



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 603 10 074 T2** 2007.06.28

(12) **Übersetzung der europäischen Patentschrift**

(97) **EP 1 517 473 B1**

(21) Deutsches Aktenzeichen: **603 10 074.0**

(96) Europäisches Aktenzeichen: **03 292 316.1**

(96) Europäischer Anmeldetag: **22.09.2003**

(97) Erstveröffentlichung durch das EPA: **23.03.2005**

(97) Veröffentlichungstag

der Patenterteilung beim EPA: **29.11.2006**

(47) Veröffentlichungstag im Patentblatt: **28.06.2007**

(51) Int Cl.⁸: **H04L 12/24** (2006.01)

H04L 12/46 (2006.01)

G06F 1/00 (2006.01)

(73) Patentinhaber:

Alcatel Lucent, Paris, FR

(74) Vertreter:

**Patentanwälte U. Knecht und Kollegen, 70435
Stuttgart**

(84) Benannte Vertragsstaaten:

**AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,
GR, HU, IE, IT, LI, LU, MC, NL, PT, RO, SE, SI, SK,
TR**

(72) Erfinder:

**De Jaegher, Jeanne Emmanuelle Rita, 1050
Brussels, BE; Manisor, Razvan, 2018 Antwerp, BE;
Six, Erwin Alfons Constant, 9270 Laarne, BE**

(54) Bezeichnung: **Verfahren zur Steuerung von Nachrichten in einer Netzperipherie-Vorrichtung eines Zugangs-
netzwerks und Netzperipherie-Vorrichtung und Netzwerkverwaltungs-Vorrichtung zur Ausführung dieses Ver-
fahrens**

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

[0001] Die vorliegende Erfindung betrifft ein Verfahren zur Steuerung von Nachrichten von einer Netzperipherie-Vorrichtung eines Zugangsnetzwerks durch Bereitstellung oder Nicht-Bereitstellung von mindestens einer Ebene-2-Zieladresse mindestens eines anderen Netzperipherie-Knotens dieses Zugangsnetzwerks an diese Netzperipherie-Vorrichtung, wie in der Präambel von Anspruch 1 weiter beschrieben.

[0002] Ein solches Verfahren ist bereits in der Technik bekannt, z.B. durch Verwendung vorkonfigurierter Filter in Zugangsmultiplexern von Ethernet-Zugangsnetzwerken wobei die zulässigen MAC-Adressen abgehender Netzperipherie-Knoten in diesen Filtern gespeichert sind. Das Verfahren und System nach dem bisherigen Stand der Technik benutzt entweder einen vorkonfigurierten Filter in den Netzperipherie-Knoten selbst oder benutzt einen mehr zentralisierten Push-Mechanismus, wobei ein zentraler Steuerungs-Server im Netzwerkverwaltungs-Modul jeden der Netzperipherie-Knoten mit seiner vorkonfigurierten Liste zulässiger Netzwerk-Vorrichtungen, mit denen er kommunizieren kann, versorgt.

[0003] In einigen Zugangsnetzwerken, zum Beispiel in verbindungslosen Zusammenfassungs-Netzwerken, wie z.B. Ethernet-Zugangsnetzwerken, sind Fehler oder Rekonfigurationen in diesem Netzwerk nach solchen Fehlern den Netzperipherie-Knoten nicht bekannt. Das bedeutet, dass wenn ein Netzwerkfehler auftritt und eine andere MAC-Adresse derselben Ebene-3-Adresse des anderen Netzperipherie-Knotens zugeordnet wird, diese Information den Filtern im Eingangs-Netzperipherie-Knoten nicht zur Verfügung steht. Die vorhandenen Push-Mechanismen, die diese Änderungen zentral verfolgen, diese Information aber nur von Zeit zu Zeit an die Netzperipherie-Knoten liefern, sind nicht dynamisch genug, um die Änderungen den Netzperipherie-Knoten, wie z.B. den Zugangsmultiplexern, schnell zu signalisieren. Der andere Mechanismus, mit dem die Filter in den Netzperipherie-Knoten beim Start vorkonfiguriert werden, liefert überhaupt keine Lösung, da bei diesem Verfahren die Änderungen während des Betriebs von Netzperipherie-Vorrichtungen, wie z.B. Zugangsmultiplexern, nie bekannt sind.

[0004] Es ist somit eine Aufgabe der vorliegenden Erfindung, ein Verfahren zur Steuerung von Nachrichten in einer Netzperipherie-Vorrichtung eines Zugangsnetzwerks des oben angegebenen bekannten Typs bereitzustellen, das dynamisch genug ist, sich an Änderungen in den Ebene-2-Zieladressen, die durch unvorhergesehene Umstände, wie z.B. Netzwerkfehler, auftreten, anzupassen.

[0005] Gemäß der Erfindung wird dieses Ziel durch die Tatsache erreicht, dass diese Ebene-2-Zieladres-

sen nur auf Anforderung durch die Netzperipherie-Vorrichtung selbst geliefert werden, wie im kennzeichnenden Teil von Anspruch 1 weiter angegeben. Da das zentralisierte Netzwerkverwaltungs-Modul die Änderungen bezüglich der erlaubten Ebene-2-Zieladressen von Netzperipherie-Vorrichtungen im Zugangsnetzwerk nachverfolgt, führt auf diese Weise, jedes Mal wenn eine Anforderung bezüglich einer solchen Kommunikation zu einer anderen Netzperipherie-Vorrichtung von einer Netzperipherie-Vorrichtung empfangen wird, das Netzwerkverwaltungs-Modul eine aktualisierte Überprüfung durch und kann die neuesten bekannten Informationen zum Netzperipherie-Knoten senden, der dementsprechend die aktuelle Information für seine weiteren Kommunikationen zur Verfügung hat.

