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

(10) **DE 699 25 380 T2** 2006.05.04

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 142 182 B1**
(21) Deutsches Aktenzeichen: **699 25 380.2**
(86) PCT-Aktenzeichen: **PCT/FR99/03099**
(96) Europäisches Aktenzeichen: **99 958 301.6**
(87) PCT-Veröffentlichungs-Nr.: **WO 00/36779**
(86) PCT-Anmeldetag: **10.12.1999**
(87) Veröffentlichungstag der PCT-Anmeldung: **22.06.2000**
(97) Erstveröffentlichung durch das EPA: **10.10.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **18.05.2005**
(47) Veröffentlichungstag im Patentblatt: **04.05.2006**

(51) Int Cl.[8]: ***H04L 1/00*** (2006.01)

(30) Unionspriorität:
9815757 **14.12.1998** **FR**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
Netcentrex, Caen, FR

(72) Erfinder:
HERSENT, Olivier, F-14000 Caen, FR

(74) Vertreter:
Bockermann, Ksoll, Griepenstroh, 44791 Bochum

(54) Bezeichnung: **VORRICHTUNG UND VERFAHREN ZUR VERARBEITUNG EINER PAKETSEQUENZ**

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf Netze mit paketweiser Datenübertragung. Sie betrifft insbesondere, aber nicht ausschließlich, gemeinsam genutzte Netze, die gemäß dem Internet-Protokoll (IP) arbeiten.

[0002] Die Erfindung kann auf der Ebene der externen Schnittstellen von Netzroutern eingesetzt werden, um Analysen und Verarbeitungen an Datenflüssen durchzuführen, die durch diese Schnittstellen gehen.

[0003] Als „Polizei"-Funktionen werden hier verschiedene Verarbeitungs- oder Prüfungsvorgänge bezeichnet, die auf der Ebene einer derartigen Schnittstelle an diese durchfließenden Datenflüssen durchgeführt werden. Als nicht einschränkend zu verstehende Beispiele können das Zählen der zwischen einer gegebenen Quellenadresse und einer gegebenen Zieladresse ausgetauschten Pakete, die Zuordnung von Prioritäten zu bestimmten Paketen, Adressumsetzungen, die selektive Zerstörung bestimmter Pakete, usw. erwähnt werden.

[0004] Diese Polizei-Funktionen können in einen Vertragsrahmen zwischen einem Teilnehmer und einem Netzverwalter eingetragen werden. Dies kann zum Beispiel bei die Durchsatzkontrolle, die Zugriffsgenehmigungen zu bestimmten mit dem Netz verbundenen Websites, die Anwendung von Reservierungsprotokollen wie RSVP, usw. betreffenden Funktionen der Fall sein. Sie können auch im Rahmen der internen Organisation eines öffentlichen oder privaten Netzes liegen, zum Beispiel, um bestimmte Zugänge zu prüfen.

[0005] Die heutigen Router bieten einen Satz von Konfigurationsbefehlen, die es ermöglichen, solche Polizei-Funktionen anzuwenden. So wird ein sich auf bestimmte Felder im Kopf der Pakete beziehendes Filter definiert, um den oder die betroffenen Flüsse zu identifizieren, wobei das Filter einer besonderen Funktion zugeordnet ist, die an den entsprechenden Paketen ausgeführt wird. Diese Filter oder „Access List" weisen gewisse Inflexibilitäten auf. So ist es nicht möglich, zwei Filter miteinander zu verketten von denen eines eine Sortierung an den vom ersten ausgewählten Pakten spezifiziert. Diese Filter sind nach einem sequentiellen Modell konstruiert: Das erste Filter, das für ein gegebenes Paket geeignet ist, wird verwendet, und die folgenden Filter, die ebenfalls geeignet sein könnten, werden ausgeschlossen. Es ist also unmöglich, mehrere einem gleichen Fluss zugeordnete Regeln und Verarbeitungen anzuwenden (zum Beispiel, um alle gemäß dem TCP-Protokoll an einem Port x gesendeten Pakete zu zählen und alle TCP-Flüsse zu einem gegebenen Server zu zählen, einschließlich derjenigen, die zum Port x gehen).

[0006] Um bestimmte dieser Einschränkungen zu umgehen, wurden Befehle definiert, die mehrere zusammengehörende Aktionen durchführen. Diese Lösungen bieten aber nur eine relative Flexibilität und verkomplizieren insbesondere die Konfigurationssprache der Router erheblich. Es fehlt auch ein homogener Rahmen, um die zukünftigen Erweiterungen der zu gewährleistenden Polizei-Funktionen zu managen.

[0007] Die Druckschrift US 5 835 726 beschreibt ein System, um Pakete in einem Fluss zu sortieren und so Pakete in einem Informatiknetz selektiv zu verändern.

[0008] Das Dokument „A Firewall Overview", von Ted Coty, CONNECTIONS, Vol. 9, Nr. 7, 1. Juli 1995, Seiten 20–23, XP000564023, erwähnt eine Filterungsoperation von Paketen, die es ermöglicht, ein Paket in Abhängigkeit von der Ziel-/Quellenadresse oder der Port-Nummer zu blockieren oder nicht.

[0009] Es ist ein Ziel der vorliegenden Erfindung, einen Verarbeitungsmodus von Folgen von Informationspaketen anzugeben, der eine große Konfigurationsflexibilität bietet, ohne die Komplexität der Konfigurationsschnittstelle merklich zu erhöhen.

