(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. November 2007 (01.11.2007)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2007/121900 A1

(51) Internationale Patentklassifikation:
H04L 29/12 (2006.01) *H04L 12/28* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2007/003383

(22) Internationales Anmeldedatum:
17. April 2007 (17.04.2007)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2006 017 940.4 18. April 2006 (18.04.2006) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.** [DE/DE]; Hansastrasse 27c, 80686 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **TÖLLE, Dietmar** [DE/DE]; Sommerstrasse 44, 81543 München (DE).

(74) Anwalt: **PFENNING, MEINIG & PARTNER GBR**; Theresienhöhe 13, 80339 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR CREATING A CONNECTION TO A SERVICE PROVIDER BY USE OF AN IPV6-TOPOLOGY PREFIX

(54) Bezeichnung: VERFAHREN ZUR HERSTELLUNG EINER VERBINDUNG MIT EINEM DIENSTEANBIETER UNTER VERWENDUNG EINES IPV6-TOPOLOGIEPRÄFIXES

Nummer	IPv6 Access Node Prefix	IPv6 Edge Node Prefix
AN 1	2005:7BA9:3453:0027::/64	2005:7BA9:3453:0028::/64
AN 2	2005:7BA9:3453:0044::/64	2005:7BA9:3453:0045::/64
AN 3	2005:7BA9:3453:0063::/64	2005:7BA9:3453:0064::/64
AN x	usw.	usw.

(57) **Abstract:** This invention relates to a method for creating a connection from a user device to a computer (server) of a service provider via an access network and a transport network. Methods of this kind are required especially to connect user devices to service providers, for example over the internet as a transport network. In this arrangement the user devices are most commonly connected to the transport network via an access network, for example an ethernet-based network. The method according to the invention serves to connect a user device to at least one computer of a service provider connected to a transport network over an access network with at least one access node computer and over the transport network with at least one transmission node computer from the access network to the transport network, whereby the user device is assigned at least one IPv6 address. It is characterized in that each pairing of any one access node computer and any one transmission node computer is assigned an unambiguous pair of bit patterns, and for the respective pairing the access node computer and the transmission node computer are each assigned a topology prefix of the IPv6 address, which in each case contains one of the two bit patterns of the pair of bit patterns.

(57) **Zusammenfassung:** Die vorliegende Erfindung betrifft ein Verfahren zur Herstellung einer Verbindung eines Nutzergerätes mit einem Rechner (Server) eines Diensteanbieters über ein Zugangsnetz und ein Transportnetz. Derartige Verfahren werden insbesondere benötigt, um Nutzergeräte mit Serviceprovidern (Diensteanbietern) beispielsweise über das Internet als Transportnetz zu verbinden. Dabei sind die Nutzergeräte meistens über ein Zugangsnetz, beispielsweise ein Ethernet-basiertes Netz mit dem Transportnetz verbunden. Das erfindungsgemäße Verfahren dient der Verbindung eines Nutzergerätes mit mindestens einem mit einem Transportnetz verbundenen Rechner eines Diensteanbieters über ein Zugangsnetz mit mindestens einem Zugangsknotenrechner und über das Transportnetz mit mindestens einem Übergangsknotenrechner vom Zugangsnetz zum Transportnetz, wobei dem Nutzergerät mindestens eine IPv6-Adresse zugeordnet wird. Es ist dadurch gekennzeichnet, dass jeder Paarung aus je einem Zugangsknotenrechner und je einem Übergangsknotenrechner

[Fortsetzung auf der nächsten Seite]

WO 2007/121900 A1

RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

ein eindeutiges Paar von Bitmustern zugeordnet wird, und für die jeweilige Paarung dem Zugangsknotenrechner und dem Übergangsknotenrechner jeweils ein Topologiepräfix der IPv6-Adresse zugeordnet wird, das jeweils eines der beiden Bitmuster des Paares von Bitmustern enthält.

Verfahren zur Herstellung einer Verbindung

Die vorliegende Erfindung betrifft ein Verfahren zur Herstellung einer Verbindung eines Nutzergerätes mit einem Rechner (Server) eines Diensteanbieters über ein Zugangsnetz und ein Transportnetz. Derartige Verfahren werden insbesondere benötigt, um Nutzergeräte mit Serviceprovidern (Diensteanbietern) beispielsweise über das Internet als Transportnetz zu verbinden. Dabei sind die Nutzergeräte meistens über ein Zugangsnetz, beispielsweise ein Ethernet-basiertes Netz mit dem Transportnetz verbunden.

Insbesondere gewinnen Ethernet-basierte Netze dank ihrer Eigenschaften, wie Leistungsfähigkeit, Einfachheit, Skalierbarkeit und Kosteneffizienz, auch im Zugangsbereich (Access) immer mehr Bedeutung. Als Beispiel hierfür kann die Standardisierung von Ethernet für VDSL-basierte Zugangssysteme bei der IEEE und des Ethernet in der First Mile Allianz (EFM) genannt wer-

den.

Ethernet eignet sich auch als Kandidat für Multi-Service-Plattformen zum Transport in aggregierenden Netzen, wie beispielsweise Metronetzen.

Um die von den Nutzern gewünschten Dienste realisieren zu können, ist es erforderlich, sowohl die Dienste (Service) als auch die Kunden (Nutzer) voneinander zu trennen und zu identifizieren. Nur so ist es möglich, dass viele Kunden von vielen verschiedenen Internet-Dienstanbietern über dasselbe Zugangsnetz, beispielsweise ein Ethernet, verschiedene Dienste nutzen können. Es ist nicht nur wichtig, die einzelnen Kundendatenströme voneinander zu trennen, sondern auch erforderlich, diese einzeln kundenspezifisch abzurechnen.

Die Kunden- bzw. Diensttrennung im Internet verläuft heutzutage sehr simpel: Der Kunde trägt in einem von ihm genutzten Gerät eine von seinem Internet-Dienstanbieter gelieferte Zugangskennung (Login und Passwort) ein. Diese Zugangskennung ist meist haushaltsspezifisch, d.h. es wird weder eine richtige Diensttrennung noch eine Kundentrennung durchgeführt. Wird die Zugangskennung eingegeben und aktiviert, so wird vom Netzbetreiber, von dem die Zugangskennung kommt, eine temporäre IP-Adresse vergeben. Die Abrechnung erfolgt nach Zeitdauer der Adressvergabe (Zeittarif), nach Datenvolumen, das über die vergebene IP-Adresse transferiert wird (Volumentarif), oder über eine Pauschale (Flatrate). Die anfallenden Kosten werden dem Eigner der Zugangskennung in Rechnung gestellt.

Eine richtige Diensttrennung wird mit diesem Schema nicht durchgeführt, da nur Internet-Zugänge verkauft werden, keine Dienste an sich. Der einzige zugeordnete Dienst ist der Internet-Zugang selbst, über den alle anderen Dienste laufen, welche als solche aber nicht erkennbar sind.

Der Datentransport zwischen Kunden und Netzbetreiber läuft heute noch meist über DSL (Digitale Teilnehmeranschlußleitung, Digital Subscriber Line) und ATM (Asynchroner Übertragungsmodus, Asynchronous Transfer Mode) bis zum Internet-Übergangsknotenrechner (IP Edge Router). Der Kunde authentifiziert sich mit seiner Zugangskennung beim IP Edge Router (meist gleichzeitig auch BRAS (Broadband Remote Access Server), welcher auch die IP-Adresse (Internet-Protokoll-Adresse) nach erfolgreicher Authentifizierung vergibt. Die eingesetzten Protokolle sind bei diesem Verfahren PPP (Punkt-zu-Punkt-Protokoll, Point-to-Point Protocol) und PPPoE (PPP über Ethernet, PPP over Ethernet). Das PPP dient dabei zur Kundentrennung im BRAS. Kundentrennung heißt in diesem Falle meist Kundenanschlusstrennung, da die Zugangskennung meist im DSL-Zugangsrechner (DSL-Router) zentral eingegeben wird. Somit kann nur der Kundenanschluss identifiziert werden, nicht aber der Dienst oder der einzelne Nutzer. Die Figuren 1 und 2 zeigen zwei Beispiele, wie die Kundenanschlüsse funktionieren.

Fig. 1 zeigt den Protokollstack und das Anschlussschema der Anbindung eines VoIP-Telefons 11 (Internettelefonie-Telefon, Voice-over-Internet-Protocol-Telefone) an einen DSL-Anschluss über ein DSL-Modem 7. Die DSL-Zugangskennung muss im Telefon 14 eingetragen werden, um vom Netzbetreiber eine IP-Adresse zugewiesen zu bekommen. Ebenso muss die VoIP-

Zugangskennung eingetragen werden, um die VoIP-Telefonnummer vom VoIP-Dienstanbieter zugewiesen zu bekommen. Netzbetreiber und Dienstanbieter können dabei dieselbe Organisation sein oder zwei getrennte.

Fig. 2 zeigt einen heutzutage gebräuchlicheren Netzaufbau an. Die DSL-Zugangskennung wird zentral im DSL-Router 7 (enthält das DSL-Modem) eingegeben, womit auch der Router 7 (Vermittlungsrechner 7) die IP-Adresse enthält. Kundenseitig können jetzt beliebig viele Geräte an den Router 7 angeschlossen werden und über diese eine vergebene IP-Adresse kommunizieren. In den Endgeräten ist jetzt keine Eintragung der Zugangskennung mehr notwendig. Im VoIP-Telefon 11 muss jetzt nur noch die VoIP-Zugangskennung eingetragen werden. Die Vergabe der internen IP-Adresse (192.168.x.x) kann automatisch durch den Router 7 über DHCP (Dynamisches Rechner-Konfigurations-Protocol) erfolgen oder manuell durchgeführt werden. Der Router 7 übernimmt automatisch die Umsetzung der IP-Adressen und Ports (NAPT - Netzwerkadress- und -schnittstellen / Adresskomponenten-Übersetzung, Network Address and Port Translation).