[0006] Weiterhin wird die Anforderung im Netzperipherie-Knoten bei Ankunft eines Paketes erzeugt, das die Ebene-2-Zieladresse des Ziel-Netzperipherie-Knotens im Zugangsnetz enthält, und bei der Überprüfung, ob diese Ebene-2-Zieladresse noch nicht in einem Kommunikations-Einschränkungs-Filter im Netzperipherie-Knoten gespeichert ist. Hierdurch wird sichergestellt, dass für noch nicht lokal gespeicherte Ziele immer die neueste Information vom Netzwerkverwaltungs-Modul erhalten wird.

[0007] Es muss darauf hingewiesen werden, dass im US-Patent US-A-5 968 176 von SHERER William Paul et al (19. Oktober 1999) ein Mehrebenen-Firewall-System offen gelegt wird, das zur Bereitstellung von Sicherheit in einem Netzwerk beiträgt, das Knoten enthält, die Sicherheitsfunktionen haben, die in mehreren Protokollebenen arbeiten. Darin wird ein Verfahren offen gelegt, mit dem Nachrichten von einer Netzperipherie-Vorrichtung oder einem Knoten eines Zugangsnetzwerks (Spalte 3, Zeilen 20–40) gesteuert werden, indem mindestens eine Ebene-2-Zieladresse mindestens einer anderen Netzperipherie-Vorrichtung des Zugangsnetzes von einem Netzwerkverwaltungs-Modul des Zugangsnetzes bereitgestellt wird oder nicht bereitgestellt wird (Spalte 4, Zeilen 21–26; Spalte 5, Zeile 4), wie in der vorliegenden Erfindung. Dieses bekannte Dokument legt jedoch weder offen noch lehrt, dass bei Eintreffen eines Paketes, das mindestens eine Ebene-2-Zieladresse enthält, die Netzperipherie-Vorrichtung überprüft, ob diese Ebene-2-Zieladresse bereits in einem Kommunikations-Einschränkungs-Filter der Netzperipherie-Vorrichtung gespeichert ist und eine Anforderung erzeugt, die diese Ebene-2-Zieladresse nur in dem Fall enthält, wenn diese Ebene-2-Zieladresse noch nicht in dem Kommunikations-Einschränkungs-Filter gespeichert ist.

[0008] Es muss weiterhin darauf hingewiesen werden, dass die internationale Patentanmeldung WO-00 52575-A der "PACKET TECHNOLOGIES LTD" von DANIELY GAD (8. September 2000) auch

ein System für die lokale verteilte Sicherheit für einen Computer (22) offen legt, der mit einem Netzwerk (42) verbunden ist. Das Netzwerk (42) sendet Pakete zum und vom Computer (22). Das System enthält eine lokale Sicherheits-Vorrichtung (20) zum Anschluss des Computers (22) an das Netzwerk (42) und zur Untersuchung jedes Pakets, um zu bestimmen, ob das Paket vom Computer (22) entsprechend einer oder mehrerer Regeln empfangen wird. Auch wenn das in diesem anderen bekannten Dokument offen gelegte Verfahren mit dem Verfahren zur Steuerung von Nachrichten von einer Netzperipherie-Vorrichtung oder einem Knoten eines Zugangsnetzwerks, wie in der Präambel von Anspruch 1 erwähnt, verglichen werden kann, legt dieses andere bekannte Dokument auch wieder weder offen noch lehrt, dass bei Eintreffen eines Paketes, das mindestens eine Ebene-2-Zieladresse enthält, die Netzperipherie-Vorrichtung überprüft, ob diese Ebene-2-Zieladresse bereits in einem Kommunikations-Einschränkungs-Filter der Netzperipherie-Vorrichtung gespeichert ist und eine Anforderung erzeugt, die diese Ebene-2-Zieladresse nur in dem Fall enthält, wenn diese Ebene-2-Zieladresse noch nicht in dem Kommunikations-Einschränkungs-Filter gespeichert ist. Darüber hinaus erwähnt dieses andere bekannte Dokument nichts über die Ziel-Zulassung wie oben beschrieben. Eine weitere charakteristische Eigenschaft der vorliegenden Erfindung wird in Anspruch 2 beschrieben.

[0009] Diese ist für den Fall von Netzwerk-Fehlern extrem interessant, wo es nicht nur bekannt ist, ob eine gewünschte MAC-Adresse noch für ein Ziel benutzt werden kann oder nicht, sondern auch zusätzliche Ebene-2-Weiterleitungs-Informationen bereitgestellt werden, wie z.B. ein VLAN-Tag, und Möglichkeiten zur Dienst-Abbildung und Dienstklassen-Trennung bereitgestellt werden. Weiterhin können durch Bereitstellung von Informationen höherer OSI-Ebenen, wie z.B. Informationen der OSI-Ebene 3 oder der OSI-Ebene 4 Möglichkeiten zur Protokoll- und Anwendungssteuerung bereitgestellt werden. Zum Beispiel können Protokolle und Anwendungen, die einen bestimmten TPC-Port benutzen, zugelassen oder blockiert werden. Mit diesen OSI-Ebenen wird auf das bekannte OSI-7-Ebenen-Modell der Datenkommunikation Bezug genommen, bei dem Ebene 1 die physikalische Ebene, Ebene 2 die Sicherungsschicht, Ebene 3 die Netzwerkebene, Ebene 4 die Transportebene, Ebene 5 die Sitzungsebene, Ebene 6 die Präsentationsebene und Ebene 7 die Anwendungsebene darstellt.

[0010] Noch eine weitere charakteristische Eigenschaft der vorliegenden Erfindung wird in Anspruch 5 beschrieben.