[0010] Die Erfindung schlägt eine Vorrichtung zur Verarbeitung einer Folge von Informationspaketen vor, die einen als Stapelspeicher organisierten Paketspeicher, in dem die Pakete der Folge in Zuordnung zu Verarbeitungs-Kennsätzen eingeordnet sind, eine Gruppe von Verarbeitungsmodulen und Überwachungsmittel aufweist, die den jedem aus dem Paketspeicher entnommenen Paket zugeordneten Verarbeitungs-Kennsatz empfangen und eines der Verarbeitungsmodule aktivieren, das in Abhängigkeit vom empfangenen Kennsatz ausgewählt wird, wobei das aktivierte Modul eine Elementarverarbeitung des entnommenen Pakets gewährleistet. Die von mindestens einem der Verarbeitungsmodule gewährleistete Elementarverarbeitung enthält die Zuordnung des entnommenen Pakets zu einem Kennsatz, der entsprechend einer Kennsatz-Übersetzungstabelle verändert wurde, wobei das verarbeitete Paket anschließend in Verbindung mit dem veränderten Kennsatz erneut im Paketspeicher eingeordnet wird.

[0011] Die Vorrichtung ermöglicht es, Polizei-Funktionen gemäß einem willkürlichen Graph von Elementarverarbeitungen zu verketten, die auf Datenflüsse einwirken, die von den Verarbeitungs-Kennsätzen identifiziert werden. Dies führt zu einem flexiblen Rahmen zum Managen der Konfiguration der Schnittstelle und der möglichen Protokoll-Erweiterungen.

[0012] Die Leistungsfähigkeit der Vorrichtung ist unabhängig von der Anzahl der Verkettungen von Elementarverarbeitungen, die an den durch die Schnittstelle gehenden Flüssen durchgeführt werden können und proportional zur komplexesten dieser Verkettungen. Dagegen verbraucht die verwendete Technik mehr Speicherplatz als eine übliche sequentielle Implementierung.

[0013] Ein weiterer Aspekt der vorliegenden Erfindung bezieht sich auf ein Verfahren zur Verarbeitung einer Folge von Informationspaketen, bei dem die Pakete der Folge in einem als Stapelspeicher organisierten Paketspeicher in Zuordnung zu Verarbeitungs-Kennsätzen eingeordnet werden, der jedem aus dem Paketspeicher entnommenen Paket zugeordnete Verarbeitungs-Kennsatz untersucht wird, um einen in Abhängigkeit vom empfangenen Kennsatz aus einer Gruppe von Verarbeitungsmodulen ausgewählten Verarbeitungsmodul zu aktivieren, wobei der aktivierte Modul eine Elementarverarbeitung des entnommenen Pakets gewährleistet. Die von mindestens einem der Verarbeitungsmodule gewährleistete Elementarverarbeitung enthält das Zuordnen des entnommenen Pakets zu einem entsprechend einer Kennsatz-Übersetzungstabelle veränderten Kennsatz, wobei das verarbeitete Paket anschließend in Verbindung mit dem veränderten Kennsatz erneut im Paketspeicher eingeordnet wird.

[0014] Weitere Besonderheiten und Vorteile der vorliegenden Erfindung gehen aus der nachfolgenden Beschreibung von nicht einschränkend zu verstehenden Ausführungsbeispielen unter Bezugnahme auf die beiliegenden Zeichnungen hervor.

[0015] Es zeigen:

[0016] Fig. 1 ein Schaltbild eines Netzes, in dem die Erfindung eingesetzt werden kann;

[0017] Fig. 2 ein Funktionsschaltbild eines Zugangsrouters einer privaten Anlage dieses Netzes;

[0018] Fig. 3 ein Funktionsschaltbild einer Flussverarbeitungsvorrichtung, die Teil einer Schnittstelle des Routers der Fig. 2 ist; und

[0019] Fig. 4 einen Graph von Elementarverarbeitungen, die von der Vorrichtung der Fig. 3 gewährleistet werden.

[0020] Fig. 1 zeigt ein gemeinsames Weitverkehrsnetz (WAN) **10**, das eine gewisse Anzahl von miteinander verbundenen Routern und Switche **11**, **12** aufweist. Hier wird der Fall betrachtet, in dem das gemeinsame Netz **10** gemäß dem IP-Protokoll arbeitet. Eine bestimmte Anzahl der Router sind Konzentrationsrouter **12**, mit denen private Anlagen **13** verbunden sind.

[0021] Eine private Teilnehmeranlage **13** ist typischerweise mit dem gemeinsamen Netz **10** mittels eines Zugangsrouters **15** verbunden, von dem eine der Schnittstellen **16** mit einer Leitung **17** zur Übertragung vom und zum Konzentrationsrouter **12** verbunden ist. Der Zugangsrouter **15** kann mit anderen Routern der privaten Anlage **13** oder mit Servern oder Terminals **18** dieser Anlage mittels weiterer Schnittstellen verbunden sein, die nicht in Fig. 1 dargestellt sind.

[0022] Fig. 2 zeigt ein Beispiel einer Architektur des Zugangsrouters **15**. Die externe Schnittstelle **16** sowie die Schnittstellen **20**, **21** mit dem Rest der privaten Anlage **13** sind mit dem Kern des Routers verbunden, der aus einer Paketweiterleitungsmaschine **22** („Packet Forwarding Engine") besteht. Die Weiterleitungsmaschine **22** befördert die Pakete auf der Basis der Adressen- und Portfelder, die in den Köpfen der Pakete gemäß dem IP-Protokoll und seinen möglichen Erweiterungen (TCP, UDP, etc.) enthalten sind, unter Zuhilfenahme von Routingtabellen von einer Schnittstelle zur anderen.

