



(19)  
Bundesrepublik Deutschland  
Deutsches Patent- und Markenamt

(10) **DE 601 17 200 T2 2006.11.23**

(12)

## Übersetzung der europäischen Patentschrift

(97) **EP 1 164 766 B1**

(51) Int Cl.<sup>8</sup>: **H04L 29/06 (2006.01)**

(21) Deutsches Aktenzeichen: **601 17 200.0**

(96) Europäisches Aktenzeichen: **01 113 614.0**

(96) Europäischer Anmeldetag: **15.06.2001**

(97) Erstveröffentlichung durch das EPA: **19.12.2001**

(97) Veröffentlichungstag  
der Patenterteilung beim EPA: **15.02.2006**

(47) Veröffentlichungstag im Patentblatt: **23.11.2006**

(30) Unionspriorität:  
**2000182015 16.06.2000 JP**

(84) Benannte Vertragsstaaten:  
**DE, GB**

(73) Patentinhaber:  
**Ionos Co., Ltd., Tokio/Tokyo, JP**

(72) Erfinder:  
**Hoshino, Hirokazu, Setagaya-ku, Tokyo, JP**

(74) Vertreter:  
**Schieber und Kollegen, 80469 München**

(54) Bezeichnung: **Steueranordnung für Kanalverbindungen**

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 eingelebt, 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****HINTERGRUND DER ERFINDUNG**

## 1. Gebiet der Erfindung

**[0001]** Die vorliegende Erfindung betrifft eine wirksame Technik, die für die Sicherheit in einem Netzwerk angewendet wird.

## 2. Beschreibung der zugrundeliegenden Technik

**[0002]** Die Verbreitung des Internets zwingt die Basis von Geschäftsformen dazu, sich zu ändern. Gegenwärtig steigt, wenn Datenzentren und Provider-Geschäfte sowie Endbenutzer ständig mit dem Internet verbunden sind, die Kriminalität aufgrund von rechtswidrigem Zugriff beträchtlich. Jetzt ist die Einführung von Sicherheiten für Regierungsorganisationen, Privatpersonen und so weiter notwendig.

**[0003]** Um einen Zugriff auf ein internes Netzwerk (Intranet) von einem externen Netzwerk (Internet oder dergleichen) zu verhindern, ist eine Firewall-Technik bekannt gewesen.

**[0004]** In der herkömmlichen Sicherheit wie der Firewall sind alle Terminals und Systeme durch eine Leitung physikalisch oder logisch miteinander verbunden, und eine Angemessenheit wird auf Basis der Firewall logisch beurteilt.

**[0005]** In der herkömmlichen Netzwerksicherheitstechnik taucht, da alle Terminals und Systeme durch eine Leitung physikalisch oder logisch miteinander verbunden sind, ein derartiges Problem auf, dass unrechtmäßiges Eindringen möglich ist.

**[0006]** Um mit diesem Problem fertig zu werden, ist das Trennen des internen Netzwerks von dem externen Netzwerk die sicherste Lösung. Anders ausgedrückt, selbst in irgendeiner beliebigen Situation (Zerstörung, Angriff oder dergleichen) kann das unrechtmäßige Eindringen verhindert werden, da das externe Netzwerk und das interne Netzwerk nicht durch eine Leitung miteinander verbunden sind.

**[0007]** Wenn jedoch ein Zugriff auf das interne Netzwerk von dem externen Netzwerk aus oder ein Zugriff auf das externe Netzwerk von dem internen Netzwerk aus völlig stillgelegt wird, kann der wechselseitige flexible Betrieb der Netzwerke nicht hergestellt werden.

**[0008]** Das heißt, die physikalische Trennung des externen Netzwerks und des internen Netzwerks kann zu der Gefahr führen, dass die Echtzeiteigenschaft und die Bidirektionalität verschlechtert werden.

**[0009]** Das US-Patent Nr. 6.026.502 offenbart eine Vorrichtung zum Verhindern, dass Hacker oder Viren in einen ausgewählten Server eindringen, welche Schaltmittel auf den Eingabe- und Ausgabeseiten von Puffern und Mittel zum Steuern des Schaltmittel umfasst.