PPP könnte auch zur Diensttrennung bzw. Kundentrennung eingesetzt werden. Jedes Endgerät könnte seine eigene DSL-Zugangskennung besitzen und zur Kommunikation eine eigene IP-Adresse erhalten. Zudem könnte jeder Nutzer seine eigene DSL-Zugangskennung erhalten, die er jedes Mal im Gerät eingetragen oder aktivieren muss. Dies ist allerdings sehr umständlich und wird nicht genutzt. Zudem ist mit IPv4 (Internetprotokoll Version 4) der Adressvorrat gering, so dass es vermieden wird, für jeden Kunden und jedes Endgerät eine eigene Zugangskennung und damit eine eigene IP-Adresse zu vergeben.

Das PPP hat noch eine weitere wichtige Aufgabe: Die Sicherstellung, dass die Dienstleistung dem richtigen Kunden in Rechnung gestellt wird. Die Rechnung geht jeweils an den Eigner der Zugangskennung. Die Eingabe und Aktivierung der Zugangskennung führt zu einem PPP-Kanal, der eindeutig diesen logischen Kanal mit dem Eigner der Zugangskennung verbindet. Diese Trennung der Kundenanschlüsse erfolgt also in Bezug auf die Abrechnung durch den PPP-Kanal und nicht durch die Ethernet- oder IP-Adresse des Kunden, die Trennung des Datenverkehrs aber durch die IP-Adresse.

Zwischenzeitlich wird IPv4 durch das Internetprotokoll Version 6 (IPv6) abgelöst. In IPv6 steht ein wesentlich größerer Adressvorrat zur Verfügung, da die IPv6-Adresse aus 128 Bit besteht gegenüber 32 Bit der IPv4-Adressen und 48 Bit der MAC-Adressen (Media Access Control, auch LAN-Adresse, Ethernet-ID oder Airport-ID genannt). Für diese IPv6-Adressen wurden auch einige zusätzliche Managementfunktionen eingeführt, die einen zusätzlichen Nutzen bringen.

Fig. 3 zeigt nun das IPv6-Adressformat. In der oberen Zeile ist die Aufteilung der 128 Bit der IPv6-Adresse in zwei logische Segmente dargestellt. Die erste Hälfte der 128 Bit dienen zur Netzwerkidentifizierung (IPv6-Netzwerkadresse, IPv6 Network Address), während die letzten 64 Bit der Schnittstellenidentifizierung dienen (IPv6-Schnittstellenidentifizierer, IPv6 Interface Identifier). In der zweiten Zeile ist dargestellt, dass sich die 64 Bit der IPv6-Netzwerkadresse wiederum in einen 48 Bit langen vorangestellten Public Topology Prefix und einen 16 Bit Site Topology Prefix untergliedern. Der sog. Public Topology Prefix ist zusammengesetzt aus weiteren Elementen, nämlich 3

Bit eines Format Prefix (FP), 13 Bit eines Top-Level-Aggregation-Identifizierers (TLA ID), 8 reservierten Bit (beispielsweise für eine Top Level Aggregation (TLA) oder eine NLA-Erweiterung (NLA Extension). Weiterhin enthält das Public Topology Prefix 24 Bit eines Next-Level-Aggregation-Identifizierers (NLA ID).

Die letzten 64 Bit der IPv6-Netzwerkadresse setzen sich zusammen aus einem vorangestellten 16-Bit-Zusatz und der nachfolgenden MAC-Adresse der Schnittstelle mit 48 Bit.

Damit sind bei einer IPv6-Adresse die ersten 48 Bit durch die Netzwerkadresse und die letzten 48 Bit durch die MAC-Adresse der Schnittstelle gewöhnlich belegt.

Die Benutzer-Authentifizierung und damit die Grundlage für die Überprüfung, ob der Kunde diesen Dienst überhaupt nutzen darf, und die Abrechnung der Dienste (AAA - Authentication, Authorisation, Accounting) erfolgt bei einem Public Ethernet 2 mittels IEEE 802.1X-Protokoll.

Fig. 4 veranschaulicht die Abläufe bei der Authentifizierung. Der Benutzer identifiziert sich zunächst bei dem genutzten Gerät (z.B. PC 12, TV 13 oder Telefon 14), indem er z.B. eine PIN (Persönliche Identifizierungsnummer) einträgt oder seine Nutzerkennung aktiviert. Über IEEE 802.1X wird nun die Zugangskennung an das nächste Netzelement des Betreibers (z.B. den Authentifizierungsdienstrechner, DHCP-Dienstrechner 11) transferiert und über ein Authentifizierungsprotokoll in Verbindung mit dem RADIUS-Protkoll mittels eines Radiusservers 10 werden die AAA-Prozeduren durchgeführt. Auf diese Weise wird ge-

währleistet, dass der Benutzer des jeweiligen Gerätes auch die Rechnung für die Inanspruchnahme des Dienstes bekommt. Wichtig ist hierbei, dass eine sichere Kommunikation zwischen Kunden und Dienstanbieter 6 erfolgt.

Die IEEE 802.1X Schnittstellenauthentifizierung (Port Authentication) sorgt für diese sichere Kommunikation und stellt sicher, dass der Zugangsrouter 11 (Access Node, AN) exakt zuordnen kann, welcher Nutzer an einem bestimmten Port des AN 11 authentifiziert ist. Die AAA-Prozeduren sorgen zunächst aber nur dafür, dass der Kunde überhaupt Dienste nutzen kann und diese dann auch abgerechnet werden. Die eigentliche Datenkommunikation ist noch nicht möglich, da der Kunde noch keine globale IP(v6)-Adresse besitzt. Die Vergabe der IPv6-Adresse erfolgt nach erfolgreicher Authentifizierung.

Hier setzt nun die vorliegende Erfindung ein, die es sich zur Aufgabe macht, eine Nutzer- und/oder Dienstetrennung innerhalb des Netzes zu ermöglichen. Weiterhin ist es Aufgabe der vorliegenden Erfindung, für eine gesicherte Kommunikation zwischen Nutzer und Dienstbetreiber zu sorgen, so dass eine gesicherte Nutzer- und/oder Dienstetrennung ermöglicht wird. Diese Aufgabe wird durch die Verfahren nach Anspruch 1, 11 und 19 gelöst. Vorteilhafte Weiterbildungen der erfindungsgemäßen Verfahren werden in den jeweiligen abhängigen Ansprüchen gegeben.

Die vorliegende Erfindung setzt an der Stelle ein, bei der die Vergabe der IPv6-Adresse nach erfolgreicher Authentifizierung erfolgt. Zentraler Gedanke dabei ist, dass die einzelnen Felder und Bereiche der IPv6-Adresse flexibel gedeutet werden können.

Um eine gesicherte Kommunikation zwischen einem Nutzer und einem Dienstbetreiber/Diensteanbieter (Serviceprovider) zu gewährleisten, wird jetzt in einem Zugangsnetz für jede Paarung aus einem Zugangsknoten und einem Übergangsknoten in das Transportnetz/Internet eine Paarung von Bitmustern vergeben, die einen Teil des Topologiepräfixes einer IPv6-Adresse bildet. Hierdurch ist es möglich, dass jeweils ein Zugangsknoten (auch als Zugangsknotenrechner bezeichnet) bezüglich eines Nutzers mit einem spezifischen eindeutig zugeordneten Übergangsknoten kommuniziert. Es wird also bewirkt, dass ein Übergangsknoten (auch als Übergangsknotenrechner bezeichnet) Datenpakete von einem bestimmten Nutzer, die zu einem bestimmten Dienstbetreiber gesandt werden, lediglich über einen über die Paarung eindeutig identifizierten Übergangsknotenrechner zu dem Dienstbetreiber gesandt werden können. In gleicher Weise ist der Transport von Datenpaketen vom Dienstbetreiber zum Nutzergerät über einen eindeutigen Pfad gesichert. Dies bedeutet also, dass jedem Übergangsknotenrechner für jeden mit ihm verbundenen Zugangsknotenrechner eine eigene zugangsknotenrechnerspezifische IPv6-Adresse zugeordnet ist, die sich in dem vorgenannten Bitmuster für jeden der Zugangsknotenrechner unterscheidet. Dasselbe gilt für den Zugangsknotenrechner, der so viele IPv6-Adressen aufweist, wie er mit Übergangsknotenrechnern verbunden ist. Es wird also ein Verfahren zur Verfügung gestellt, zur Herstellung einer Verbindung eines Nutzergerätes mit mindestens einem mit einem Transportnetz verbundenen Rechner eines Diensteanbieters über ein Zugangsnetz mit mindestens einem Zugangsknotenrechner und über das Transportnetz mit mindestens einem Übergangsknotenrechner vom Zugangsnetz zum Transportnetz, wobei dem Nutzergerät

mindestens eine IPv6-Adresse zugeordnet wird, dadurch gekennzeichnet, dass jeder Paarung aus je einem Zugangsknotenrechner und je einem Übergangsknotenrechner ein eindeutiges Paar von Bitmustern zugeordnet wird, und für die jeweilige Paarung dem Zugangsknotenrechner und dem Übergangsknotenrechner jeweils ein Topologiepräfix der IPv6-Adresse zugeordnet wird, das jeweils eines der beiden Bitmuster des Paares von Bitmustern enthält. Es wird also bei der vorliegenden Erfindung die Eindeutigkeit der Zuordnung zwischen einem Knotenrechner und seiner IPv6-Adresse aufgehoben.