[0011] Dadurch wird die Alterung in die Filter in den Netzperipherie-Knoten eingeführt, in denen die zu-

lässigen MAC-Adressen gespeichert sind. Hierdurch wird erneut sichergestellt, dass regelmäßig die neuesten Informationen in den Filtern gespeichert werden, wodurch eine dynamische Kommunikationssteuerung garantiert wird.

[0012] Noch eine weitere charakteristische Eigenschaft der vorliegenden Erfindung wird in Anspruch 6 beschrieben.

[0013] Indem die Anforderung zusätzliche Benutzerinformation bezüglich des Senders des Paketes enthält, werden Möglichkeiten für die Gebührenerhebung eröffnet, wie es auch in Anspruch 7 angegeben wird. Dies erlaubt weiterhin die Steuerung der Benutzer-zu-Benutzer-Kommunikation im Zugangsnetzwerk selbst, die im Allgemeinen unter normalen Betriebsbedingungen nicht zulässig ist, da sie normalerweise nicht im Netzwerkverwaltungs-Modul gespeichert wird. Indem jedoch die Möglichkeit bereitgestellt wird, solche MAC-Adressen durch Abfrage der Abrechnungs-Vorrichtung zu liefern, wie in Anspruch 8 angegeben, wird nun eine solche Benutzer-zu-Benutzer-Kommunikation im Zugangsnetzwerk möglich.

[0014] In Anspruch 9 wird weiterhin angegeben, dass das weitere Durchlaufen eines eintreffenden Paketes durch das Zugangsnetzwerk blockiert wird, wenn die Ebene-2-Zieladresse, zum Beispiel die MAC-Adresse für das Paket, nicht in der Netzperipherie-Vorrichtung gespeichert ist oder nicht durch die Netzperipherie-Vorrichtung vom Netzwerkverwaltungs-Modul empfangen wird.

[0015] Die vorliegende Erfindung betrifft auch einen Netzperipherie-Knoten und ein Kommunikations-Einschränkungs-Modul eines Netzwerkverwaltungs-Moduls, die in der Lage sind, das oben beschriebene Verfahren auszuführen, wie in den Ansprüchen 10-15, bzw. 16-21 beansprucht.

[0016] Die oben erwähnten Aufgaben und Eigenschaften der Erfindung werden deutlicher, und die Erfindung selbst wird am besten verstanden, wenn man auf die folgende Beschreibung einer Ausführung in Verbindung mit den begleitenden Zeichnungen Bezug nimmt, in denen

[0017] [Fig. 1](#) einen Überblick über ein Zugangsnetzwerk AN mit mehreren Netzperipherie-Vorrichtungen, internen Vermittlungen, einem Netzwerkverwaltungs-Modul und anderen benachbarten Netzwerken gibt, in dem eine Kommunikation von Netzperipherie-Vorrichtung ED1 zu Netzperipherie-Vorrichtung ED2 gewünscht wird, und

[0018] [Fig. 2](#) Details einer Netzperipherie-Vorrichtung ED1 und des Netzwerkverwaltungs-Moduls NMM gemäß der Erfindung zeigt.

[0019] Die vorliegende Erfindung betrifft ein Verfahren zur Steuerung und Einschränkung von Nachrichten zu erlaubten Netzperipherie-Vorrichtungen in einem Zugangsnetzwerk. Ein solches Zugangsnetzwerk, vorzugsweise ein verbindungsloses Zusammenfassungs-Netzwerk, wie z.B. ein Ethernet-Zugangsnetzwerk, wird in [Fig. 1](#) gezeigt. Diese Figur zeigt 4 Netzperipherie-Vorrichtungen ED1 bis ED4 dieses Netzwerks AN, wobei ED1 und ED2 Zugangsmultiplexer zur Zusammenfassung von Verkehr mehrerer Teilnehmer sind, die als kleine Häuser dargestellt werden, die mit diesen Zugangsmultiplexern gekoppelt sind. Andere Netzperipherie-Vorrichtungen, wie ED3 und ED4, enthalten Schnittstellen-Vorrichtungen zu einem oder mehreren Netzwerken von Netzbetreibern, z.B. stellt ED3 eine Schnittstelle zu den Netzbetreibern NSP B und NSP C bereit, und ED4 stellt eine Schnittstelle zum Netzbetreiber NSP A bereit.

[0020] Zugangsnetzwerke werden im Allgemeinen von einem Netzwerkverwaltungs-Modul verwaltet, das in [Fig. 1](#) durch Block NMM dargestellt wird. Im Allgemeinen ist es die Aufgabe eines solchen Netzwerkverwaltungs-Moduls, das Zugangsnetzwerk zu konfigurieren, indem Bandbreiten, Gebührenerfassungs- und Benutzerverwaltungs-Funktionen zugeordnet werden. Für die vorliegende Erfindung ist ein spezieller Aspekt der Netzwerkverwaltung wichtig, nämlich ihr Speicher M1 zur Speicherung einer Liste von zulässigen Ebene-2-Adressen für entsprechende zulässige Ziel-Netzperipherie-Vorrichtungen für jede Netzperipherie-Vorrichtung, für die Pakete in das Zugangsnetzwerk eintreten.