**ZUSAMMENFASSUNG DER ERFINDUNG**

**[0010]** Die vorliegende Erfindung wurde gemacht unter den obigen Umständen und deshalb ist ein Gegenstand der vorliegenden Erfindung, die flexible Zusammenarbeit eines internen Netzwerks mit einem externen Netzwerk zu ermöglichen, während ein direktes Eindringen in das interne Netzwerk bezüglich des Zugriffs von dem externen Netzwerk her durch physikalische Mittel verhindert wird.

**[0011]** Der obige Gegenstand ist erreicht worden durch die Bereitstellung einer Schalter-Schaltungssteuerungsvorrichtung wie durch Nebenanspruch 1 definiert.

**[0012]** Ein anderer Gegenstand der vorliegenden Erfindung ist, ein Sicherheitssystem bereitzustellen, das ein unrechtmäßiges Eindringen verhindert durch Verwendung einer wippenartigen Schalttechnik in Terminals und Systemen, welche für die jeweiligen Zwecke verteilt sind.

**[0013]** Gemäß der vorliegenden Erfindung können Daten vor unrechtmäßigen Vorgängen sicher geschützt werden, da das externe Netzwerk und das interne Netzwerk durch die wippenartige Schalttechnik physikalisch getrennt werden gemäß dem Steuersignal einer Zugriffsanforderung je nach einem Zweck.

**[0014]** Außerdem können gemäß der vorliegenden Erfindung, da das externe Netzwerk und das interne Netzwerk gemäß dem Steuersignal einer Zugriffsanforderung je nach Zweck getrennt sind, Daten zwischen dem externen Netzwerk und dem internen Netzwerk ohne Schädigung der Echtzeiteigenschaft oder der Bidirektionalität gesendet und empfangen werden.

**KURZE BESCHREIBUNG DER ZEICHNUNGEN**

**[0015]** Diese und andere Gegenstände und Vorteile dieser Erfindung werden vollständiger offensichtlich werden aus der folgenden ausführlichen Beschreibung zusammengenommen mit den begleitenden Zeichnungen, in denen folgendes gilt:

**[0016]** [Fig. 1](#) ist ein Blockdiagramm, das die Prinzipstruktur der vorliegenden Erfindung zeigt;

**[0017]** [Fig. 2](#) ist ein Blockdiagramm, das die Prinzipstruktur der vorliegenden Erfindung zeigt;

[0018] [Fig. 3](#) ist ein Blockdiagramm, das die Prinzipstruktur der vorliegenden Erfindung zeigt;

[0019] [Fig. 4](#) ist ein Blockdiagramm, das die Prinzipstruktur der vorliegenden Erfindung zeigt;

[0020] [Fig. 5](#) ist ein funktionelles Blockdiagramm, das die Einzelheiten gemäß einer Ausführungsform zeigt;

[0021] [Fig. 6](#) ist ein Diagramm, das die Struktur einer Wippen-Schaltbox (seesaw switching box, SSWB) und eine Wahrheitstabelle gemäß einer Ausführungsform zeigt;

[0022] [Fig. 7](#) ist ein erklärendes Diagramm, das den Betrieb einer Schaltungssteuerungsvorrichtung gemäß einer Ausführungsform zeigt;

[0023] [Fig. 8](#) ist ein erklärendes Diagramm, das den Betrieb einer Schaltungssteuerungsvorrichtung gemäß einer anderen Ausführungsform zeigt;

[0024] [Fig. 9](#) ist ein erklärendes Diagramm, das den Betrieb einer Schaltungssteuerungsvorrichtung gemäß einer nochmals anderen Ausführungsform zeigt;

[0025] [Fig. 10](#) ist ein erklärendes Diagramm, das den Betrieb einer Schaltungssteuerungsvorrichtung gemäß einer noch anderen Ausführungsform zeigt;

[0026] [Fig. 11](#) ist ein systematisches Diagramm, das ein angewendetes Beispiel einer Ausführungsform zeigt;