Das Bitmuster, mit dem jeweils eine Paarung unterschieden wird, kann eine unterschiedliche, den jeweiligen Netzanforderungen entsprechende Länge aufweisen. Es ist möglich, dass das Bitmuster nur wenige Bits oder auch sehr viele Bits aufweist. Vorteilhaft, jedoch nicht notwendig, ist ein Bitmuster, das eine Länge von 16 Bit aufweist. In diesem Falle ist es möglich, dieses Bitmuster als Site Topology Prefix in den ersten 64 Bits der IPv6-Adresse unterzubringen, so dass die Kombination von Public Topology Prefix und diesem Bitmuster eine 64 Bit lange Netzwerkadresse bilden. Das Bitmuster kann jedoch auch kürzer oder länger sein, wobei auf die Länge des Public Topology Prefix den jeweiligen Bedürfnissen im jeweiligen Netz angepasst werden können.

Um auch die jeweilige Nutzung und auch den jeweiligen Nutzer eindeutig zuzuordnen und Nutzer und/oder Dienste voneinander zu trennen, um anschließend beispielsweise eine nutzer- und dienstspezifische Abrechnung durchzuführen, kann weiterhin jedem Nutzer und/oder jedem genutzten Dienst ein eindeutiges Bitmuster zugeordnet werden. Dieses Bitmuster kann nun

ebenfalls bei der Zuweisung der IPv6-Adresse in die IPv6-Adresse eingebracht werden, so dass die IPv6-Adresse des Nutzergerätes zusätzlich den Nutzer als auch den genutzten Dienst oder auch nur eine dieser Komponenten codiert. Auch dieses Bitmuster kann unterschiedlich lang sein und an unterschiedlicher Position innerhalb der IPv6-Adresse untergebracht sein. Es ist jedoch besonders vorteilhaft, wenn für das Bitmuster zur Nutzer-/Dienstetrennung die ersten 16 Bit des IPv6-Schnittstellenidentifizierers verwendet werden. Diese 16 Bit können dann weiter aufgeteilt werden, beispielsweise jedoch nicht notwendigerweise in 8 Bit für die Nutzertrennung und 8 Bit für die Dienstetrennung. Dies würde ermöglichen, 256 Nutzer und 256 Dienste, d.h. insgesamt 65536 verschiedene Nutzer- und Dienstekombinationen eindeutig zu trennen. Dies erscheint aus heutiger Sicht als ausreichend. Es ist jedoch auch möglich, beispielsweise 10 Bit für die Nutzertrennung und 6 Bit für die Dienstetrennung zu verwenden oder auch für das Bitmuster zur Nutzer- und/oder Dienstetrennung mehr oder weniger als 16 Bit zu verwenden. Es wäre beispielsweise auch möglich, das Bitmuster für die Paarungsidentifizierung wie oben beschrieben und das Bitmuster für die Nutzer-/Gerätetrennung gemeinsam mit einer Länge von 32 Bit (es ist auch mehr oder weniger möglich) vorzusehen, wobei diese 32 Bit den Anforderungen des jeweiligen Netzwerks flexibel unter die einzelnen Bitmuster verteilt werden.

Es ist weiterhin möglich, in die IPv6-Adressen nicht zwingend in den letzten 48 Bit die MAC-Adresse aufzunehmen. Es wäre auch möglich, dort mit einem Bitmuster die Nutzer- und Gerätetrennung durchzuführen, so dass sich dann innerhalb des Netzwerks logische MAC-Adressen bilden, die mittels des entsprechenden Pro-

tokolls in die realen MAC-Adresse aufgelöst werden müssen.

Mit den beschriebenen erfindungsgemäßen Verfahren kann nun eine eindeutige Nutzer- und Dienstetrennung ausschließlich über die Vergabe der IPv6-Adressen erfolgen. Insbesondere ist es auch möglich, eine Dienstebindung (Service Bindung) durchzuführen, da der Nutzer auch andere Geräte oder an anderen Orten sein eigenes Gerät nutzen kann, ihm aber trotzdem immer eindeutig sein Nutzer- und Dienstprofil mittels der IPv6-Adresse bzw. der jeweiligen Bitmuster zugeordnet werden kann. Auch die Inrechnungstellung erfolgt immer zugeordnet, egal ob der Nutzer an anderen Geräten oder an anderen Orten mit seinem eigenen Gerät tätig ist. Das jeweilige Profil und die jeweilige Abrechnung wird dazu einfach an eine andere Adresse gebunden (Service Bindung). Weiterhin wird durch die Paarbildung der IPv6-Adressen zwischen dem Zugangsknotenrechnern und den Übergangsknotenrechnern eine sichere Kommunikation auf Ethernetebene erzielt, da die Datenverbindung nicht mehr durch Identitätsklau manipuliert werden können. Auch die Datenbehandlung wird auf Ethernetebene durch diese Paarbildung verbessert. Hierzu kann jeder Kombination von IPv6-Topologiepräfixen ein spezielles Ethernet-Label, z.B. VLAN Tag oder MPLS Label, zugeordnet werden und z.B. durch GVRP (generic VLAN registration protocol) oder GARP (generic attribute registration protocol) im Public Ethernet bekanntgemacht werden.

Die Zuordnung der IPv6-Adressen wie oben beschrieben, beispielsweise durch DHCPv6, kann dynamisch erfolgen und nur für die Dauer der jeweiligen Authentifizierung gültig sein. Es ist jedoch auch eine statische Zuordnung der Bitmuster möglich. Die Authentifizie-

rung des benutzten Gerätes bzw. Nutzers beim Dienstanbieter (Provider) in Kombination mit der eindeutigen Identifizierung des Benutzers am Gerät stellt also einen komfortablen Mechanismus zur Authentifizierung und damit zur Berechnung einer Dienstleistung bereit. Auf diese Weise fallen dann auch zusätzliche Authentifizierungsschritte, wie z.B. Eingabe der VoIP-Zugangskennung weg, da der Dienstanbieter bereits über die eindeutige IPv6-Adresse sowohl den Nutzer als auch den Dienst unterscheiden kann.

Einzig beim Wechsel des benutzten Gerätes muss die VoIP-Zugangskennung neu eingegeben werden, wenn beispielsweise ein Nutzer ein fremdes VoIP-Telefon, z.B. des Nachbarn, nutzen möchte, wobei das Gespräch jedoch auf Rechnung des konkreten Nutzers gehen soll. Hier muss der Nutzer dem jeweiligen Dienstanbieter mitteilen, dass mit der IPv6-Adresse des Nachbarn temporär mit dem VoIP-Count des Nutzers zu assoziieren ist.

Im folgenden werden einige Beispiele eines erfindungsgemäßen Verfahrens gegeben. In dieser Beschreibung zeigen

Fig. 1 die Netzanbindung eines Endgerätes an einen Dienstanbieter nach dem Stand der Technik;

Fig. 2 eine Netzanbindung mehrerer Endgeräte an einen Dienstanbieter nach dem Stand der Technik;

Fig. 3 das Format einer IPv6-Adresse;

Fig. 4 ein Netzwerk eines Public Ethernet mit

dem Mechanismus der Benutzerauthentifizierung;

Fig. 5 die Authentifizierung nach der vorliegenden Erfindung;

Fig. 6 ein Public Ethernet mit Darstellung der Vergabe der IPv6-Adressen; und

Fig. 7 Beispiele für Paarungen von IPv6-Präfixen für Zugangsknotenrechner (Access Node) und Übergangsknotenrechner (Edge Node).

In allen Figuren wurden für gleiche oder ähnliche Elemente gleiche oder ähnliche Bezugszeichen verwendet.

Figur 5 zeigt das Authentifizierungsverfahren in einem Public Ethernet, wie es beispielsweise in Figur 4 oder Figur 6 dargestellt ist für die einzelnen Netzelemente und Kunden.

Das Kundennetzelement (Supplicant) startet eine IEEE 802.1X-Authentifizierung mit einem Zugangsknotenrechner (802.1X-Authentikator, AN). Der AN wiederum nimmt Kontakt mit einem Authentifizierungsdienstrechner (Radius-Server) 10 auf. Dieser Authentifizierungsdienstrechner 10 hat Zugriff auf eine Kundendatenbank, in der neben den Kontaktdaten (Authenticate) des Kunden auch die Tarifierungs- und Dienstinformationen gespeichert sind. Diese bezeichnen u.a. die einem Kunden zugänglichen Dienste und die vereinbarten Dienstprofile und die dazugehörigen Tarifinformationen. Die eigentliche Authentifizierung zwischen dem Supplicant (beispielsweise PC 12) und dem Authentifizierungsdienstrechner 10 läuft dann

über das Extensible Authentication Protocol (EAP) sowie eine wählbare Authentifizierungsmethode. Diese Authentifizierungsmethode ist es, die für die die Verschlüsselung der Information bei der Authentifizierung sorgt. Sie ermöglicht auch, die zugeordnete IPv6-Adresse dieses Kunden zu speichern und zu reservieren, so dass die Adresse immer wieder verwendet werden kann. So ist neben einer dynamischen IPv6-Adressvergabe auch eine statische IPv6-Adressvergabe zu realisieren.

Je nachdem welches Gerät bzw. welcher Nutzer sich authentifizieren will, wird der Zugangsknotenrechner AN 11 einen anderen Authentifizierungsdienstrechner 10 kontaktieren. Die Auswahl des richtigen Authentifizierungsdientsrechners (Authentifizierungsservers) kann entweder über die Kontaktdaten des gewünschten Dienstanbieters erfolgen, beispielsweise SIP.Anbietername.de, oder auch über dessen IPv6-Adresse. Eine weitere Möglichkeit besteht in der Auswertung der Herkunftsadresse (Source Address) des dienstanfordernden Nutzers.

Die Authentifizierung kann auch wie sonst in zwei Schritten erfolgen, einmal beim Internetdienstanbieter (Internet Service Provider) und zum anderen beim gewünschten Dienstanbieter selbst. Die Authentifizierung sorgt in jedem Fall für die Assoziierung des authentisierten Ports/Schnittstelle mit einem Nutzer. Danach erfolgen separat die Vergabe der IPv6-Adresse und die Authentisierung des Dienstes und Nutzers mit der IPv6-Adresse bzw. Teilen hiervon.