[0023] Manche der Schnittstellen des Zugangsrouters **15** sind nur in einer oder in beiden Übertragungsrichtungen mit Verarbeitungsvorrichtungen, oder Flussprozessoren, **24**, **25** versehen, die Polizei-Funktionen gewährleisten. Im illustrierenden Beispiel der Fig. 2 gehört die Vorrichtung **24** zur externen Schnittstelle **16** in ausgehender Richtung, und die Vorrichtung **25** gehört zu einer anderen Schnittstelle **20** in eingehender Richtung.

[0024] Der Zugangsrouter wird von einer Steuerungseinheit **26** überwacht, die aus einem Mikrocomputer oder einer Workstation bestehen kann, die eine Routing-Software ausführt, die insbesondere dazu dient, die Routingtabelle der Weiterleitungsmaschine **22** und die Flussprozessoren **24**, **25** zu konfigurieren und mit ihnen Prüf- oder Protokollinformationen auszutauschen. Diese Befehle und Austauschvorgänge erfolgen über eine geeignete Anwendungsprogrammierungsschnittstelle (API).

[0025] Die meisten existierenden Paket-Routing- und Weiterleitungs-Softwareprogramme sind frei verfügbar in Unix-Umgebungen, aber ihre Leistungsfähigkeit ist üblicherweise aufgrund der häufigen Unterbrechungen des Betriebssystems begrenzt. Es ist sehr viel schneller, ein Echtzeit-Betriebssystem wie VxWorks zu verwenden, aber dies verkompliziert die Implementation der Routing-Software.

[0026] Es ist die Aufgabe der Flussprozessoren **24**, **25**, das Nicht-Echtzeit-Betriebssystem (wie Unix), auf dessen Basis die Steuerungseinheit **26** arbeitet, bei den komplexen Tasks der Manipulation der Flüsse zu unterstützen, die Echtzeit-Leistungen erfordern (Weiterleitung, Filterung, Verschlüsselung, etc.). Diese

Prozessoren verwenden eine gewisse Anzahl von Werkzeugen zur Manipulation der Flüsse, die entsprechend jeder beliebigen Kombination dynamisch verbunden sein können, um die geforderten Prozesse auszuführen. Diese Konfiguration kann über das Betriebssystem Unix durch Aufrufen der API-Funktionen durchgeführt werden, was die Einrichtung neuer Funktionalitäten durch den Programmierer wesentlich vereinfacht.

[0027] Wie schematisch in Fig. 1 dargestellt, besteht eine der vom Flussprozessor **24** der externen Schnittstelle **16** des Zugangsrouters **15** durchgeführten Prozesse darin, jedes Paket zu einem Konzentrationsrouter **12** zu senden, wobei er dem Paket eine numerische Signatur hinzugefügt (Block **40**). Diese Signatur bezeugt, dass die fraglichen Pakete den anderen Flussprüfungsoperationen (Block **39**) unterzogen wurden, die vom Prozessor **24** durchgeführt werden.

[0028] Die entsprechende Schnittstelle **28** des Konzentrationsrouters **12** weist einen Modul zur Analyse der über die Leitung **17** empfangenen Pakete auf, um sich vom Vorhandensein der Signatur zu überzeugen.

[0029] Diese Signaturtechnik ermöglicht es vorteilhafterweise, die Flussprüfungsoperationen zu dezentralisieren, die für die Vertragsbeziehungen zwischen dem Verwalter des Konzentrationsrouters **12**, der den Anschlussdienst zum gemeinsamen Netz **10** liefert, und den Teilnehmern notwendig sind, deren Anlagen **13** mit diesem Konzentrationsrouter **12** verbunden sind. In herkömmlichen Ausführungsformen werden diese Flussprüfungsoperationen auf der Ebene des Konzentrationsrouters durchgeführt. Daraus entsteht eine beträchtliche Komplexität des Konzentrationsrouters, wenn er mit einer größeren Anzahl von privaten Anlagen verbunden ist, und ein Mangel an Flexibilität für die Teilnehmer, wenn Änderungen erforderlich sind.

[0030] Die Tatsache, dass diese Flussprüfungsoperationen in Höhe der Zugangsrouter **15** durchgeführt werden, bringt in dieser Hinsicht eine große Flexibilität. Die Signatur der Pakete garantiert dann dem Dienstanbieter, dass die Leitung **17** ihm keine gültigen Pakete schickt, die außerhalb des Vertragsrahmens mit dem Teilnehmer liegen. Wenn ein solches Paket ankommen würde, würde es die Schnittstelle **28** des Konzentrationsrouters **12** einfach eliminieren, nachdem sie die Abwesenheit der entsprechenden Signatur festgestellt hat.

[0031] Es können verschiedene herkömmliche Methoden verwendet werden, um die Signatur der Pakete auf der Basis eines den Routern **12** und **15** gemeinsamen Geheimnisses zu konstruieren und zu analysieren. Die Signatur kann insbesondere die Form eines Codeworts haben, das zum Inhalt des Pakets hinzugefügt und auf der Basis des ganzen oder eines Teils dieses Inhalts und eines geheimen Schlüssels berechnet wird, wobei die Berechnung mit Hilfe einer Funktion durchgeführt wird, die äußerst schwierig invertierbar ist, um den Geheimschlüssel wiederzugewinnen. Man kann so eine Technik des Zerhackens des Inhalts oder nur eines Teils des Inhalts des Pakets verwenden, zum Beispiel ein MD5-Zerhacken (siehe R. Rivest, RFC 1231, „The MD5 Message Digest Algorithm").