[0027] [Fig. 12](#) ist ein systematisches Diagramm, das ein angewendetes Beispiel einer Ausführungsform zeigt;

[0028] [Fig. 13](#) ist ein Flussdiagramm, das eine Prozedur des Umstellens von einem externen Kommunikationsmodus auf einen internen Kommunikationsmodus zeigt;

[0029] [Fig. 14](#) ist ein Flussdiagramm, das eine Prozedur des Umstellens von einem internen Kommunikationsmodus auf einen externen Kommunikationsmodus zeigt; und

[0030] [Fig. 15](#) ist ein Zeitgabediagramm für die Schaltungssteuerungsvorrichtung gemäß der Ausführungsform.

#### AUSFÜHRLICHE BESCHREIBUNG DER BEVOR-ZUGTEN AUSFÜHRUNGSFORMEN

[0031] Jetzt wird eine Beschreibung von bevorzugten Ausführungsformen der vorliegenden Erfindung mit Bezug auf die begleitenden Zeichnungen ausführlicher gegeben.

[0032] [Fig. 1](#) ist ein funktionelles Blockdiagramm, das das Konzept der vorliegenden Erfindung zeigt.

[0033] Wie in [Fig. 1](#) gezeigt sind Terminals und Systeme für die jeweiligen Zwecke klassifiziert und verteilt in die folgenden drei Bereiche.

[0034] In der Figur bezeichnet Bezugssymbol **1** ein internes Netzwerk, das wichtige Daten besitzt und ein System, welches aus einem Mehrzwecknetzwerk besteht, das mit einem Computersystem über eine Kommunikationsleitung verbunden ist. In der vorliegenden Beschreibung ist das interne Netzwerk gerichtet auf ein System mit einem Terminal oder einem Netzwerk, welches nicht an den oben erwähnten Draht oder eine Außenleitung einschließlich drahtlos angeschlossen ist.

[0035] In der Figur bezeichnet Bezugssymbol **2** ein externes Netzwerk. In der vorliegenden Beschreibung ist das externe Netzwerk gerichtet auf ein Netzwerk, ein System mit dem Netzwerk oder ein Netzstrukturteil wie ein Terminal oder eine Modular-Buchse, welche an ein Internet-Netzwerk, ein öffentliches Netz, einen Draht wie eine exklusive Leitung oder eine Außenleitung einschließlich drahtlos angeschlossen ist.

[0036] Bezugssymbol **3** bezeichnet ein Steuer-Terminal (wippenartiges Schalsicherheitssystem) zum Steuern des internen Netzwerks und des externen Netzwerks, welches das bedeutendste Element der vorliegenden Erfindung ist.

[0037] Das Steuer-Terminal **3** ist aufgebaut aus einem Schalter-Server **31**, einem Schalter-Steuerungsabschnitt **32**, einem Puffer **33**, einem Puffer **34** und einer Wippen-Schaltbox (SSWB) **35**. Die jeweiligen Funktionsabschnitte dieser Glieder werden später ausführlicher beschrieben.

[0038] In dem System wie in [Fig. 2](#) beschrieben hat das Steuer-Terminal **3** eine Funktion von Empfangen einer Anforderung von dem externen Netzwerk und von Übertragen der Anforderung an das interne Netzwerk. Außerdem hat das Steuer-Terminal **3** eine Funktion von Empfangen von Daten von dem internen Netzwerk und von Übertragen der Daten an das externe Netzwerk. In der Figur ist die Wippen-Schaltbox (SSWB) **35** in einem Zustand, wo der Puffer **34** und der Puffer **33** miteinander verbunden sind, um das Anforderungssignal von dem externen Netzwerk **2** an das interne Netzwerk **1** zu übertragen.