Figur 6 zeigt nun ein Public Ethernet 2, das mit verschiedenen Internet-Netzwerk-Dienstanbietern (Internet Network Service Provider, NSP) 4, 4' verbunden

ist. Die NSPs 4, 4' haben unterschiedliche, weltweit eindeutige IPv6-Public-Topology-Präfixe. In diesem Beispiel hat jeder Übergangsknotenrechner (Edge Node Router, EN, nach heutigem Stand auch BRAS) 3a, 3b einen 48 Bit-Präfix. Es ist jedoch auch möglich, dass die Anzahl der Bits für die Public Topology Präfixe für die einzelnen logischen Segmente in der hierarchischen IP-Adressvergabe geändert werden kann. Die benötigte Anzahl wird von der benötigen Anzahl verschiedener Netzelemente im jeweiligen Netz bestimmt und lässt sich folglich bei der Netzplanung individuell anpassen. So kann beispielsweise das Präfix des Übergangsknotenrechners auch nur 46 Bit lang sein, womit weniger Übergangsknotenrechner angeschlossen werden können, allerdings im selben Netz viermal so viele Zugangsknotenrechner (Access Nodes, AN, 8a, 11).

Im Folgenden wird nun die Adressvergabe für den Netzwerkserviceprovider 4 dargestellt. Für den Netzwerkserviceprovider 4' des Netzwerks 1' erfolgt die Adressvergabe entsprechend.

Dabei ist zu beachten, dass für sämtliche Netzwerkelemente des Public Ethernet 2 sowohl von dem Netzwerkserviceprovider 4 als auch von dem Netzwerkserviceprovider 4' des Netzwerks 1' parallel Adressen vergeben werden, so dass ein Netzelement hier immer zwei Adress-Präfixe besitzt, von jedem der Netzwerkserviceprovider je eines.

Bei der vorliegenden Erfindung vergibt nun der Übergangsknotenrechner EN 3a (der Übergangsknotenrechner EN 3b handelt entsprechend) per IPv6-Adressdelegation für jeden im Netzwerk 2 angeschlossenen Zugangsknotenrechner AN 8a, 11 ein individuelles IPv6 64 Bit-

Präfixpaar. Jedes Präfix eines derartigen Paares besteht aus einem 48 Bit Public Topology Prefix sowie einem selbstverwalteten Site Topology Prefix. Das 48 Bit lange Public Topology Prefix ist für jeden Übergangsknotenrechner EN 3a, 3b, 3a' weltweit eindeutig. Damit sind auch die 64 Bit-Präfixe für die mit einem bestimmten Übergangsknotenrechner verbundenen Zugangsknotenrechner 8a, 11 ebenfalls eindeutig, da die 16 Bit Site Topology von jedem Übergangsknotenrechner jeweils nur einem Zugangsknotenrechner zugewiesen wird. Jeder Übergangsknotenrechner vergibt also eine Paarung von Site-Topology-Präfixen nur einmal, wobei der eine Präfix dem Zugangsknotenrechner und der andere Präfix dem Übergangsknotenrechner zugeordnet wird.

Figur 7 zeigt Paarungen von Topology-Präfixen mit einer Länge von 64 Bit für drei Zugangsknotenrechner AN 1, AN 2, AN 3 (diese können beispielsweise mit dem Zugangsknotenrechner 8a, 11 etc. in Figur 6 gleichgesetzt werden). Für jeden der Zugangsknotenrechner AN 1, AN 2, AN 3 ist eine Paarung von Site-Topology-Präfixen mit 16 Bit Länge zugeordnet, beispielsweise für den Zugangsknotenrechner AN 1 die Paarung 0027 mit 0028, für den Zugangsknotenrechner 2 die Paarung 0044 mit 0045 und für den Zugangsknotenrechner 3 die Paarung 0063 mit 0064. Zusammen mit dem Public-Topology-Präfix des Übergangsknotenrechners 2 (2005:7BA9:3453) ergibt sich nun der Topology-Präfix für den Zugangsknotenrechner AN 1 und den entsprechenden Übergangsknotenrechner so wie in der ersten Zeile der Figur 7 angegeben. Damit besteht eine eindeutige Zuordnung zwischen dem Zugangsknotenrechner 1 und dem zugehörigen Übergangsknotenrechner, der diese Site-Topology-Präfixe vergeben hat. In Figur 7 kann der Übergangsknotenrechner in der dritten Spalte der

Tabelle immer derselbe sein, der für die jeweilige Paarung mit einem Zugangsknotenrechner AN 1, AN 2, AN 3 folglich jeweils eine eigene definierte IPv6-Adresse erhält.

Da jeder Übergangsknotenrechner 3a, 3b, 3a' für jeden im Netz 2 befindlichen Zugangsknotenrechner 8a, 11 eine solche Paarung vergibt, wird das Netz in eine Vielzahl von eindeutigen Zweierbeziehungen zwischen Zugangsknotenrechnern und Übergangsknotenrechnern aufgelöst bzw. hierdurch definiert.

Von einem bestimmten EN erhalten die verschiedenen ANs im Public Ethernet 2 also je einen eigenen 64 Bit Access Node Prefix (siehe Tabelle). Gleichzeitig wird als Next Hop (in der Routing Tabelle) der 64 Bit Edge Node Prefix eingetragen. Diesen muss sich das Edge Node ebenfalls merken und für diesen Prefix nur Pakete akzeptieren, die vom Access Node mit dem korrespondierenden 64 Bit Access Node Prefix kommen. Die IPv6-Adressen sind zwar nicht direkt in den Datenpaketen zwischen AN und EN enthalten, aber sie sind indirekt in den MAC-Adressen enthalten. Dadurch, dass Ethernet die beiden Netzelemente verbindet, müssen aufgrund der Next Hop Einträge in den Routing-Tabellen von AN und EN die Next Hop IPv6-Adressen mittels ARP (Adressenauflösungsprotokoll, Address Resolution Protocol) aufgelöst werden. Damit sind die IPv6 Access / Edge Node Prefix Paare indirekt in den MAC-Source/Destination-Adressen enthalten. Die Netzelemente können zu diesem Zweck sich selbst logische MAC-Adressen für die verschiedenen IPv6-Adressen vergeben. Mittels dieser speziellen Adress-Vergabe ist die Kommunikation zwischen einem AN und einem EN damit eindeutig.

Die einzelnen Kundenanschlüsse, die an das AN angeschlossen sind, können über DHCPv6 voneinander eindeutig getrennt werden. Die Kundentrennung erfolgt über die Schnittstellen/Geräteauthentifizierung und dam darüber liegenden Authentifizierungsprotokoll. IEEE 802.1X bildet dabei nur den Kommunikationsmechanismus zwischen Kundengerät und AN. Das Authentifizierungsprotokoll sorgt dann dafür, dass der Dienst dem richtigen Kunden in Rechnung gestellt wird. ES gibt im Stand der Technik eine Vielzahl von Authentifizierungsprotokollen, die hier nicht weiter erläutert werden müssen. Je nach eingesetztem Protokoll wird die Nutzertrennung aber sehr einfach, komfortabel und sicher durchgeführt. Als Beispiel sei hier nur genannt, dass die Nutzer-Authentifizierung z.B. über das Benutzer-Login bei einem Mehrbenutzer-Betriebssystem (z.B. Windows XP) durchgeführt werden kann. Je nachdem, welcher Benutzer sich beim Betriebssystem anmeldet, wird über dieses Verfahren auch ein anderer Nutzer beim Dienstanbieter authentifiziert. Dieser Nutzer erhält dann auch die Rechnung für den Dienst. Ein Kunde authentifiziert sich mit seinem Gerät eindeutig beim AN mittels IEEE 802.1X Port Authentication. Mit dieser Authentifizierung wird auch automatisch dem Kunden ein 64 Bit Address Prefix zugeordnet. Danach wird per DHCPv6 die IPv6-Adresse vergeben. Die komplettierte IPv6-Adresse besteht aus dem 64 Bit Access Node Prefix des AN, an dem der Kundenanschluss realisiert ist, sowie einer 64 Bit Interface ID (IID), die aus der MAC-Adresse des Ports und einem 16 Bit Zusatz besteht.

Der Dienst, der in Anspruch genommen wird, kann ebenfalls über die IPv6-Adresse getrennt werden. Dazu kann der unveränderliche 16 Bit Zusatz im IDD-Feld genutzt werden, um die Dienste und ggf. auch ver-

schiedenen Nutzer eines Gerätes eindeutig zu trennen. Mit einem Gerät kann man 65536 verschiedene Nutzer- und Dienstekombinationen eindeutig trennen, was aus heutiger Sicht mehr als genug sein sollte. Wenn man 256 verschiedene Dienste nutzen würde, so könnten dieses Gerät 256 verschiedene Benutzer benutzen. Die Dienst- und Nutzertrennung könnte somit ausschließlich über die vergebene Adresse geprüft, authentifiziert und abgerechnet werden.

Um beispielsweise 256 verschiedene Benutzer, die jeweils 256 verschiedene Dienste nutzen, voneinander trennen zu können, werden als Bitmuster die Bits 65-72 der IPv6-Adresse verwendet, um die Nutzer zu trennen und als Bitmuster die Bits 73-80 zu verwenden, um deren Dienste zu trennen. Als Bits 81 - 128 werden die MAC-Adress-Bits des Computers eingesetzt. Im AN wird bei der Authentifizierung gleichzeitig der Bitbereich für den authentifizierten Benutzer fixiert und speziell überwacht.