[0032] Man kann auch eine Chiffriermethode verwenden, um die Signatur der Pakete zu bilden. Der Inhalt des Pakets wird dann mit Hilfe eines privaten Schlüssels chiffriert, wobei die Schnittstelle **28** des Konzentrationsrouters die entsprechende Dechiffrierung mit Hilfe eines öffentlichen oder privaten Schlüssels gewährleistet. Die nicht chiffrierten oder mit einem falschen Schlüssel chiffrierten Pakete werden dann auf der Ebene der Schnittstelle **28** zerstört.

[0033] Optional kann man vorsehen, dass die Schnittstelle **28** des Konzentrationsrouters ebenfalls die Pakete signiert, die sie auf der Leitung **17** sendet, und dass die Schnittstelle **16** des Zugangsrouters diese Signatur überprüft, um die Gültigkeit der empfangenen Pakete zu sicherzustellen.

[0034] Fig. 3 zeigt die Organisation eines Flussprozessors **24** oder **25** einer Schnittstelle des Zugangsrouters **15**.

[0035] Der Flussprozessor empfängt eine Folge von eingehenden Paketen **30**, die je einen Kopf **31** entsprechend dem IP-Protokoll aufweisen, und liefert eine Folge von ausgehenden Paketen **32** mit einem Kopf **33**, nachdem er bestimmte Elementarverarbeitungen durchgeführt hat, deren Art von den betreffenden Datenflüssen abhängt.

[0036] Die eingehenden Pakete **30** werden in einem Paketspeicher **35** eingeordnet, der als Stapelspeicher vom Typ First-In-First-Out (FIFO) organisiert ist. Jedes Paket wird an den Speicher **35** mit einem Verarbeitungs-Kennsatz **36** geliefert. Der Verarbeitungs-Kennsatz hat zu Anfang einen bestimmten Wert (0 im dargestellten Beispiel) für die eingehenden Pakete **30**.

[0037] Der Flussprozessor wird von einer Einheit **37** überwacht, die mit einer Tabelle **38** zusammenwirkt, die es ermöglicht, jedem Wert des Verarbeitungs-Kennsatzes einen besonderen Verarbeitungsmodul zuzuordnen. Im in Fig. 3 dargestellten, vereinfachten Beispiel weist der Flussprozessor eine Gruppe von fünf Verarbeitungsmodulen M1–M5 auf, die Elementarverarbeitungen unterschiedlicher Art durchführen.

[0038] Nach der Ausführung einer Elementarverarbeitung fragt die Überwachungseinheit **37** den Paketspeicher **35** ab. Wenn dieser nicht leer ist, wird gemäß der FIFO-Organisation ein Paket daraus entnommen. Die Überwachungseinheit **37** fragt die Tabelle **38** ab, um zu bestimmen, welches Verarbeitungsmodul dem Kennsatz dieses Pakets entspricht. Die Einheit **37** aktiviert dann das betreffende Modul, damit dieses die entsprechende Elementarverarbeitung durchführt. In manchen Fällen kann diese Elementarverarbeitung eine Veränderung des Paketinhalts nach sich ziehen, insbesondere seines Kopfs.

[0039] Es ist klar, dass die „Entnahme" des Pakets, auf die Bezug genommen wird, eine Entnahme aus dem FIFO-Speicher im logischen Sinn ist. Das Paket wird nicht unbedingt aus dem Speicher entfernt. Die Adressen der Pakete im Speicher **35** können üblicherweise mittels Pointern verwaltet werden, um die FIFO-Organisation zu berücksichtigen. Der aktivierte Verarbeitungsmodul kann einfach über die Adresse des laufenden Pakets verfügen, um die Lesevorgänge, Analysen, Veränderungen oder Unterdrückungen durchzuführen, die ggf. erforderlich sind.

[0040] Das erste Verarbeitungsmodul M1, dem der Ursprungs-Kennsatz 0 zugeordnet ist, ist ein Filtermodul, das die Adressen- und/oder Protokolldefinitions- und/oder Portfelder des IP-Kopfes der Pakete analysiert. Mit Hilfe einer Zuordnungstabelle T1 liefert der Filtermodul M1 einen zweiten Verarbeitungs-Kennsatz, der eine Verkettung von Elementarverarbeitungen identifiziert, die anschließend am Paket durchgeführt werden müssen. Nachdem der zweite Verarbeitungs-Kennsatz für das aus dem Speicher **35** entnommene Paket bestimmt wurde, speichert das Filtermodul M1 das Paket mit dem zweiten Verarbeitungs-Kennsatz erneut im Speicher **35**. Die folgende Elementarverarbeitung wird dann in dem Moment durchgeführt, in dem das Paket erneut aus dem Speicher entnommen wird.

[0041] Das Modul M2 ist ein Modul, um Pakete, die zu bestimmten Flüssen gehören, zu zählen. Im Fall der in Fig. 3 dargestellten Zuordnungstabelle **38** wird dieser Modul M2 für die Verarbeitungs-Kennsätze 2 und 4 aufgerufen. Wenn er ein Paket verarbeitet, inkrementiert das Modul M2 einen Zähler mit der Anzahl von Bytes des Pakets, oder anderenfalls mit dem Wert 1 im Fall eines Paketzählers. Der Zähler kann gesichert sein, insbesondere, wenn er zur Fakturierung an den Teilnehmer durch den Verwalter des Netzes **10** dient. Bei einem gesicherten Zähler werden beim Zugangsanbieter regelmäßig Übertragungskredite angefordert, wobei die relevanten Pakete zerstört werden, wenn der Kredit erschöpft ist.