[0039] Außerdem hat das Steuer-Terminal **3** eine Funktion von Empfangen einer Anforderung von dem internen Netzwerk und von Übertragen der Anforderung an das externe Netzwerk, wie in [Fig. 3](#) beschrieben. Außerdem hat das Steuer-Terminal **3** eine Funktion von Empfangen von Daten von dem externen

Netzwerk und von Übertragen der Daten an das interne Netzwerk. In der Figur ist die Wippen-Schaltbox (SSWB) 35 in einem Zustand, wo das interne Netzwerk 1 und der Schalter-Server 31 miteinander verbunden sind, um das Anforderungssignal von dem internen Netzwerk 1 an das externe Netzwerk 2 zu übertragen.

**[0040]** Das Steuer-Terminal 3 ist außerdem in der Lage, das Anforderungssignal und das Datensignal bidirektional sowohl an das interne Netzwerk 1 als auch an das externe Netzwerk 2 zu senden und dort zu empfangen, wie in [Fig. 4](#) beschrieben.

**[0041]** In dem Fall der Verwendung des Steuer-Terminals 3 in dem obigen bidirektionalen Modus ist es möglich, dass ein Puffer 37 zwischen dem Schalter-Server 31 und der Wippen-Schaltbox (SSWB) 35 zwischengeschaltet ist, und ein Puffer 36 zwischen dem internen Netzwerk 1 und der Wippen-Schaltbox (SSWB) 35 zwischengeschaltet ist, so dass das Innere des Steuer-Terminals 3 seitlich symmetrisch bezüglich des internen Netzwerks 1 und des externen Netzwerks 2 ist. In diesem Fall hält der Puffer 36 die Anforderung von dem internen Netzwerk, bis der externe Seiten-Schalter (SW2) geschlossen wird. Außerdem hat der Puffer 36 eine Filterfunktion zum Beurteilen, ob unrechtmäßige Daten in der Anforderung von dem internen Netzwerk vorhanden sind, und zum Verwerfen der Anforderung, falls die unrechtmäßigen Daten nachgewiesen werden.

**[0042]** Der Puffer 37 hat eine Funktion Halten der Daten, welche von dem externen Netzwerk 2 durch den Schalter-Server 31 empfangen und dann geeignet verarbeiten werden, bis der interne Seiten-Schalter (SW1) geschlossen wird.

**[0043]** Die andere Operation des Steuer-Terminals 3 ist identisch mit der, die in den oben genannten [Fig. 2](#) und [Fig. 3](#) beschrieben ist, und deshalb wird ihre Beschreibung ausgelassen.

**[0044]** Die Struktur, dass das Innere des Steuer-Terminals 3 seitlich symmetrisch ist, ist nur in [Fig. 4](#) gezeigt. Jedoch ist eine derartige Struktur anwendbar auch auf einen Fall, wo das Steuer-Terminal 3 in irgendeiner beliebigen Betriebsart verwendet wird.

**[0045]** Nachfolgend wird eine Beschreibung der Strukturen, der Funktionen und der Operation der jeweiligen Einheiten in einer Objektverteilungseinheit (Einheiten verteilt je nach den jeweiligen Zwecken) gemäß dieser Ausführungsform gegeben mit Bezug auf [Fig. 5](#).

**[0046]** Der Schalter-Server 31 besteht aus einem Computersystem, welches aus einem Bus als einem Hauptteil, einer Zentraleinheit (CPU), einem Speicher, einem externen Speicher, einer Schnittstelle

(E/A) und so weiter gebildet wird. Ein Programm wird in dem externen Speicher installiert und die Zentraleinheit (CPU) ist so gestaltet, dass sie das Programm in den Speicher lädt und das Programm sequenziell ausführt, um dadurch das Steuerbefehlsignal der Wippen-Schaltbox (SSWB) 35 an den Schalter-Steuerungsabschnitt 32 auszugeben.

**[0047]** Anders ausgedrückt, der Schalter-Server 31 führt eine Verarbeitung aus als Reaktion auf den Zweck, zum Beispiel Anfordern notwendiger Daten von dem internen Netzwerk als Reaktion auf die Anforderung von dem externen Netzwerk und Versuch, die Daten, die von dem internen Netzwerk erhalten werden, konsistent mit der Anforderung von dem externen Netzwerk zu machen. Außerdem überträgt der Schalter-Server 31 ein Steuersignal an den Schalter-Steuerungsabschnitt 32 zum exklusiven Schalten der jeweiligen Gatter (SW1 und SW2) der externen Netzwerkseite und der internen Netzwerkseite auf Basis der Anforderung oder eines Signals wie ein Datensignal.