Logt sich beispielsweise 149 im Betriebssystem ein, akzeptiert der AN nur noch diejenigen IP-Pakete von diesem Port, die im Bitbereich 65-72 den Wert 149 haben. Von diesem Gerät kann jetzt nur noch mittels 256 verschiedenen IPv6-Adressen als Source-Adresse kommuniziert werden, die zur Dienstetrennung genutzt werden können. Somit kann z.B. die VoIP-Zugangskennung entfallen, da diese IP-Adresse einem Kunden und der Nutzung von VoIP eindeutig zugeordnet ist. Würde ein anderer Nutzer, z.B. mit dem Bitmuster 173, eingeloggt und damit authentifiziert und würde er die IPv6-Adresse für VoIP vom Benutzer 149 nutzen, so würde jedes Paket mit dieser IPv6-Source-Adresse geblockt werden, da das AN einen anderen IPv6-Bereich der Bits 65-72 erwartet, nämlich 173, und diese daher

als ungültig erkennt und verwirft. Die Aufteilung der 16 Bits in der IID ist wiederum flexibel einstellbar, man kann jede beliebige Nutzer-/Dienstekombination einstellen, sofern das Produkt aus Nutzer*Dienste pro Nutzer kleiner als 65536 bleibt. Bei Verwendung einer größeren oder kleineren Anzahl von Bits der IPv6-Adresse zur Nutzer-/Dienstetrennung können nahezu beliebige Anzahlen von Nutzern und/oder Diensten voneinander getrennt werden.

Bei diesem Verfahren authentifiziert sich jedes Gerät im Kundennetz beim AN mittels IEEE 802.1X. Zu diesem Zweck muss das Home Gateway (Gateway = Protokollumsetzer) eine 802.1X Weiterleitungsfunktion besitzen (802.1X Relay). Eine andere Möglichkeit besteht in der zentralen Authentifizierung durch das Home Gateway. Dann müssen sich die Geräte im Kundennetz jeweils beim Home Gateway authentifizieren. Dazu muss das Home Gateway eine 802.1X Proxy Server Funktion besitzen. Die Vergabe der Nutzungsrechte durch das Home Gateway könnte auch durch ein UBICOM-Verfahren erfolgen.

Im Fall, dass der Kunde den Computer mitnimmt (z.B. zum Nachbarn) und den dortigen Netzzugang nutzt, wird auch die Authentifizierung problemlos ablaufen, da der 64 Bit Prefix unverändert bleibt, da beide Netzzugänge (wahrscheinlich) am selben AN angeschlossen snid.

Wäre der Nachbar an einem anderen AN angeschlossen, würde sich die 16 Bit Site Topology der IPv6-Adresse ändern. Der Nutzer kann sich mit seinem Computer dennoch authentifizieren, da diese Prozedur über ein gesichertes Protokoll abläuft. Der Authentication Server kann bei erfolgreicher Authentifizierung die ur-

sprüngliche 16 Bit Site Topology mit dem Nutzer und seinem Dienstprofil temporär assoziieren. Das Profil wird also temporär an eine andere Adresse gebunden (Service Binding).

Einzig beim Benutzen eines anderen Gerätes muss also der Nutzer eine separate Zugangskennung eingeben, um sich mit einer anderen IPv6-Adresse temporär zu assoziieren.

Es ist wesentlich bei der vorliegenden Erfindung, dass die Bitmuster, die zur Identifizierung der Paarungen aus Übergangsknotenrechner und Zugangsknotenrechner verwendet werden und auch die Bitmuster, die zur Dienste- und/oder Nutzertrennung verwendet werden in ihrer Länge und auch in ihrer Positionierung innerhalb der IPv6-Adresse nicht festgelegt sind. Entscheidend ist hier, dass in Abhängigkeit von der Netzstruktur und den Bedürfnissen der jeweiligen Netzbetreiber die einzelnen Positionen der IPv6-Adresse flexibel interpretiert werden können. So ist beispielsweise auch eine Aufteilung möglich, bei der die innerhalb der IPv6-Adressen der Public Topology Prefix eine Länge von 40 Bit aufweist, der Site Topology Prefix 21 Bit, die Bitmuster zur Nutzertrennung und zur Dienstetrennung zusammen 19 Bit und sich daran die 48 Bit Ethernet-MAC-Adresse anschließt. Eine Trennung in 48 Bit Public Topology Prefix, 26 Bit Site Topology Prefix, 6 Bit für eines oder beide Bitmuster zur Nutzer- und/oder Dienstetrennung und anschließend 48 Bit Ethernet-MAC-Adresse sind ebenfalls möglich. Die Bits, die für die Bitmuster der Nutzer- und Dienstetrennung verwendet werden, können unter den beiden Bitmustern für die Dienste- und Nutzertrennung völlig flexibel aufgeteilt sein.

Durch die erfindungsgemäße Zuordnung von Bitmustern wird also eine hohe Flexibilität erreicht und dem Netzwerkarchitekten die Möglichkeit an die Hand gegeben, die spezifischen Gegebenheiten des jeweiligen Netzwerks bei der Aufteilung der IPv6-Adressbits auf die verschiedenen Bereiche zu berücksichtigen.

Patentansprüche

1. Verfahren zur Herstellung einer Verbindung eines Nutzergerätes mit mindestens einem mit einem Transportnetz verbundenen Rechner eines Diensteanbieters über ein Zugangsnetz mit mindestens einem Zugangsknotenrechner und über das Transportnetz mit mindestens einem Übergangsknotenrechner vom Zugangsnetz zum Transportnetz, wobei dem Nutzergerät mindestens eine IPv6-Adresse zugeordnet wird,
d a d u r c h g e k e n n z e i c h n e t ,
dass jeder Paarung aus je einem Zugangsknotenrechner und je einem Übergangsknotenrechner ein eindeutiges Paar von Bitmustern zugeordnet wird, und für die jeweilige Paarung dem Zugangsknotenrechner und dem Übergangsknotenrechner jeweils ein Topologiepräfix einer IPv6-Adresse zugeordnet wird, das jeweils eines der beiden Bitmuster des Paares von Bitmustern enthält.

2. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das Bitmuster höchstens oder genau 16 Bit lang ist.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die IPv6-Adresse als erste 64 Bit einen netzspezifischen Topologiepräfix, der sich aus 48 Bit eines für jedes Netzwerk spezifischen Public Topology-Präfix und 16 Bit eines Site Topology-Präfix zusammensetzt, und als letzte 64 Bit einen gerätspezifischen Schnittstellen-Identifizierer, der als letzte 48 Bit die MAC-Adresse der Schnittstelle enthält, aufweist.

4. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das Topologiepräfix das Bitmuster als Bit Nr. 49 bis Bit Nr. 64 des Site Topologie-Präfix der IPv6-Adresse enthält.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass jedem Zugangsknotenrechner und/oder jedem Übergangsknotenrechner für jedes der zugeordneten Topologiepräfixe eine IPv6-Adresse zugeordnet wird.

6. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass jeder Kombination von IPv6-Topologiepräfixen ein spezielles Ethernetlabel zugeordnet wird und im Public Ethernet bekanntgemacht wird.

7. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, dass mindestens einem oder jedem Zugangsknotenrechner und/oder mindestens einem oder jedem Übergangsknotenrechner für jede seiner IPv6-Adressen eine eigene MAC-Adresse zugeordnet wird.

8. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, dass mindestens einem oder jedem Zugangsknotenrechner und/oder mindestens einem oder jedem Übergangsknotenrechner für jede seiner IPv6-Adressen in den letzten 48 Bit der IPv6-Adresse ein von seinen anderen IPv6-Adressen verschiedenes Bitmuster zugeordnet wird (logische MAC-Adresse).

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass dem Nutzergerät seine IPv6-Adresse(n) nach Authentifizierung des Nutzers statisch und/oder dynamisch zugeordnet wird.

10. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die zugeordnete IPv6-Adresse(n) des Nutzergeräts nur für die Dauer der Authentifizierung gültig ist/sind.

11. Verfahren zur Herstellung einer Verbindung eines Nutzergerätes mit mindestens einem mit einem Transportnetz verbundenen Rechner eines Diensteanbieters über ein Zugangsnetz mit mindestens einem Zugangsknotenrechner und über das Transportnetz mit mindestens einem Übergangsknotenrechner vom Zugangsnetz zum Transportnetz, wobei dem Nutzergerät eine IPv6-Adresse zugeordnet wird,
d a d u r c h g e k e n n z e i c h n e t,
dass jedem Nutzer und/oder jedem genutzten Dienst jeweils ein eindeutiges Bitmuster zugeordnet wird, und dem Nutzergerät jeweils ein Interface-Identifizierer der IPv6-Adresse zugeordnet wird, der dieses Bitmuster enthält.

12. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das Bitmuster höchstens oder genau 16 Bit lang ist.

13. Verfahren nach einem der beiden vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Bitmuster ein erstes Teilbitmuster, das dem Nutzer zugeordnet ist, und/oder ein zweites Teilbitmuster, das dem genutzten Dienst zugeordnet ist, aufweist.

14. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass je ein erstes und ein zweites Teilbitmuster vorgesehen sind, wobei beide Teilbitmuster zusammen höchstens oder genau 16 Bit lang sind.

15. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das erste und/oder zweite Teilbitmuster höchstens oder genau 8 Bit lang sind.

16. Verfahren nach einem der Ansprüche 10 bis 14, dadurch gekennzeichnet, dass das Bitmuster Bestandteil der ersten 16 Bit des Interface-Identifizierers der IPv6-Adresse des Nutzergerätes ist.

17. Verfahren nach einem der Ansprüche 10 bis 15, dadurch gekennzeichnet, dass dem Nutzergerät seine IPv6-Adresse(n) nach Authentifizierung des Nutzers statisch und/oder dynamisch zugeordnet wird.

18. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die zugeordnete IPv6-Adresse(n) des Nutzergeräts nur für die Dauer der Authentifizierung gültig ist.