[0021] Schaut man dieses Netzwerkverwaltungs-Modul in [Fig. 2](#) detaillierter an, kann man sehen, dass neben diesem Speicher M1, in dem diese Listen für alle zulässigen Netzperipherie-Ziel-Knoten und ihre entsprechenden Ebene-2-Zieladressen gespeichert sind, das Netzwerkverwaltungs-Modul ein Kommunikations-Einschränkungs-Modul (CRM) enthält, das in der Lage ist, diese Ebene-2-Zieladressen aus dem Speicher M1 abzurufen, und das sie an einen Netzperipherie-Knoten, zum Beispiel ED1, liefert, aber nur nachdem es von ED1 eine Anforderung bezüglich dieser speziellen Zieladresse empfangen hat. Zu diesem Zweck enthält die Netzperipherie-Vorrichtung ED1 eine Kommunikations-Steuerungs-Vorrichtung CCD, welche diese Anforderungen erzeugt. In einigen Ausführungen werden diese Anforderungen bei Eintreffen eines Paketes immer erzeugt. In einer bevorzugten Ausführung der Erfindung werden diese Anforderungen nur erzeugt, wenn ein Paket eintrifft, das diese Ebene-2-Zieladresse enthält und nur, nachdem in der Netzperipherie-Vorrichtung (ED1) überprüft wurde, dass diese Ebene-2-Zieladresse noch nicht in einem darin befindlichen Kommunikations-Einschränkungs-Filter (CRF) gespeichert ist. Diese Überprüfung wird in [Fig. 2](#) durch ei-

nen ersten Kommunikations-Pfeil von der CCD zum CFR mit der Nachricht "MAC2?" gezeigt, die anzeigt, dass die CCD sich informiert, ob MAC2 im CFR vorhanden ist. Die Antwort vom CFR an die CCD wird durch den Pfeil vom CFR zur CCD mit der Nachricht "noMAC2" angezeigt, die anzeigt, dass diese Ebene-2-Zieladresse noch nicht im Kommunikations-Einschränkungs-Filter gespeichert ist. Es sei angemerkt, dass bei Initialisierung der Netzperipherie-Vorrichtung der Filter mit einigen vorher festgelegten zulässigen Adressen vorkonfiguriert oder leer sein kann.

[0022] Wenn die Kommunikations-Steuerungs-Vorrichtung CCD somit diese Ebene-2-Zieladresse in diesem Filter nicht gefunden hat, erzeugt sie die Anforderung, welche diese gewünschte Ebene-2-Zieladresse enthält und leitet sie an das Kommunikations-Einschränkungs-Modul (CRM) im Netzwerkverwaltungs-Modul (NMM) weiter. Dies wird schematisch durch den Pfeil mit der Nachricht "req MAC2" gezeigt. Bei Empfang dieser Anforderung überprüft das CRM in der Speichervorrichtung M1, ob ED1 die Erlaubnis hat, Pakete an die Ebene-2-Zieladresse MAC2 weiterzuleiten. Dies wird durch den Pfeil mit der Nachricht "MAC2/ED1?" vom CRM nach M1 schematisch dargestellt. Wenn diese Adresse in der Liste von M1 für die Vorrichtung ED1 enthalten ist, wird diese aus M1 zum CRM abgerufen, was durch den Pfeil mit der Bezeichnung "MAC2" zurück von M1 zum CRM dargestellt wird. Diese Information wird anschließend zurück zur Kommunikations-Steuerungs-Vorrichtung CCD des Netzperipherie-Knotens ED1 weitergegeben, der anschließend diese Adresse MAC2 zum Kommunikations-Einschränkungs-Filter CRF weiterleitet, wie durch den Pfeil von der CCD zum CRF mit der Nachricht "MAC2" dargestellt. Sie wird dort eine vorher festgelegte Zeit gespeichert, zum Beispiel 120 Sekunden. Nachdem diese Zeit abgelaufen ist, wird dieser Eintrag wieder aus dem Filter CRF entfernt. Dies erlaubt es, regelmäßig abzufragen, ob Ebene-2-Zieladressen noch erlaubt sind, sowie eine regelmäßige Aktualisierung mit Änderungen. Eine weitere Möglichkeit für einen sehr dynamischen Mechanismus ist es, das Kommunikations-Einschränkungs-Modul jedes Mal abzufragen, wenn ein neues Paket eintrifft. Dann wird der Filter jedes Mal aktualisiert, wenn ein neues Paket eintrifft, unabhängig davon, ob die Ebene-2-Zieladresse bereits im Filter vorhanden ist oder nicht. Für diese Implementationen kann sogar ein Filter in den Netzperipherie-Einrichtungen weggelassen werden. Diese Art der Lösung erfordert jedoch zusätzliche Kommunikations-Zeit zwischen dem Netzperipherie-Knoten und dem Netzwerkverwaltungs-Modul.

[0023] Für den Fall, dass die angeforderte Adresse MAC 2 nicht für die Kommunikation von ED1 zulässig ist, findet das Kommunikations-Einschränkungs-Modul CRM diese Adresse nicht in M1, und folglich kann es die Adresse nicht zurück zu ED1 senden. Diese

Adresse kann somit auch nicht im Kommunikations-Einschränkungs-Filter gespeichert werden, so dass die Kommunikations-Steuerungs-Einrichtung CCD bei Empfang eines eintreffenden Paketes mit dieser Ebene-2-Adresse als Ziel dann den Eintritt dieses Paketes in das Zugangsnetzwerk blockieren wird.

[0024] Für den Fall, dass im Ziel-Netzperipherie-Knoten ED2, von dem MAC2 eine Ebene-2-Adresse eines Anschlusses war, ein Fehler aufgetreten ist, wird ein neuer Anschluss mit einer neuen MAC-Adresse benutzt. Das Netzwerkverwaltungs-Modul überträgt diese aktuelle Information über ein darin enthaltenes ARP-Modul zu M1, entweder direkt oder über das CRM. ARP ist die Abkürzung für Address Resolution Protocol, was ein vorhandener Mechanismus ist, der für die Verteilung der aktualisierten Adressen sorgt. Dies geht jedoch über den Umfang dieses Patentes hinaus, und weitere Informationen über diesen Mechanismus finden sich in spezieller Literatur.

