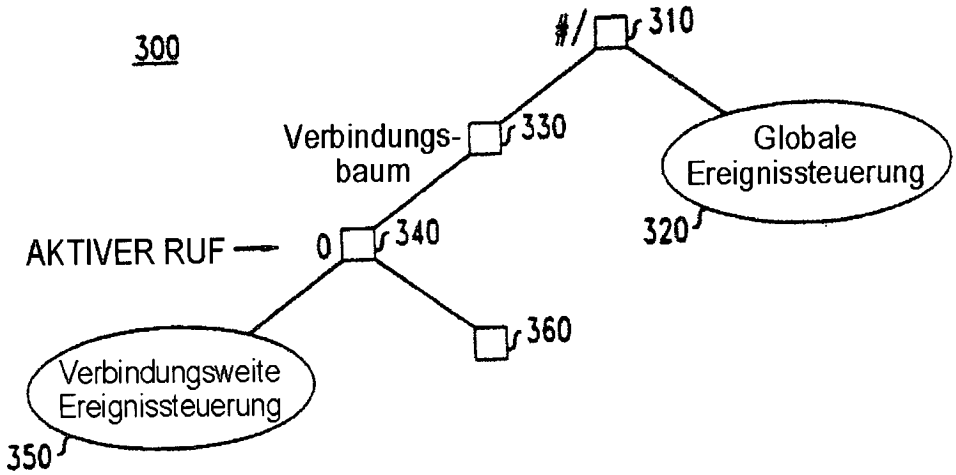

300
#/
310
Verbindungs-
baum
330
Globale
Ereignissteuerung
320
AKTIVER RUF
0
340
360
Verbindungsweite
Ereignissteuerung
350