[0042] Das Modul M3 der Fig. 3 ist ein Prioritätsmanagementmodul. Im Fall der in Fig. 3 dargestellten Zuordnungstabelle **38** wird dieser Modul M3 für den Verarbeitungs-Kennsatz 3 aufgerufen. Das Modul M3 bearbeitet das Feld TOS („Type Of Service") des IP-Kopfes der Pakete. Der TOS wird im Netz zur Verwaltung der Weiterleitungsprioritäten verwendet, um auf bestimmten Verbindungen eine bestimmte Dienstqualität zu liefern. Das Feld TOS kann gemäß vorher gespeicherten Tabellen verändert werden. Diese Tabellen können unter der Kontrolle des Zugangsanbieters definiert werden, um zu verhindern, dass Pakete in ungeeigneter Weise mit einer hohen Priorität übertragen werden, wodurch das Netz gestört werden könnte.

[0043] Die zuletzt an einem Paket des Speichers **35** durchgeführte Elementarverarbeitung ist entweder seine Zerstörung (Modul M4 aktiviert durch den Kennsatz 8), oder seine Rückführung zum Ausgang des Flussprozessors (Modul M5 aktiviert durch den Kennsatz 5 oder 9). Der Modul M4 kann verwendet werden, um Pakete zu zerstören, die ein bestimmtes Ziel und/oder einen bestimmten Ursprung haben.

[0044] Die Module M2 und M3, die nicht die für ein Paket vorzunehmenden Verarbeitungen beenden (außer im Fall der Zerstörung), arbeiten je mit einer Kennsatz-Übersetzungstabelle T2, T3. Diese Übersetzungstabelle bezeichnet für den aus dem Speicher **35** mit dem laufenden Paket entnommenen Verarbeitungs-Kennsatz einen anderen Verarbeitungs-Kennsatz, der die folgende zu gewährleistende Elementarverarbeitung bezeichnet. Die von diesem Modul M2 oder M3 gewährleistete Elementarverarbeitung endet durch die Zuordnung des Pakets zu diesem anderen Verarbeitungs-Kennsatz und die Wiedereinspeisung des so verarbeiteten Pakets in den Speicher **35**.

[0045] So kann man sehr unterschiedliche Verarbeitungskombinationen an den verschiedenen den Prozessor durchfließenden Datenflüssen durchführen.

[0046] Fig. 4 zeigt ein vereinfachtes Beispiel, das den in Fig. 3 dargestellten Tabellen **38**, T1–T3 entspricht. Das eingehende Paket **30**, das dem ersten Kennsatz 0 zugeordnet ist, wird zunächst der vom Modul M1 durchgeführten Filterung unterzogen.

[0047] In einem besonders betrachteten Fall zählt der Flussprozessor **24** die von einer Quellenadresse AS1 zu einer Zieladresse AD1 und einem Port P1 gesendeten Pakete und verändert das Feld TOS dieser Pakete, ehe er sie über die Leitung **17** ausliefert, was dem oberen Zweig des Graphs der Fig. 4 entspricht. Darüber hinaus zählt der Flussprozessor **24** die von einer Quellenadresse AS2 zu einem Port P2 kommenden Pakete, ehe er sie zerstört, was dem unteren Zweig der Fig. 4 entspricht. Die anderen Pakete werden einfach an die Leitung **17** geliefert. Der Vorgabewert (9) des Verarbeitungs-Kennsatzes, der vom Modul M1 zurückgeschickt wird, bezeichnet also einfach

den Ausgangsmodul M5. Wenn der Modul M1 im aus dem Speicher **35** entnommenen Paket die Kombination AS1, AD1, P1 in den zutreffenden Adressen- und Portfeldern erfasst, schickt er das Paket mit dem Verarbeitungs-Kennsatz 2 zurück. Wenn die Werte AS2, P2 in den Adressen- und Portfeldern erfasst werden, ist es der Kennsatz 4, der mit dem Paket zurückgeschickt wird.

[0048] Diese Kennsätze 2 und 4 entsprechen beide dem Zählmodul M2. Der Kennsatz zeigt für diesen Modul auch die Speicheradresse des Zählers an, der inkrementiert werden muss. Die Tabelle T2, mit der das Modul M2 arbeitet, ermöglicht es am Ende der Verarbeitung, die Rückkehr zum nächsten zu aktivierenden Modul durchzuführen (M3 bezeichnet mit Kennsatz 3 die Pakete, deren TOS verändert werden muss, M4 bezeichnet mit Kennsatz 8 die zu zerstörenden Pakete).

[0049] Der Modul M3 empfängt Pakete mit dem Verarbeitungs-Kennsatz 3 und schickt sie mit dem Kennsatz 9 zurück, nachdem er die erforderliche Veränderung des Felds TOS durchgeführt hat.

[0050] Ausgehend von diesem vereinfachten Beispiel sieht man, dass der Flussprozessor es ermöglicht, ausgehend von der Identifikation eines Flusses durch den Filtermodul M1, verschiedene Kombinationen von Elementarverarbeitungen auf relativ einfache und schnelle Weise durchzuführen.

[0051] Ein Hauptvorteil dieser Vorgehensweise ist die Flexibilität der Konfigurationsoperationen des Flussprozessors. Die Tabellen **38**, T1–T3, die einen beliebigen Graph von Elementarverarbeitungen definieren, wie derjenige, der in Fig. 4 dargestellt ist, können relativ einfach und mit einem geringen Echtzeitzwang mittels der Managementeinheit **36** über die API konstruiert werden. Gleiches gilt für die Informationen, die es den Modulen M1–M5 erlauben, ihre Elementarverarbeitungen durchzuführen (Beschreibung der durch den Modul M2 durchzuführenden Zählvorgänge, Art der Änderung der Felder TOS durch den Modul M3, ...).