**[0048]** Der Schalter-Steuerungsabschnitt 32 besteht aus einer Vielzahl von Schnittstellen (E/A) hauptsächlich mit der Zentraleinheit (CPU) und dem Speicher. Anders ausgedrückt, der Schalter-Steuerungsabschnitt 32 ist so ausgelegt, dass er die Wippen-Schaltbox (SSWB) 35 auf Basis des Steuerbefehlssignals von dem Schalter-Server 31 steuert.

**[0049]** Der Schalter-Steuerungsabschnitt 32 ist völlig außer Kontakt mit einem Datensignalweg auf dem Netzwerk und überwacht den Schalter-Server 31, den Puffer 34, den Puffer 33 bzw. die Wippen-Schaltbox (SSWB), damit der Zustand der Einheit verwaltet wird.

**[0050]** Dann überträgt der Schalter-Steuerungsabschnitt 32 ein Steuersignal, das verbunden ist mit den jeweiligen Modusänderungen, an die Puffer 34 und 33 auf Basis der Informationen von dem Schalter-Server 31 oder dergleichen (siehe [Fig. 13](#) und [Fig. 14](#)).

**[0051]** Außerdem überträgt der Schalter-Steuerungsabschnitt 32 die Moduszustandssignale der Puffer 34 und 33 an den Schalter-Server 31. Ebenso empfängt der Schalter-Steuerungsabschnitt 32 ein Schalterumschaltungsteuersignal von dem Schalter-Server 31 für die Wippen-Schaltbox (SSWB) 35, beurteilt die Angemessenheit mit Bezug auf den Moduszustand der Puffer 34 und 33 und überträgt das Schalterumschaltungssteuersignal an die Wippen-Schaltbox (SSWB).

**[0052]** Die Puffer 33 und 34 sind im Wesentlichen von der Struktur her miteinander identisch, aber sie sind verschieden insofern, als dass der Puffer 34 in Reihe mit dem externen Netzwerk geschaltet ist, und

als dass der Puffer **33** zwischen der Wippen-Schaltbox (SSWB) **35** und dem Schalter-Server **31** zwischengeschaltet ist.

**[0053]** Der Puffer **34** hält die Anforderung von dem externen Netzwerk, bis der externe Seiten-Schalter (SW2) geschlossen wird. Außerdem hat der Puffer **34** eine Filterfunktion, um zu beurteilen, ob unrechtmäßige Daten in der Anforderung von dem externen Netzwerk vorhanden sind, und die Anforderung nach Nachweis der unrechtmäßigen Daten zu verwerfen.

**[0054]** Der Puffer **33** hat eine Funktion Halten der Daten, welche von dem internen Netzwerk durch den Schalter-Server **31** empfangen und entsprechend verarbeitet werden, bis der externe Seiten-Schalter (SW2) geschlossen wird.

**[0055]** Die Wippen-Schaltbox (SSWB) **35** besteht aus einem Flip-Flop-Element (FF) und Schaltern (SW1, SW2), und steuert jeden einzelnen dieser Schalter **1** und **2** in einen Kurzschlusszustand gemäß dem Wert eines Befehlssignals T von dem Schalter-Steuerungsabschnitt **32**, welches in das Flip-Flop-Element (FF) eingegeben wird.

**[0056]** Das heißt, die Wippen-Schaltbox (SSWB) **35** hat eine Funktion Empfangen des Steuersignals von dem Schalter-Steuerungsabschnitt **32** und ausschließliches Umschalten der Schalter (SW1 und SW2) auf die Seite des externen Netzwerks **2** und auf die Seite des internen Netzwerks **1** aufgrund der Operation des Flip-Flop-Elements (FF). Bezuglich dieser Sache wird der Operationsalgorithmus der Wippen-Schaltbox (SSWB) mit der Wahrheitstabelle in [Fig. 6](#) beschrieben.