[0025] [Fig. 2](#) zeigt diesen Mechanismus durch einen Pfeil mit der Bezeichnung MAC20 zwischen ARP und M1. Der Absender des Paketes wird ebenfalls unter Verwendung des ARP-Mechanismus darüber informiert, dass ein anderer Anschluss, der zum Beispiel die Ebene-2-Adresse MAC20 hat, zu verwenden ist. M1 enthält nun für ED1 eine aktualisierte Liste, in der MAC2 weggelassen und stattdessen MAC20 hinzugefügt ist. Der Absender des Paketes, der nun informiert ist, MAC20 zu benutzen, fügt diese neue Ebene-2-Adresse in die Kopfinformation seines Paketes ein. Wenn das CRM anschließend M1 abfragt, ob MAC20 für ED1 zulässig ist, liefert M1 die Information, dass diese MAC20 in der Tat zulässig ist.

[0026] Die Adresse MAC 20 wird anschließend vom CRM an die CCD geliefert, die diese Information anschließend im CRF speichert. Dementsprechend wird, wenn neue Pakete in der CCD eintreffen, die MAC20 in ihrer Kopfinformation haben, die CCD vom CRF die Information erhalten, dass MAC20 zulässig ist.

[0027] Zusätzlich zum Abrufen zulässiger Ebene-2-Zieladressen, wie z.B. von MAC-Adressen in Ethernet-Netzwerken, kann das CRM weiterhin von einem anderen Speicher im NMM, der mit VLANM bezeichnet wird, zusätzliche Ebene-2-Weiterleitungs-Information erhalten, wie z.B. ein VLAN-Tag. VLAN ist die Abkürzung für Virtual Local Area Network (virtuelles lokales Netz) und hat den Vorteil, eine verbesserte Leistungsfähigkeit und Verwaltbarkeit, eine Unabhängigkeit von der physikalischen Topologie und eine erhöhte Sicherheit zu bieten. Die oben erwähnten Vorteile können in dem oben beschriebenen Szenarium zur Trennung von Diensten im Zugangsnetzwerk verwendet werden.

[0028] Es ist auch möglich, dass das CRM von einem anderen Speicher, zum Beispiel M3 in [Fig. 2](#), die mit der zulässigen Ebene-2-MAC-Adresse verbundene Ebene 3 oder höhere Ebenen zu erhalten. Die Information über die höhere Ebene ist nützlich, wenn bestimmte Protokolle oder Anwendungen eingeschränkt werden müssen.

[0029] Das CRM kann als Kommunikations-Software-Einschränkungs-Agent im Netzwerkverwaltungs-Modul oder als Hardware-Modul implementiert werden.

[0030] In einigen Ausführungen des Verfahrens und der Netzperipherie-Vorrichtung kann die Kommunikations-Steuerungs-Vorrichtung CCD des Netzperipherie-Knotens auch in der Lage sein, innerhalb der erzeugten Anforderungen Benutzerinformation bezüglich des Benutzers, der das Paket gesendet hat, einzufügen. Die Benutzerinformation kann Informationen der physikalischen Ebene umfassen, wie z.B. die Leitung des Zugangsmultiplexers, an die der Benutzer angeschlossen ist. Diese Benutzerinformation wird somit in der Anforderung an das CRM des Netzwerkverwaltungs-Moduls weitergeleitet. Letzteres entnimmt diese Benutzerinformation aus der Anfrage und kann diese einem Abrechnungs-Modul CM liefern. Das CM kann entsprechend reagieren, indem es Gebührenerfassungs-Information an das CRM liefert. Diese Information ist für den Fall nützlich, wenn die gewünschte Ebene-2-Adresse nicht im M1 gespeichert ist. Dies passiert zum Beispiel für Benutzer-zu-Benutzer-Kommunikationen innerhalb des Zugangsnetzwerks selbst, die normalerweise von der Netzwerkverwaltung nicht erlaubt werden, da sie normalerweise nicht in Rechnung gestellt werden können. Unter Verwendung des vorliegenden Mechanismus, bei dem das CRM das Abrechnungs-Modul CM bei Empfang einer solchen Anforderung abfragt, wird das Abrechnungs-Modul jedoch über diese Art der Kommunikation unterrichtet, so dass es dafür Gebühren erheben kann. Das CM kann dann weiterhin diese Information zum CRM liefern, das diese Information dazu benutzen kann, zu entscheiden, die angeforderte Ebene-2-Adresse zuzulassen, indem es diese Adresse als Reaktion auf eine Anforderung vom ED1 liefert, die diese Ebene-2-Adresse enthält. Obwohl die Prinzipien der Erfindung oben in Zusammenhang mit einer speziellen Vorrichtung beschrieben wurden, muss deutlich verstanden werden, dass diese Beschreibung nur als Beispiel und nicht als Einschränkung des Umfangs der Erfindung erfolgt.

Patentansprüche

1. Verfahren zur Steuerung von Nachrichten von einer Netzperipherie-Vorrichtung (ED1) eines Zugangsnetzwerks (AN) durch Bereitstellung oder Nicht-Bereitstellung mindestens einer Ebene-2-Zieladresse (MAC2) mindestens einer Netzperipherie-

rie-Vorrichtung (ED2) des Zugangsnetzwerks (AN) an die Netzperipherie-Vorrichtung (ED1) durch ein Netzwerkverwaltungs-Modul (NMM) des Zugangsnetzwerks (AN),

dadurch gekennzeichnet, dass bei Eintreffen eines Paketes, das mindestens eine Ebene-2-Zieladresse enthält, die Netzperipherie-Vorrichtung (ED1)

- überprüft, ob die mindestens eine Ebene-2-Zieladresse in einem Kommunikations-Einschränkungs-Filter (CRF) der Netzperipherie-Vorrichtung (ED1) gespeichert ist und
- eine Anforderung erzeugt, welche die mindestens eine Ebene-2-Zieladresse nur in dem Fall enthält, dass die mindestens eine Ebene-2-Zieladresse nicht in dem Kommunikations-Einschränkungs-Filter (CRF) gespeichert ist.