[0052] In der Praxis kann der Flussprozessor verschiedene andere Verarbeitungsmodule als diejenigen aufweisen, die als Beispiel in den Fig. 3 und Fig. 4 dargestellt sind, je nach den Bedürfnissen der besonderen Anlage (zum Beispiel Managementmodul der Ausgangswarteschlangen, Adressumsetzungsmodul, ...).

[0053] Die oben beschriebene Signaturfunktion der gesendeten Pakete kann Teil der Elementarverarbeitung sein, die vom Ausgangsmodul M5 gewährleistet wird. In einer typischen Ausführung des Zugangsrouters ist der Flussprozessor **24** in einer integrierten Schaltung für eine spezifische Anwendung (ASIC) enthalten, die um einen Mikrocontrollerkern herum organisiert ist. Diese Ausführung ermöglicht es, dass es keinerlei physikalischen Zugang zwischen den Flussprüfungsmodulen **39** (zumindest denen, die die Beziehungen zwischen dem Teilnehmer und dem Verwalter des Netzes **10** betreffen) und dem Modul M5 gibt, der die Signatur der Pakete übernimmt, entsprechend dem Block **40** der Fig. 1. Dies verbessert die Sicherheit der Verbindung aus der Sicht des Netzverwalters.

Patentansprüche

1. Vorrichtung zur Verarbeitung einer Folge von Informationspaketen, **dadurch gekennzeichnet**, dass sie einen als Stapelspeicher organisierten Paketspeicher (**35**), in dem die Pakete (**30**) der Folge in Zuordnung zu Verarbeitungs-Kennsätzen (**36**) eingeordnet sind, eine Gruppe von Verarbeitungsmodulen (M1–M5) und Überwachungsmittel (**37**) aufweist, die den jedem aus dem Paketspeicher entnommenen Paket zugeordneten Verarbeitungs-Kennsatz empfangen und eines der Verarbeitungsmodule aktivieren, der in Abhängigkeit vom empfangenen Kennsatz ausgewählt wird, wobei der aktivierte Modul eine Elementarverarbeitung des entnommenen Pakets gewährleistet, und dass die von mindestens einem der Verarbeitungsmodule (M2, M3) gewährleistete Elementarverarbeitung die Zuordnung des entnommenen Pakets zu einem Kennsatz enthält, der entsprechend einer Kennsatz-Übersetzungstabelle (T2, T3) verändert wurde, wobei das verarbeitete Paket anschließend in Verbindung mit dem veränderten Kennsatz erneut im Paketspeicher (**35**) eingeordnet wird.

2. Vorrichtung nach Anspruch 1, bei der zu Beginn jedem Paket (**30**) der Folge ein erster Verarbeitungs-Kennsatz zugeordnet ist, bei der die Überwachungsmittel (**37**) einen Filtermodul (M1), der Teil der Gruppe von Verarbeitungsmodulen ist, als Reaktion auf dem Empfang des ersten Verarbeitungs-Kennsatzes aktivieren, und bei der die vom Filtermodul gewährleistete Elementarverarbeitung eine Analyse eines Vorspanns des entnommenen Pakets und die Zuordnung des Pakets zu einem zweiten Verarbeitungs-Kennsatz enthält, der vom Ergebnis der Analyse abhängt.

3. Vorrichtung nach Anspruch 1 oder 2, bei der die Gruppe von Verarbeitungsmodulen einen Ausgangsmodul (M5) aufweist, der das entnommene Paket zu einem Ausgang der Vorrichtung mit einer Signatur überträgt, die auf einem gemeinsamen Geheimnis mit einem Konzentrationsrouter (**12**) eines Telekommunikationsnetzes (**10**) beruht und die authentifiziert, dass das Paket den von der Vorrichtung (**24**) durchgeführten Verarbeitungen unterzogen wurde.

4. Verfahren zur Verarbeitung einer Folge von Informationspaketen, dadurch gekennzeichnet, dass die Pakete (**30**) der Folge in einem als Stapelspeicher organisierten Paketspeicher (**35**) in Zuordnung zu Verarbeitungs-Kennsätzen (**36**) eingeordnet werden, dass der jedem aus dem Paketspeicher entnommenen Paket zugeordnete Verarbeitungs-Kennsatz untersucht wird, um einen in Abhängigkeit vom empfangenen Kennsatz aus einer Gruppe von Verarbeitungsmodulen (M1–M5) ausgewählten Verarbeitungsmodul zu aktivieren, wobei der aktivierte Modul eine Elementarverarbeitung des entnommenen Pakets gewährleistet, und dass die von mindestens einem der Verarbeitungsmodule (M2, M3) gewährleistete Elementarverarbeitung das Zuordnen des entnommenen Pakets zu einem entsprechend einer Kennsatz-Übersetzungstabelle (T2, T3) veränderten Kennsatz enthält, wobei das verarbeitete Paket anschließend in Verbindung mit dem veränderten Kennsatz erneut im Paketspeicher eingeordnet wird.