19. Verfahren zur Herstellung einer Verbindung eines Nutzergerätes mit mindestens einem mit einem Transportnetz verbundenen Rechner eines Diensteanbieters über ein Zugangsnetz mit mindestens einem Zugangsknotenrechner und über das Transportnetz mit mindestens einem Übergangsknotenrechner vom Zugangsnetz zum Transportnetz, wobei dem Nutzergerät eine IPv6-Adresse zugeordnet wird,
dadurch gekennzeichnet,
dass jeder Paarung aus je einem Zugangsknotenrechner und je einem Übergangsknotenrechner ein eindeutiges Paar von ersten Bitmustern zugeordnet wird,
für die jeweilige Paarung dem Zugangsknotenrech-

ner und dem Übergangsknotenrechner jeweils ein Topologiepräfix der IPv6-Adresse zugeordnet wird, das jeweils eines der beiden ersten Bitmuster des Paares von ersten Bitmustern enthält, und

dass jedem Nutzer und/oder jedem genutzten Dienst jeweils ein zweites eindeutiges Bitmuster zugeordnet wird, und dem Nutzergerät jeweils ein Interface-Identifizierer der IPv6-Adresse zugeordnet wird, der dieses zweite Bitmuster enthält

wobei sich die IPv6-Adresse des Nutzergerätes zusammensetzt aus dem Topologie-Präfix des mit dem Nutzergerät verbundenen Zugangsknotenrechners und dem dem Nutzergerät zugeordneten Interface-Identifizierer.

20. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass mindestens eines der ersten und/oder zweiten Bitmuster höchstens oder genau 16 Bit lang ist.

21. Verfahren nach einem der beiden vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die IPv6-Adresse als erste 64 Bit einen netzspezifischen Topologiepräfix, der sich aus 48 Bit eines für jedes Netzwerk spezifischen Public Topology-Präfix und 16 Bit eines Site Topology-Präfix zusammensetzt, und als letzte 64 Bit einen gerätspezifischen Schnittstellen-Identifizierer, der als letzte 48 Bit die MAC-Adresse der Schnittstelle enthält, aufweist.

22. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das Topologiepräfix das erste Bitmuster des Bitmusterpaares als Bit Nr. 49 bis Bit Nr. 64 des Site Topologie-Präfix der IPv6-Adresse enthält.

23. Verfahren nach einem der Ansprüche 19 bis 22, dadurch gekennzeichnet, dass das zweite Bitmuster ein erstes Teilbitmuster, das dem Nutzer zugeordnet ist, und/oder ein zweites Teilbitmuster, das dem genutzten Dienst zugeordnet ist, aufweist.

24. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass je ein erstes und ein zweites Teilbitmuster vorgesehen sind, wobei beide Teilbitmuster zusammen höchstens oder genau 16 Bit lang sind.

25. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das erste und/oder zweite Teilbitmuster höchstens oder genau 8 Bit lang sind.

26. Verfahren nach einem der Ansprüche 19 bis 25, dadurch gekennzeichnet, dass das zweite Bitmuster Bestandteil der ersten 16 Bit des Interface-Identifizierers der IPv6-Adresse des Nutzergerätes ist.

27. Verfahren nach einem der Ansprüche 18 bis 25, dadurch gekennzeichnet, dass jedem Zugangsknotenrechner und/oder jedem Übergangsknotenrechner für jedes der zugeordneten Topologiepräfixe eine IPv6-Adresse zugeordnet wird.

28. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass jeder Kombination von IPv6-Topologiepräfixen ein spezielles Ethernetlabel zugeordnet wird und im Public Ethernet bekanntgemacht wird.

29. Verfahren nach Anspruch 27 oder 28, dadurch gekennzeichnet, dass mindestens einem oder jedem

Zugangsknotenrechner und/oder mindestens einem oder jedem Übergangsknotenrechner für jede seiner IPv6-Adressen eine eigene MAC-Adresse zugeordnet wird.

30. Verfahren nach Anspruch 27 oder 28, dadurch gekennzeichnet, dass mindestens einem oder jedem Zugangsknotenrechner und/oder mindestens einem oder jedem Übergangsknotenrechner für jede seiner IPv6-Adressen in den letzten 48 Bit der IPv6-Adresse ein von seinen anderen IPv6-Adressen verschiedenes Bitmuster zugeordnet wird (logische MAC-Adresse).

31. Verfahren nach einem der Ansprüche 19 bis 30, dadurch gekennzeichnet, dass dem Nutzergeräte seine IPv6-Adresse(n) nach Authentifizierung des Nutzers statisch und/oder dynamisch zugeordnet wird.

32. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die zugeordnete IPv6-Adresse(n) des Nutzergeräts nur für die Dauer der Authentifizierung gültig ist/sind.

FIG. 1

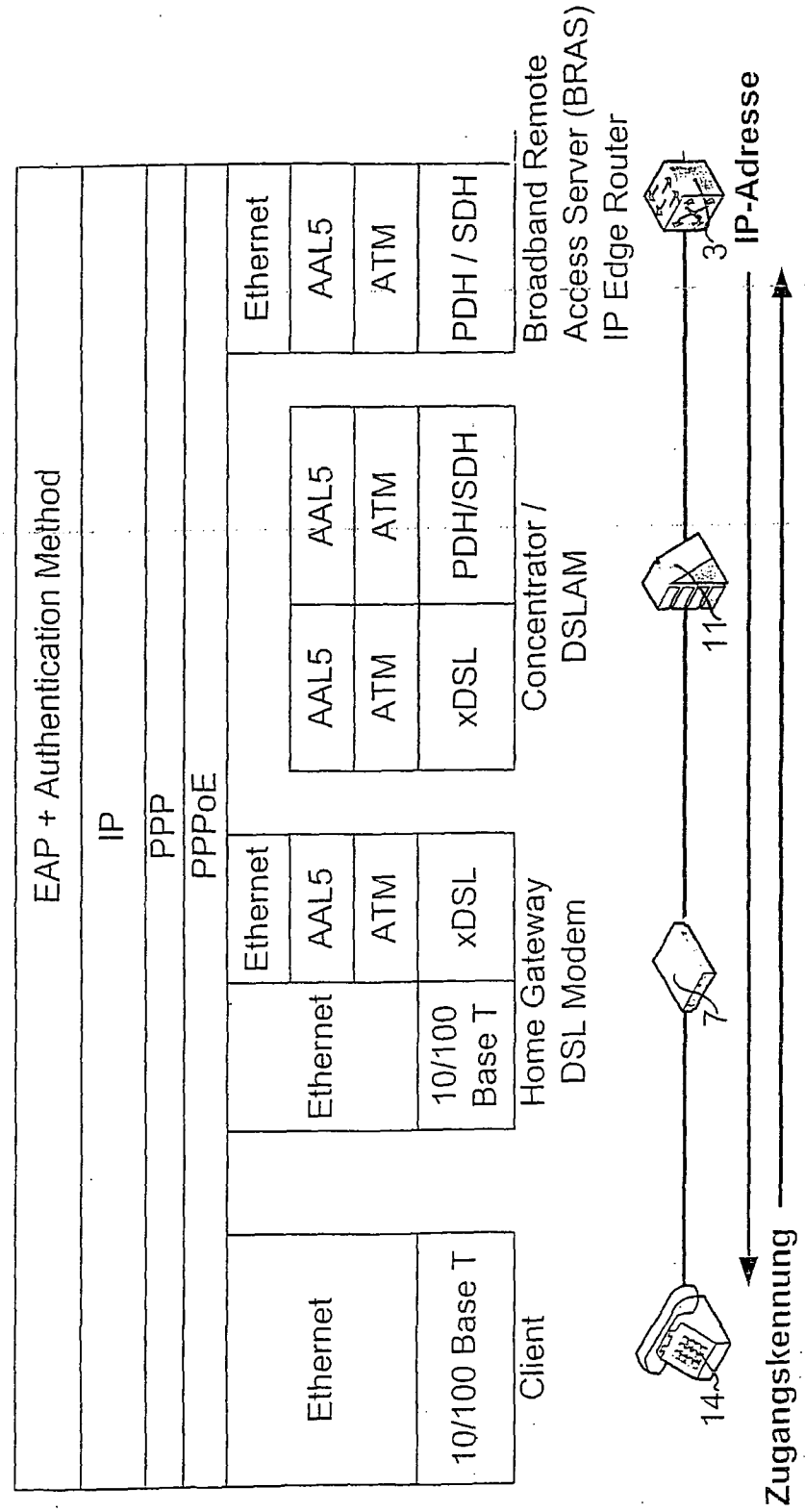
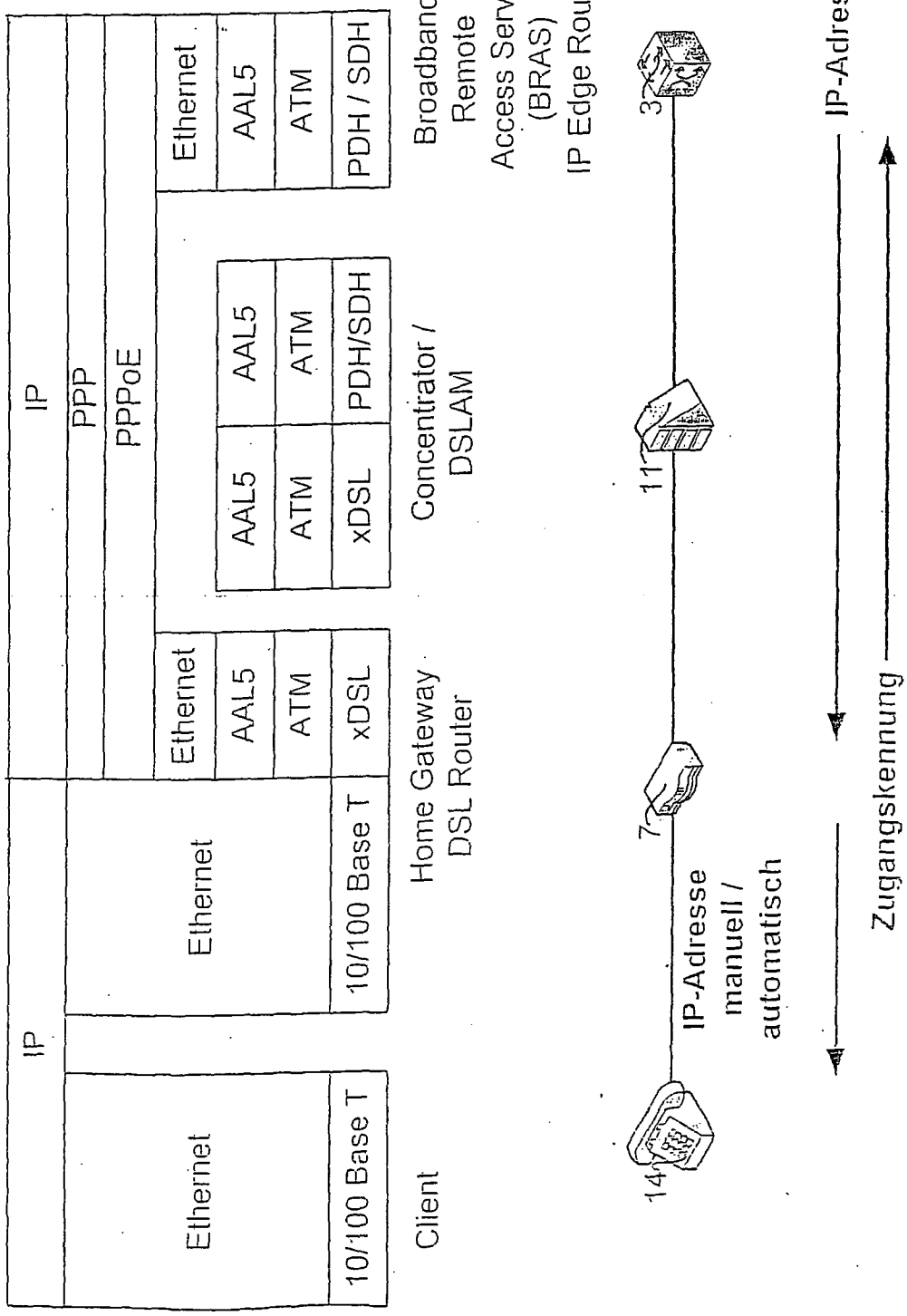