2. Verfahren gemäß Anspruch 1, wobei zusätzliche Information geliefert und zusammen mit der mindestens einen Ebene-2-Zieladresse (MAC2) in der Netzperipherie-Vorrichtung (ED1) gespeichert wird.

3. Verfahren gemäß Anspruch 2, wobei die zusätzliche Information Ebene-2-Weiterleitungs-Information umfasst.

4. Verfahren gemäß Anspruch 2, wobei die zusätzliche Information aus Informationen über höhere OSI-Ebenen besteht.

5. Verfahren gemäß einem beliebigen der vorherigen Ansprüche 1 bis 4, wobei die mindestens eine Ebene-2-Zieladresse (MAC2) der mindestens einen Netzperipherie-Vorrichtung (ED2) aus dem Kommunikations-Einschränkungs-Filter (CRF) der Netzperipherie-Einrichtung (ED1) nach einer vorher festgelegten Zeitdauer entfernt wird.

6. Verfahren gemäß einem beliebigen der vorherigen Ansprüche 1 bis 5, wobei die Anforderung weiterhin Benutzer-Information bezüglich des Senders des Paketes enthält.

7. Verfahren gemäß Anspruch 6, wobei das Netzwerkverwaltungs-Modul (NMM) die Benutzer-Information an ein Abrechnungs-Modul (CM) liefert.

8. Verfahren gemäß Anspruch 7, wobei das Abrechnungs-Modul (CM) weitere Gebührenerfassungs-Information bezüglich des Paket-Absenders an das Netzwerkverwaltungs-Modul (NMM) liefert, das daraufhin mit der Lieferung der mindestens einen Ebene-2-Zieladresse an den Netzperipherie-Knoten (ED1) fortfahren kann.

9. Verfahren gemäß einem beliebigen der obigen Ansprüche 1 bis 8, wobei wenn die mindestens eine Ebene-2-Zieladresse nicht in der Netzperipherie-Vorrichtung (ED1) gespeichert ist oder sie nicht an der Netzperipherie-Vorrichtung vom Netzwerkverwal-

tungs-Modul (NMM) empfangen wird, die Netzperipherie-Vorrichtung (ED1) verhindert, dass das eintreffende Paket das Zugangsnetzwerk (AN) weiter durchläuft.

10. Netzperipherie-Vorrichtung (ED1) eines Zugangsnetzwerks (AN), wobei die Netzperipherie-Vorrichtung (ED1) einen Kommunikations-Einschränkungs-Filter (CRF) enthält, der so angepasst ist, dass er mindestens eine Ebene-2-Zieladresse (MAC2) von mindestens einer anderen Netzperipherie-Vorrichtung (ED2) des Zugangsnetzwerks (AN) speichert,

dadurch gekennzeichnet, dass die Netzperipherie-Vorrichtung (ED1) weiterhin eine Kommunikations-Steuerungs-Vorrichtung (CCD) enthält, die so angepasst ist, dass sie bei Eintreffen eines Paketes, das mindestens eine Ebene-2-Zieladresse (MAC2) enthält,

- überprüft, ob die mindestens eine Ebene-2-Zieladresse bereits in dem Kommunikations-Einschränkungs-Filter (CRF) gespeichert ist,
- eine Anforderung der mindestens einen Ebene-2-Zieladresse an ein Netzwerkverwaltungs-Modul (NMM) außerhalb des Zugangsnetzwerks sendet, wenn die mindestens eine Ebene-2-Zieladresse nicht in dem Kommunikations-Einschränkungs-Filter (CRF) gespeichert ist, und
- die mindestens eine Ebene-2-Zieladresse weiter an den Kommunikations-Einschränkungs-Filter (CRF) liefert.

11. Netzperipherie-Vorrichtung (ED1) gemäß Anspruch 10, wobei der Kommunikations-Einschränkungs-Filter (CRF) in der Lage ist, zusätzliche mit der mindestens einen Ebene-2-Zieladresse verbundene Informationen zu speichern.

12. Netzperipherie-Vorrichtung (ED1) gemäß Anspruch 11, wobei die zusätzlichen Informationen Ebene-2-Ziel-Information, Leitweglenkungs-Information oder weitere Informationen über die physikalische Ebene umfassen.

13. Netzperipherie-Vorrichtung (ED1) gemäß einem beliebigen der obigen Ansprüche 10 bis 12, wobei der Kommunikations-Einschränkungs-Filter (CRF) so angepasst ist, die mindestens eine Ebene-2-Zieladresse nach einer vorher festgelegten Zeitdauer zu entfernen.

14. Netzperipherie-Vorrichtung (ED1) gemäß einem beliebigen der obigen Ansprüche 10 bis 13, wobei die Kommunikations-Steuerungs-Vorrichtung (CCD) weiterhin so angepasst ist, Benutzer-Informationen bezüglich des Absenders des Paketes in die Anforderung einzufügen.

15. Netzperipherie-Vorrichtung (ED1) gemäß einem beliebigen der obigen Ansprüche 10 bis 14, wo-

bei die Kommunikations-Steuerungs-Vorrichtung (CCD) weiterhin so angepasst ist, die Weitergabe des eintreffenden Paketes im Zugangsnetzwerk zu blockieren, wenn die mindestens eine Ebene-2-Zieladresse nicht im Kommunikations-Einschränkungs-Filter (CRF) gespeichert ist oder nicht von dem Netzwerkverwaltungs-Modul (NMM) empfangen wird.