FIG. 4

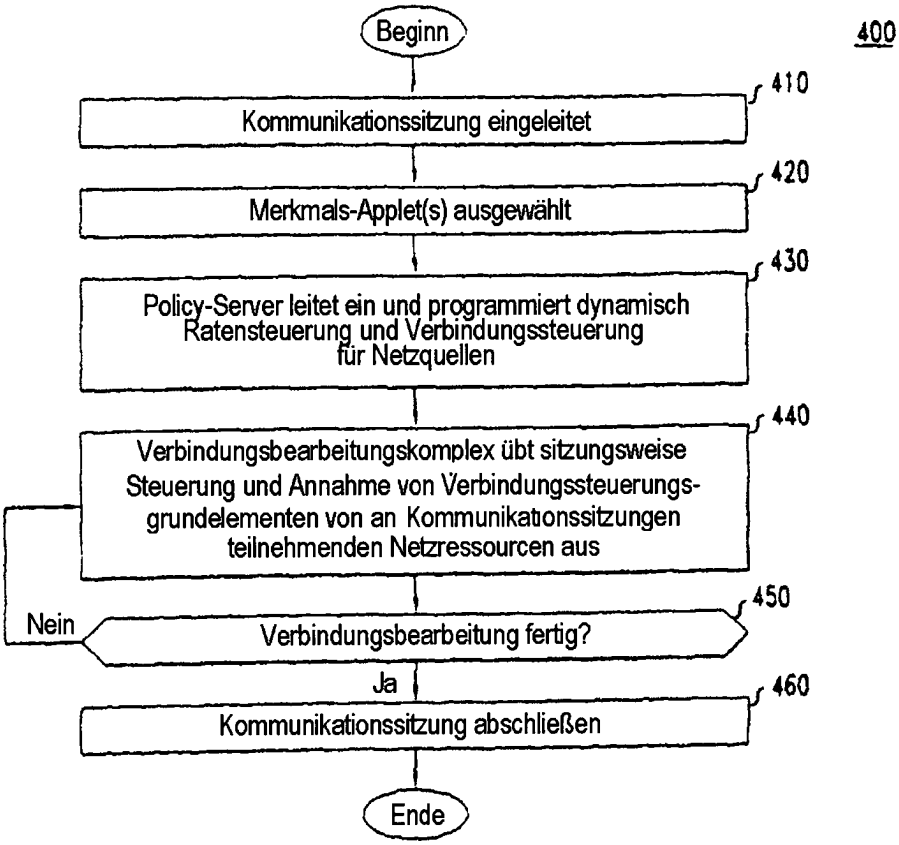
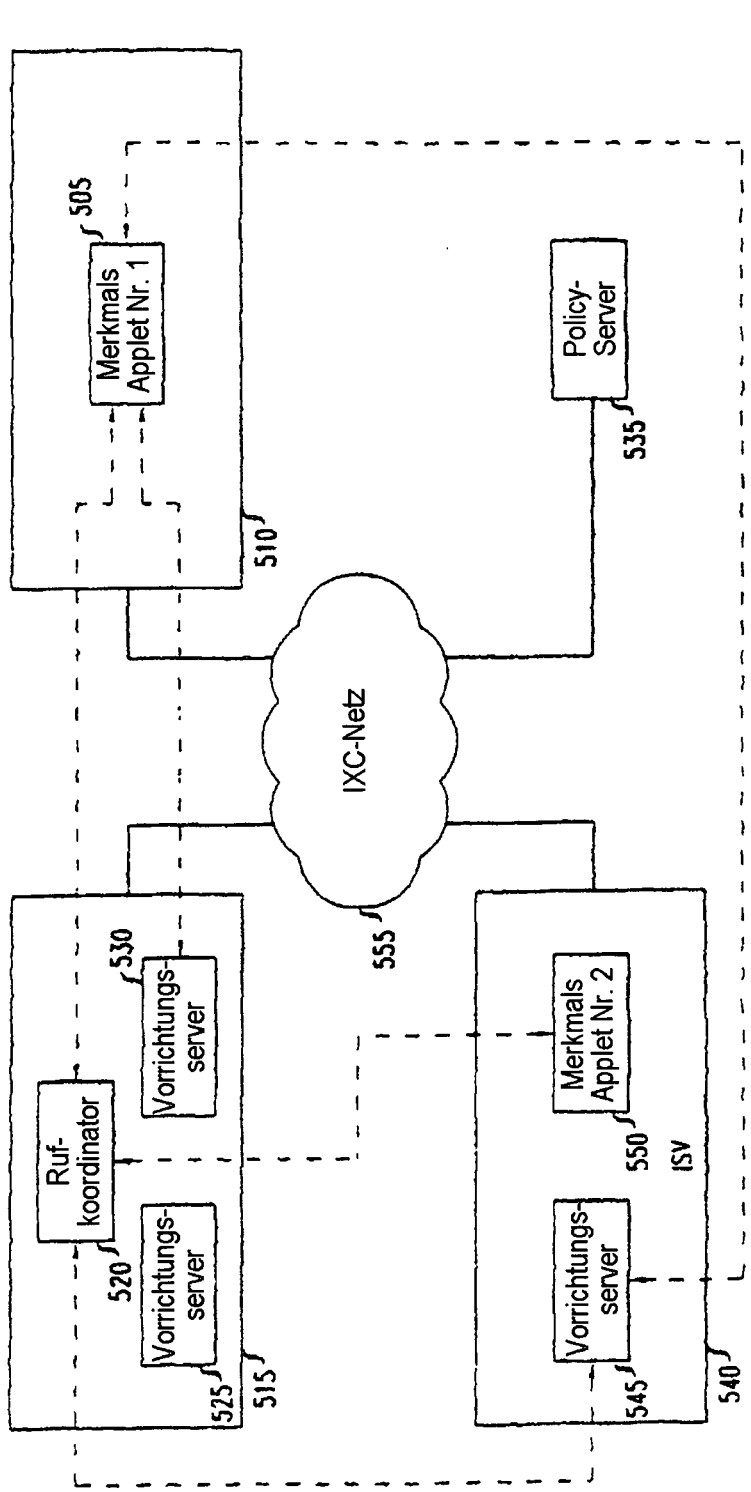

400
Beginn
410
Kommunikationssitzung eingeleitet
420
Merkmals-Applet(s) ausgewählt
430
Policy-Server leitet ein und programmiert dynamisch Ratensteuerung und Verbindungssteuerung für Netzquellen
440
Verbindungsbearbeitungskomplex übt sitzungsweise Steuerung und Annahme von Verbindungssteuerungs-grundelementen von an Kommunikationssitzungen teilnehmenden Netzressourcen aus
450
Nein
Verbindungsbearbeitung fertig?
Ja
460
Kommunikationssitzung abschließen
Ende

FIG. 5


500
505
Merkmals Applet Nr. 1
510
Policy-Server
535
IXC-Netz
555
530
Vorrichtungs-server
Ruf-koordinator
520
Vorrichtungs-server
525
515
Merkmals Applet Nr. 2
550
ISV
Vorrichtungs-server
545
540