5. Verfahren nach Anspruch 4, bei dem jedes Paket, nachdem es verschiedenen Elementarverarbeitungen unterzogen wurde, mit einer Signatur geliefert wird, die auf einem gemeinsamen Geheimnis mit einem Konzentrationsrouter (**12**) eines Telekommunikationsnetzes (**10**) beruht und die authentifiziert, dass das Paket den Elementarverarbeitungen unterzogen wurde.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

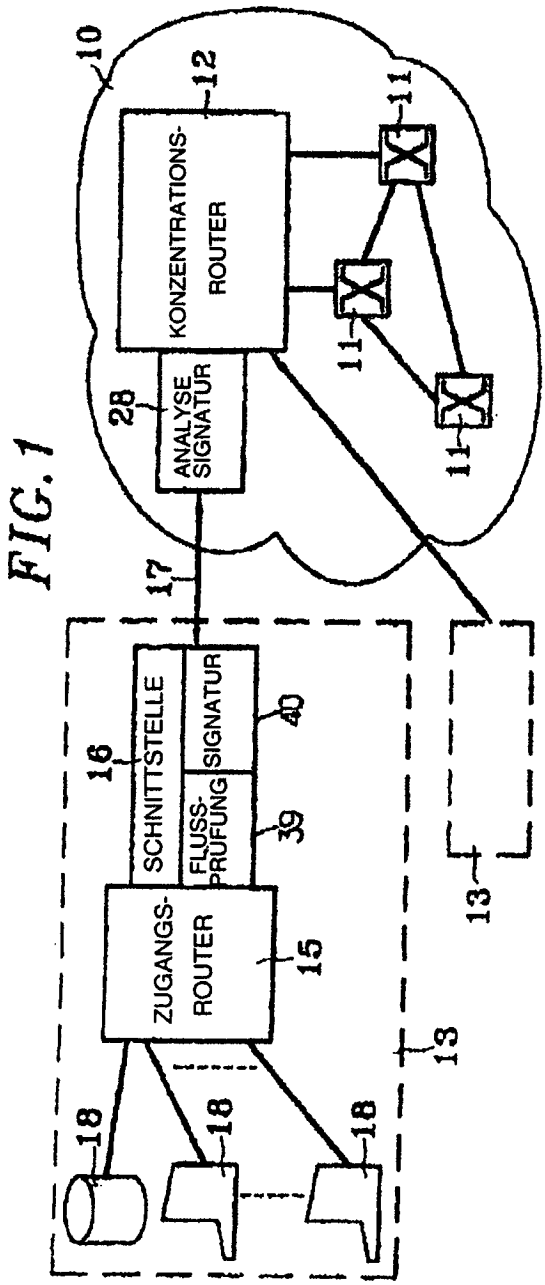