16. Kommunikations-Einschränkungs-Modul (CRM) eines Netzwerkverwaltungs-Moduls (NMM) für ein Zugangsnetzwerk (AN), das so angepasst ist, von einer Speichervorrichtung (M1) des Netzwerkverwaltungs-Moduls (NMM) mindestens eine Ebene-2-Zieladresse (MAC2) zu erhalten, um sie an eine Netzperipherie-Vorrichtung (ED1) des Zugangsnetzwerks (AN) zu liefern, dadurch gekennzeichnet, dass das Kommunikations-Einschränkungs-Modul (CRM) weiterhin so angepasst ist, die Ebene-2-Zieladresse (MAC2) nur an die Netzperipherie-Vorrichtung (ED1) zu liefern, wenn eine Anforderung von der Netzperipherie-Vorrichtung (ED1) empfangen wird und wenn die mindestens eine Ebene-2-Zieladresse in der Anforderung von der Netzperipherie-Vorrichtung (ED1) abgerufen wird.

17. Kommunikations-Einschränkungs-Modul (CRM) gemäß Anspruch 16, das weiterhin so angepasst ist, zusätzlich zu der mindestens einen Ebene-2-Zieladresse (MAC2) zusätzliche Informationen, die mit der mindestens einer Ebene-2-Zieladresse (MAC2) verbunden sind, abzurufen und an die Netzperipherie-Vorrichtung (ED1) zu liefern.

18. Kommunikations-Einschränkungs-Modul (CRM) gemäß Anspruch 17, das weiterhin so angepasst ist, zusätzliche Ebene-2-Ziel-Informationen aus anderen Speicher-Mitteln (VLANM) des Netzwerkverwaltungs-Moduls (NMM) zu erhalten und die zusätzlichen Ebene-2-Ziel-Informationen an die Netzperipherie-Vorrichtung (ED1) zu liefern.

19. Kommunikations-Einschränkungs-Modul (CRM) gemäß Anspruch 17, das weiterhin so angepasst ist, Informationen über höhere OSI-Ebenen, welche die mindestens eine Ebene-2-Zieladresse (MAC2) betreffen, von einem Zusammenfassungs-Ressourcen-Plattform-Modul (Aggregation Resource Platform, ARP) zu erhalten und die Informationen über höhere OSI-Ebenen an die Netzperipherie-Vorrichtung (ED1) zu liefern.

20. Kommunikations-Einschränkungs-Modul (CRM) gemäß einem beliebigen der obigen Ansprüche 16 bis 19, das weiterhin so angepasst ist, zusätzliche Benutzer-Informationen aus der Anforderung von der Netzperipherie-Vorrichtung (ED1) zu entnehmen, um sie weiterhin zu einem Abrechnungs-Modul (CM) zu liefern.

21. Kommunikations-Einschränkungs-Modul (CRM) gemäß Anspruch 20, das weiterhin so angepasst ist, von dem Abrechnungs-Modul (CM) Benutzer-Rechnungserstellungs-Informationen zu empfangen, wobei das Kommunikations-Einschränkungs-Modul (CRM) so angepasst ist, auf deren Basis die mindestens eine Ebene-2-Adresse zu liefern, sogar wenn die mindestens eine Ebene-2-Adresse nicht aus der Speichervorrichtung (M1) abgerufen werden konnte.