Client talks to BRAS using PPP / PPPoE
EAP + Authentication Method
IP
PPP
PPPoE
Ethernet
10/100 Base T
Client
Ethernet
AAL5
ATM
Ethernet
10/100 Base T
xDSL
Home Gateway
DSL Modem
AAL5
ATM
xDSL
AAL5
ATM
PDH/SDH
Concentrator /
DSLAM
Ethernet
AAL5
ATM
PDH / SDH
Broadband Remote
Access Server (BRAS)
IP Edge Router
IP-Adresse
Zugangskennung
14
7
11
3

FIG. 2

DSL Router talks to BRAS using PPP / PPPoE



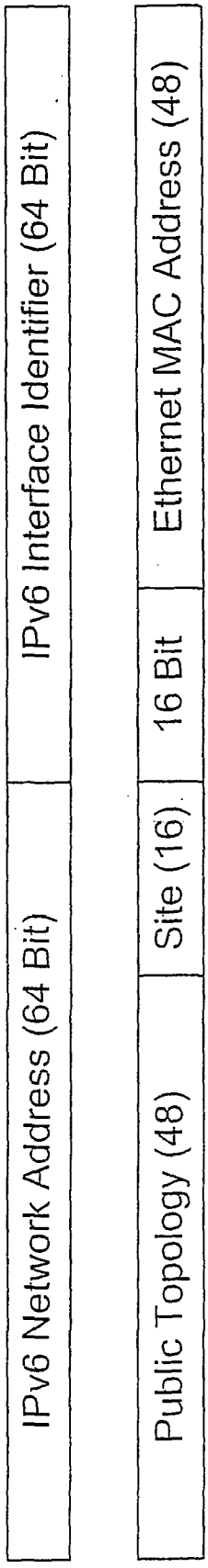

IPv6 Network Address (64 Bit)
IPv6 Interface Identifier (64 Bit)
Public Topology (48)
Site (16)
16 Bit
Ethernet MAC Address (48)

FIG. 3

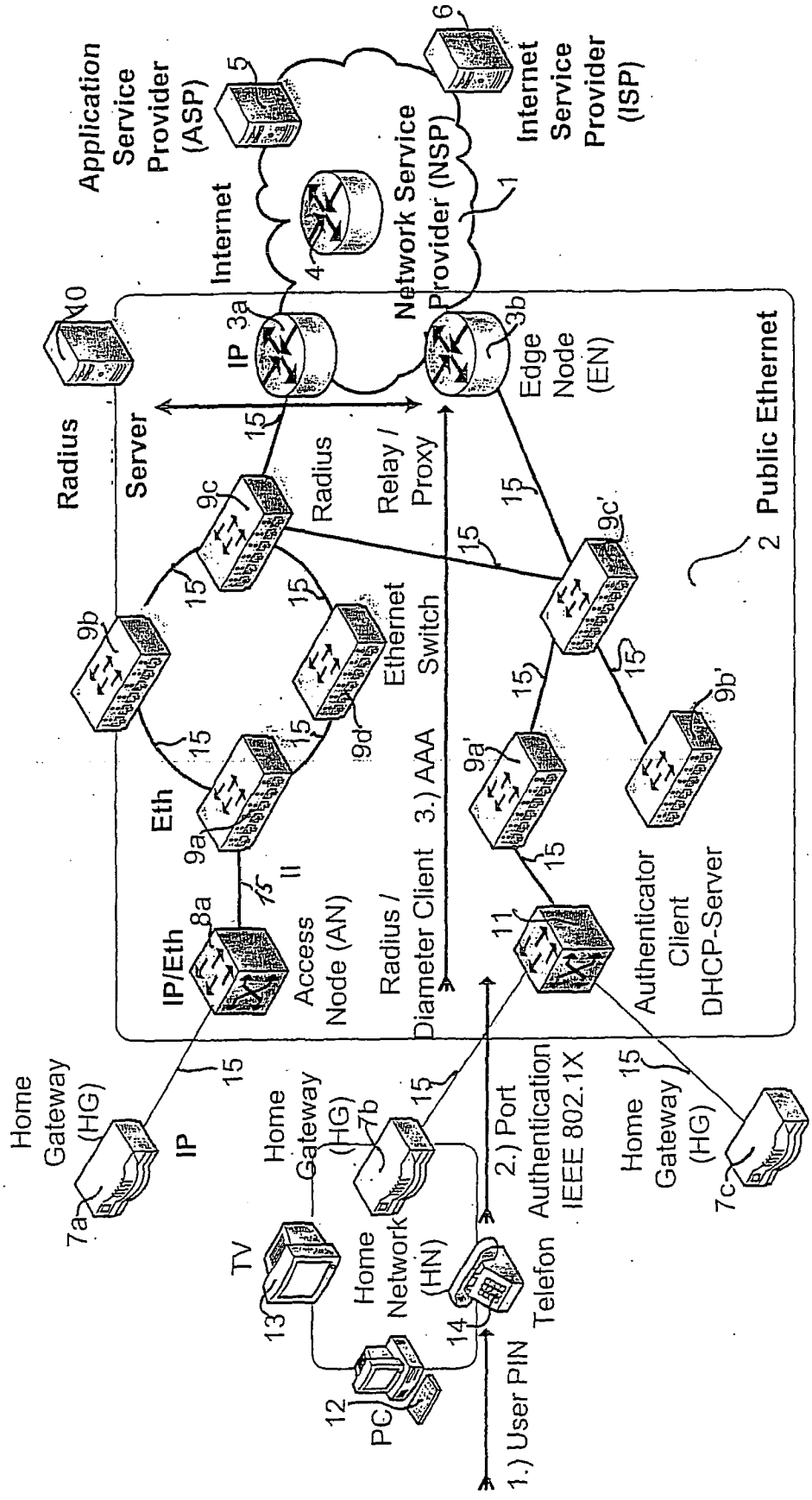

Application Service Provider (ASP)
Internet
Network Service Provider (NSP)
Internet Service Provider (ISP)
Radius Server
IP
Edge Node (EN)
Relay / Proxy
Radius
Ethernet Switch
Eth
IP/Eth
Access Node (AN)
Radius / Diameter Client
3.) AAA
Authenticator Client DHCP-Server
2 Public Ethernet
Home Gateway (HG)
IP
2.) Port Authentication IEEE 802.1X
1.) User PIN
Telefon
TV
PC
Home Network (HN)