**[0057]** Wie oben beschrieben haben in dieser Ausführungsform die oben beschriebenen jeweiligen Einheiten die jeweils unterschiedlichen Rollen und sind unabhängig voneinander und verteilt, wodurch sie in der Lage sind, wichtige Daten vor dem Knacken oder dem unrechtmäßigen Eindringen zu schützen. Insbesondere da der Schalter-Steuerungsabschnitt **32** völlig außerhalb des Datensignalwegs auf dem Netzwerk ist, wird, sogar wenn der Schalter-Server **31** oder der Puffer **33** und **34** geknackt werden, solches Knacken erfasst, wodurch die Wippen-Schaltbox (SSWB) kontrolliert werden kann.

**[0058]** Falls der Schalter-Server **31** und die Puffer **33, 34** in Doppelstruktur gebracht werden unter Verwendung des obigen Steuerverfahrens kann ein gesteigertes Sicherheitssystem strukturiert werden, das automatisch von der geknackten Einheit auf eine Voreinheit umgeschaltet.

**[0059]** In einer tatsächlichen Anwendung hat eine Zeitgabe, bei welcher der Schalter-Server **31** den Betriebsmodusumschaltbefehl erteilt (ein Zeitgabedia-

gramm ist in [Fig. 15](#)), die folgenden vorgeschlagenen Muster.

(1) Umschalten in einem Zeitbereich, wo die Zahl der Anforderungen an den Schalter-Server gering ist.

Der Zeitbereich, während dessen die Zahl der Anforderungen klein ist, wird auf Basis des Zugriffszustands auf den Schalter-Server **31** gesucht, und die Tatsache, dass eine externe Anforderung von dem Schalter-Server während dieses Zeitraums nicht empfangen wird, wird dem Benutzer mitgeteilt, und Kommunikation mit dem internen Netzwerk wird während dieses Zeitraums durchgeführt.

(2) periodisches Umschalten Für den Fall, dass es keinen Zeitbereich gibt, in dem die Anforderungen unterbrochen werden, schaltet die Schaltung von dem externen zu dem internen Netzwerk für jede vorher festgelegte Zeit um. Eine Zeit, die für die Kommunikation mit dem internen Netzwerk für einen Vorgang erforderlich ist, wird verringert, indem die Häufigkeit des Umschaltens erhöht wird, wodurch eine Verzögerung der Anforderung des Benutzers von dem externen Netzwerk verringert werden kann.

(3) Umschalten für jede Anforderung von dem Benutzer Zum Beispiel zu der Zeit einer Anwendung, wo der Benutzer gerne Informationen zu einer speziellen einzelnen Information von Einzelinformationen, die in dem internen Netzwerk gespeichert sind, ansehen möchte, schaltet die Schaltung jedes Mal um, wenn die einzelne Information angefordert wird. Die Information kann geschützt werden, indem nur die notwendige Mindestinformation auf die externe Netzwerkseite übertragen wird.

**[0060]** Die obigen Steuerungen (1) bis (3) werden auf Basis des Programms durchgeführt, das in dem Speicher des Schalter-Servers **1** installiert ist.

**[0061]** Dann wird der Betrieb dieses Systems beschrieben werden mit Bezug auf [Fig. 7](#) bis [Fig. 10](#).

**[0062]** Da nur irgendeiner des Schalters (SW2) auf der Seite des externen Netzwerks **2** und des Schalters (SW1) auf der Seite des internen Netzwerks **1** physikalisch geschlossen wird innerhalb des Systems (SWSEC) (Nicht-Kurzschluss-Struktur), werden, selbst falls der Schaltersteuerbefehl, der die Schaltoperation des SWSEC-Systems steuert, oder der Informationsempfangs- und -ursprungsserver (Schalter-Server **31** in dieser Ausführungsform) geknackt wird, das interne Netzwerk und das externe Netzwerk nicht elektrisch leitfähig gemacht.