Es folgen 2 Blatt Zeichnungen

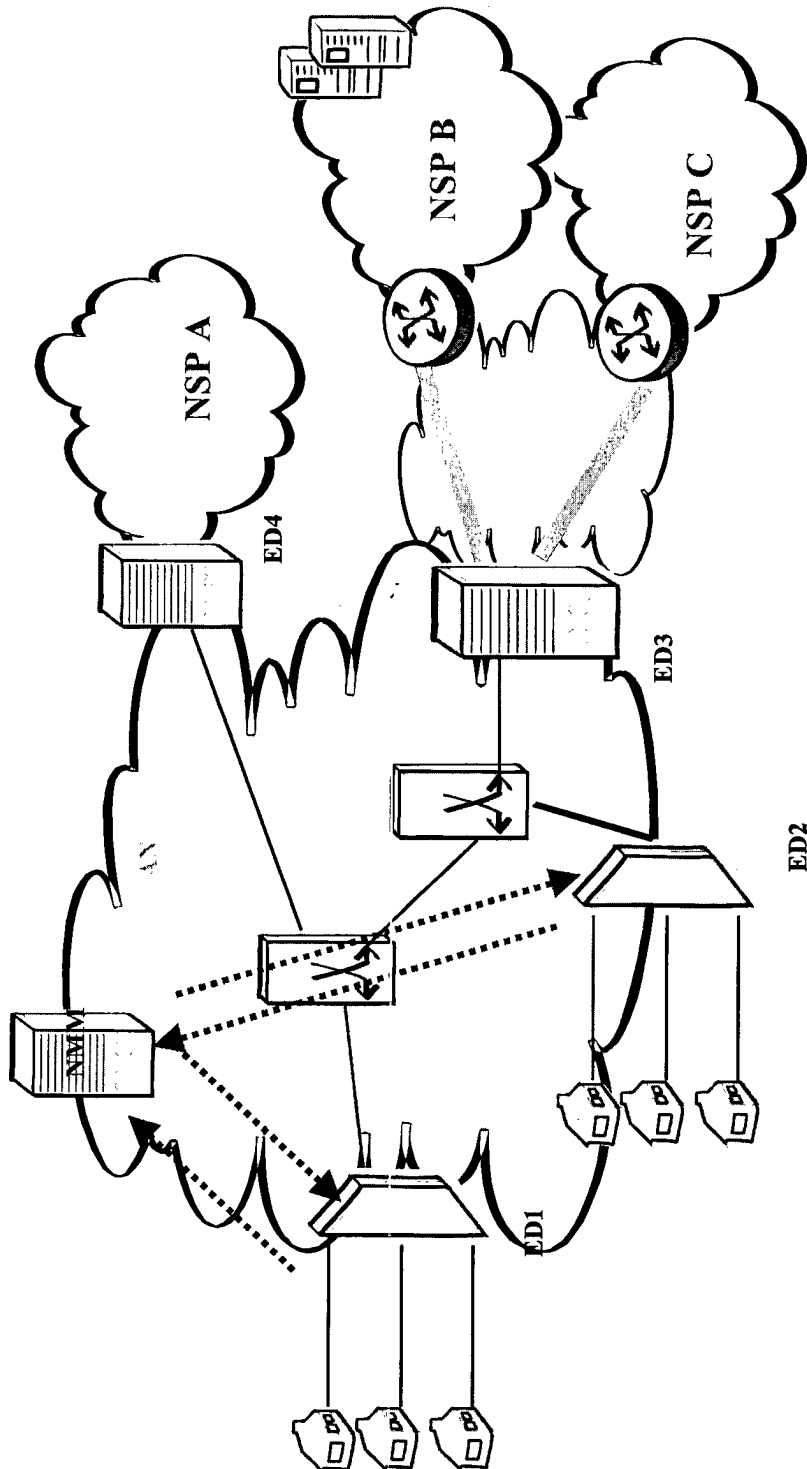


Fig. 1

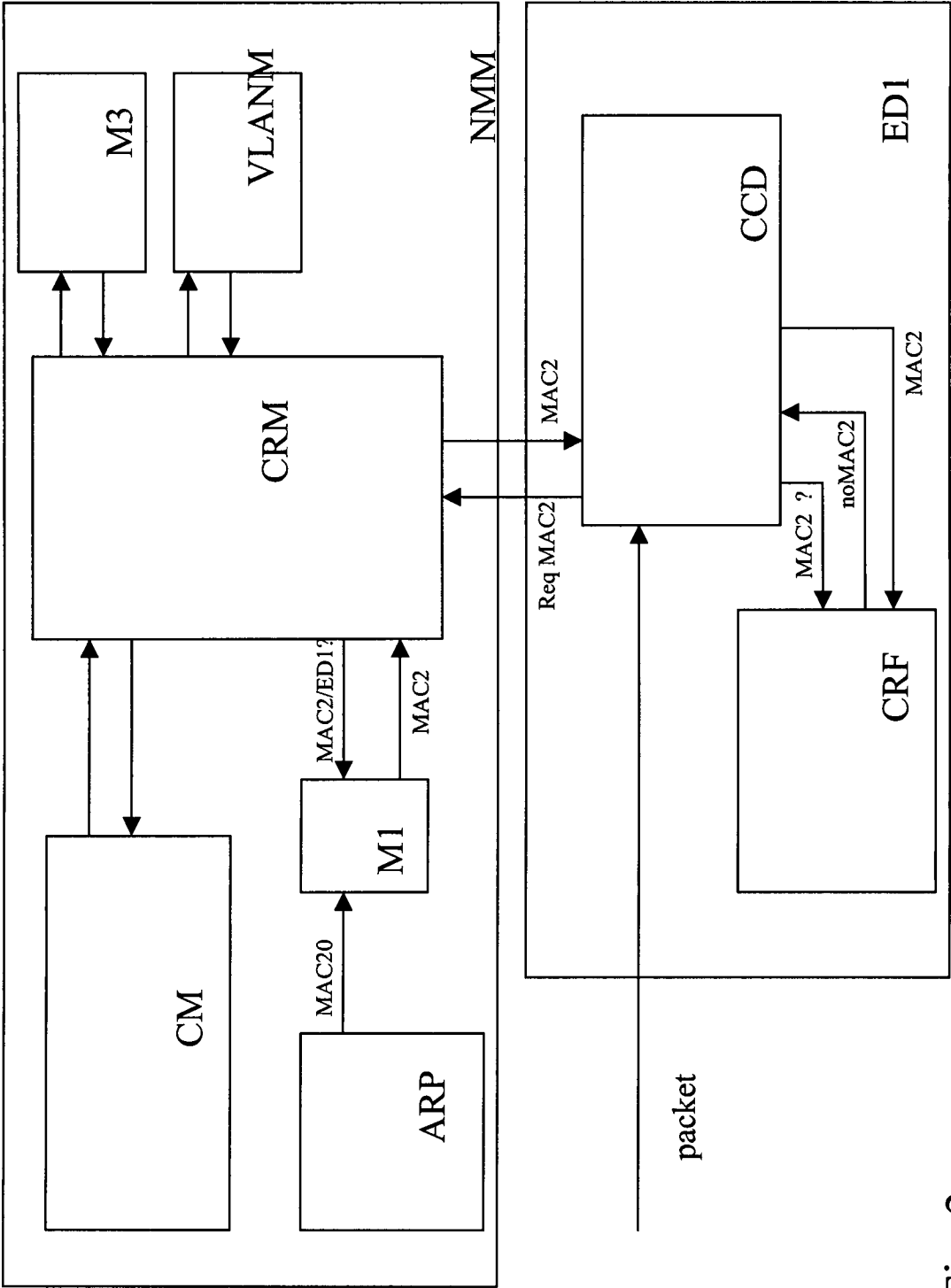


Fig. 2