FIG. 4

FIG. 5

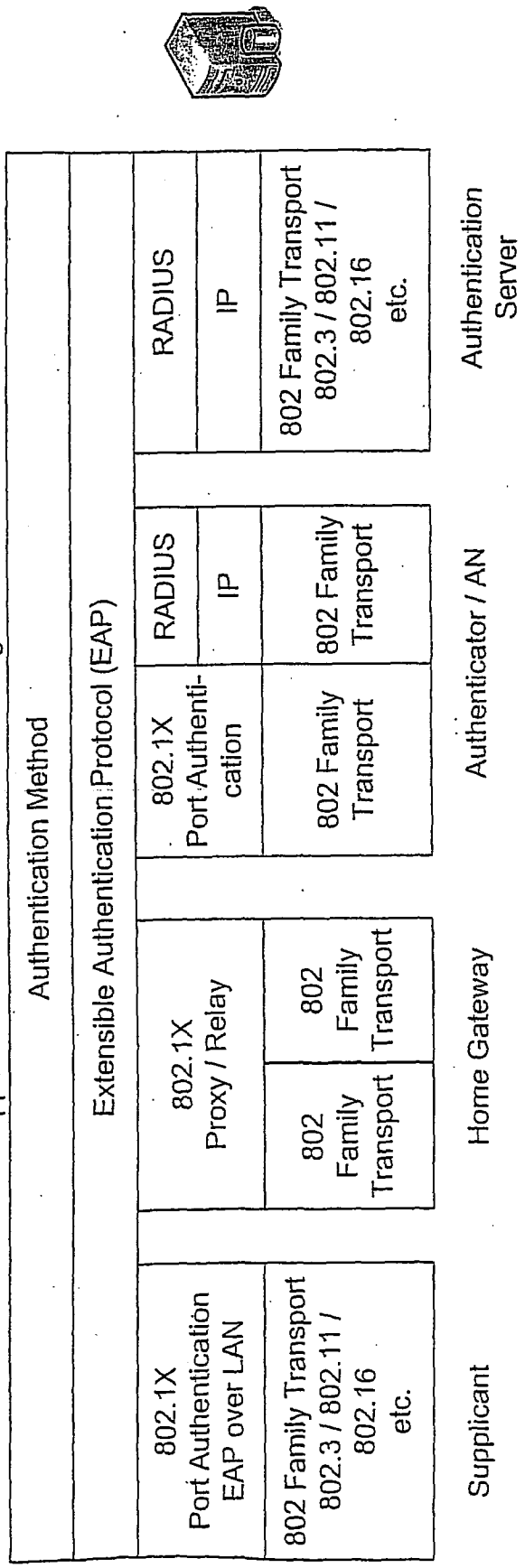
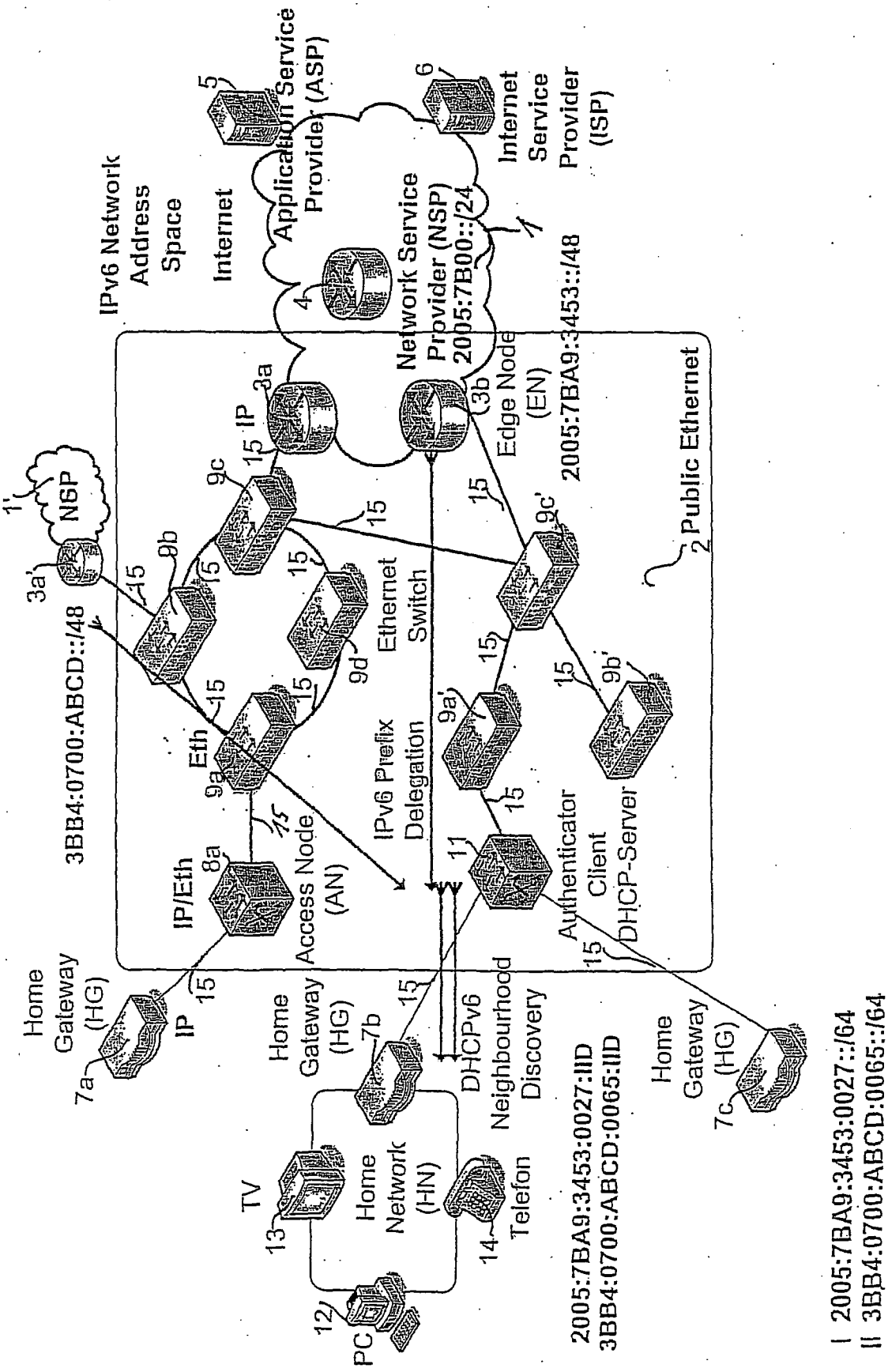

Supplicant talks to RADIUS server using EAP method
Authentication Method
Extensible Authentication Protocol (EAP)
802.1X Port Authentication EAP over LAN
802 Family Transport 802.3 / 802.11 / 802.16 etc.
802.1X Proxy / Relay
802 Family Transport
802 Family Transport
802.1X Port Authenti-cation
802 Family Transport
RADIUS
IP
802 Family Transport
RADIUS
IP
802 Family Transport 802.3 / 802.11 / 802.16 etc.
Supplicant
Home Gateway
Authenticator / AN
Authentication Server

FIG. 6


IPv6 Network Address Space
Internet
Application Service Provider (ASP)
Network Service Provider (NSP) 2005:7B00::/24
Internet Service Provider (ISP)
2005:7BA9:3453::/48
Public Ethernet
Edge Node (EN)
N6P
3BB4:0700:ABCD::/48
IP
IP/Eth
Eth
Ethernet Switch
Access Node (AN)
IPv6 Prefix Delegation
Authenticator
Client
DHCP-Server
DHCPv6
Neighbourhood Discovery
Home Gateway (HG)
Home Network (HN)
TV
Telefon
PC
2005:7BA9:3453:0027::IID
3BB4:0700:ABCD:0065::IID
I 2005:7BA9:3453:0027::/64
II 3BB4:0700:ABCD:0065::/64

Nummer	IPv6 Access Node Prefix	IPv6 Edge Node Prefix
AN 1	2005:7BA9:3453:0027::/64	2005:7BA9:3453:0028::/64
AN 2	2005:7BA9:3453:0044::/64	2005:7BA9:3453:0045::/64
AN 3	2005:7BA9:3453:0063::/64	2005:7BA9:3453:0064::/64
AN x	usw.	usw.

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/003383

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/12
ADD. H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2006/080728 A1 (WEN HAIBO [CN] ET AL) 13 April 2006 (2006-04-13) paragraph [0002] - paragraph [0042] paragraph [0061] - paragraph [0082] paragraph [0091] - paragraph [0109] figures 1-5 ----- -/--	11-13, 17,18 1-10, 14-16, 19-32

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 July 2007	06/08/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Riegler, Jörg

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/003383

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JOO-CHUL LEE ET AL: "Implementation of IPv6 prefix delegation mechanism using DHCPv6 protocol" ADVANCED COMMUNICATION TECHNOLOGY, 2005, ICACT 2005. THE 7TH INTERNATIONAL CONFERENCE ON PHOENIX PARK, KOREA FEB. 21-23, 2005, PISCATAWAY, NJ, USA,IEEE, 21 February 2005 (2005-02-21), pages 635-640, XP010813718 ISBN: 89-5519-123-5	1-10, 14-16, 19-32
A	page 635, paragraph 2. - page 637 Seite 635 - Seite 637, Kapitel 2. Related Search Seite 639, Kaptiel 4. Test	11-13, 17,18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2007/003383

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006080728 A1	13-04-2006	CN 1761233 A	19-04-2006
		EP 1648134 A1	19-04-2006
		JP 2006115499 A	27-04-2006

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2007/003383

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/12
ADD. H04L12/28

Nach der internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X Y	US 2006/080728 A1 (WEN HAIBO [CN] ET AL) 13. April 2006 (2006-04-13) Absatz [0002] - Absatz [0042] Absatz [0061] - Absatz [0082] Absatz [0091] - Absatz [0109] Abbildungen 1-5 --- -/--	11-13, 17,18 1-10, 14-16, 19-32

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
27. Juli 2007	06/08/2007

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Riegler, Jörg

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2007/003383

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	JOO-CHUL LEE ET AL: "Implementation of IPv6 prefix delegation mechanism using DHCPv6 protocol" ADVANCED COMMUNICATION TECHNOLOGY, 2005, ICACT 2005. THE 7TH INTERNATIONAL CONFERENCE ON PHOENIX PARK, KOREA FEB. 21-23, 2005, PISCATAWAY, NJ, USA,IEEE, 21. Februar 2005 (2005-02-21), Seiten 635-640, XP010813718 ISBN: 89-5519-123-5	1-10, 14-16, 19-32
A	Seite 635, Absatz 2. - Seite 637 Seite 635 - Seite 637, Kapitel 2. Related Search Seite 639, Kaptiel 4. Test	11-13, 17,18

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2007/003383

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2006080728 A1	13-04-2006	CN 1761233 A	19-04-2006
		EP 1648134 A1	19-04-2006
		JP 2006115499 A	27-04-2006