FIG. 1

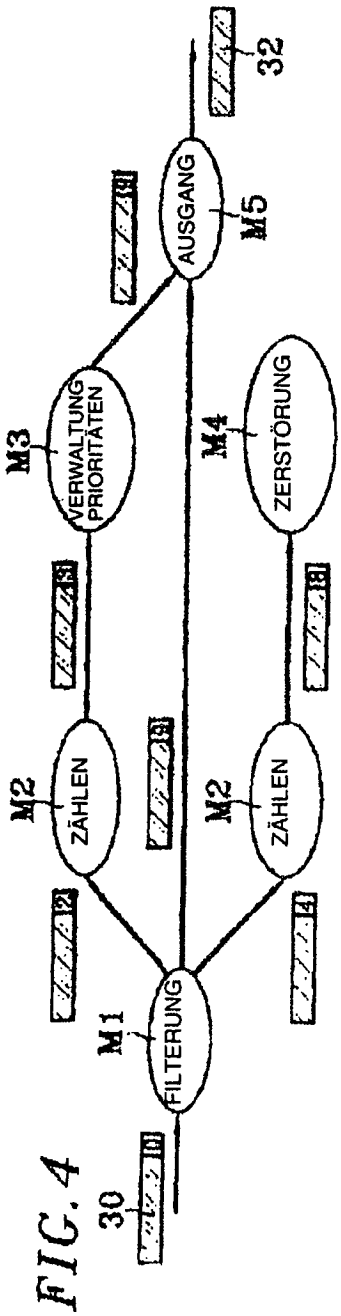


FIG. 4

FIG.2

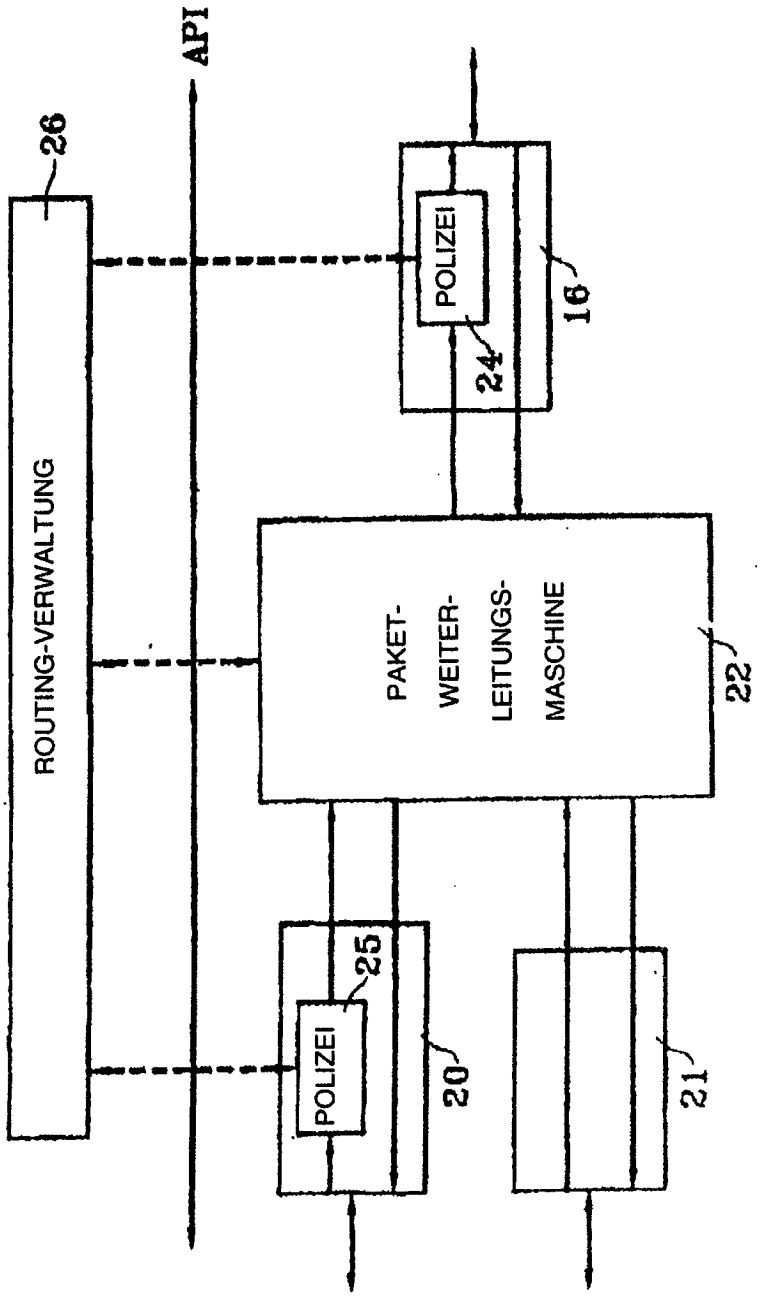
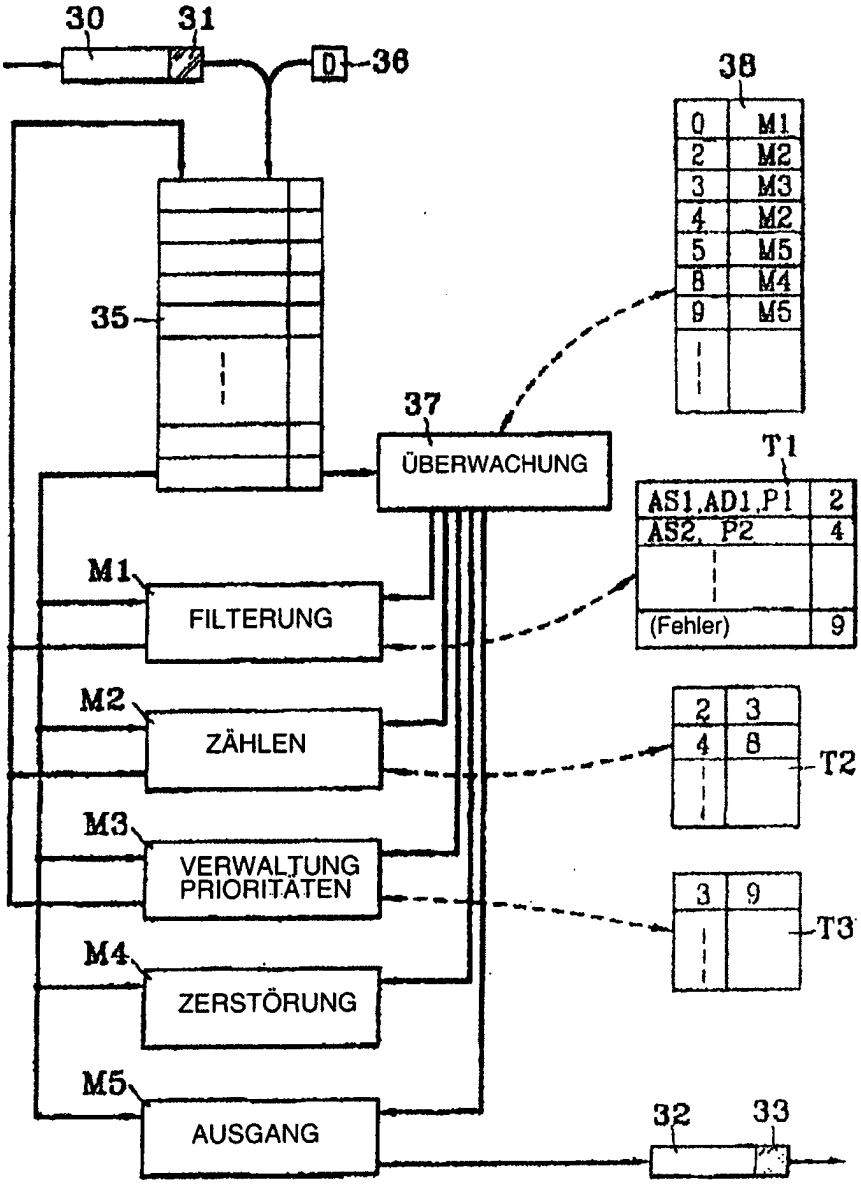

API
26
ROUTING-VERWALTUNG
POLIZEI
24
16
PAKET-
WEITER-
LEITUNGS-
MASCHINE
22
POLIZEI
25
20
21

FIG.3


30
31
36
38
0 M1
2 M2
3 M3
4 M2
5 M5
8 M4
9 M5
35
37
ÜBERWACHUNG
T1
AS1,AD1,P1 2
AS2, P2 4
(Fehler) 9
M1
FILTERUNG
M2
ZÄHLEN
2 3
4 8
T2
M3
VERWALTUNG PRIORITÄTEN
3 9
T3
M4
ZERSTÖRUNG
M5
AUSGANG
32
33