**[0063]** Außerdem wird für die jeweiligen Einheiten (den Schalter-Server **31**, den Puffer **34** und den Puffer **33**) ein Steuer- und Überwachungsmechanismus (Schalter-Steuerungsabschnitt **32** in dieser Ausfüh-

rungsform), welcher vollständig außerhalb des Datensignalwegs auf dem Netzwerk ist, angeordnet, und die Schaltersteuerung wird ausgeführt, wodurch die Steuerung von dem externen Netzwerk wegen des Knacken nicht angenommen wird.

**[0064]** In diesem Beispiel wird die Zeitgabe, bei welcher der Schalter **35** gesteuert wird, nicht durch das SWSEC-System auf die autonome Art und Weise geschaltet, sondern der Schalter-Server **31** gibt die Steueranweisungen aus, wodurch das Schalten selbst dann ausgeführt werden kann, falls es keine Anforderung von dem externen Netzwerk **2** gibt. Für den Fall, dass es eine Anforderung gibt, während das interne Netzwerk von dem externen Netzwerk **2** durch Schalten getrennt ist, wird die Anforderung in dem Puffer **34** gespeichert, und wenn die Schaltung des SWSEC-Systems auf die Seite des externen Netzwerks **2** umschaltet, wird die Anforderung an den Schalter-Server **31** von dem Puffer **34** gesendet.

**[0065]** Für den Fall, dass die Verbindung des Schalter-Servers **31** und des externen Netzwerks **2** ohne irgendeine Unterbrechung fortbesteht, wird ein Zeitraum, wo das externe Netzwerk **2** mit dem internen Netzwerk **1** verbunden ist, periodisch bereitgestellt, und die Daten, die zu schützen sind, werden an das interne Netzwerk **1** übertragen. Die Daten, die von dem Schalter-Server **31** zu erzeugen sind während einer Übertragung, werden in dem Puffer **33** gespeichert. Außerdem wird in dem Fall, wo die Menge von Daten, die zu übertragen sind, groß ist, ein Informationsserver (nicht gezeigt), in welchem andere Informationen sind als die Informationen, die zu schützen sind, auf der externen Netzwerkseite angeordnet, wodurch die Anforderung für die Informationen, welche nicht geschützt sein können, immer empfangen werden kann.

**[0066]** Dann wird der Betrieb beschrieben werden.

**[0067]** Wenn eine Anforderung an das interne Netzwerk **1** von der Seite des externen Netzwerks **2** vorgenommen wird, wird das Anforderungssignal in dem Puffer **34** gespeichert.

**[0068]** In dieser Situation beurteilt die Zentraleinheit (CPU) innerhalb des Puffers **34**, ob die Anforderung unrechtmäßig ist oder angemessen, unter Verwendung eines Filterprogramms, das in dem externen Speicher installiert ist, und falls sie unrechtmäßig ist, wird die Anforderung verworfen.

**[0069]** Dann, falls es ein Paketpuffer-Modus ist, was angezeigt, dass der Schalter (SW2) der Wippen-Schaltbox (SSWB) in einem getrennten (offenen) Zustand ist, das heißt in einem Zustand, wo das interne Netzwerk **1** und der Schalter-Server **31** Datenkommunikation ausführen, wird die Anforderung gespeichert in dem Puffer **34** und es wird gewartet, bis es ein Paket-

durchgang-Modus wird, was angezeigt, dass der Schalter (SW2) der Wippen-Schaltbox (SSWB) durchgeschaltet wird, woraufhin das interne Netzwerk **1** und der Schalter-Server **31** die Datenkommunikation beenden.

**[0070]** Wenn das interne Netzwerk **1** und der Schalter-Server **31** die Datenkommunikation beenden, gibt der Schalter-Server **31** an den Schalter-Steuerungsabschnitt **32** ein Steuersignal aus zum Umschalten der Schaltung des Schalters der Wippen-Schaltbox (SSWB) **35** von dem Schalter (SW1) zu dem Schalter (SW2). Nach Empfang des Steuersignals überwacht der Schalter-Steuerungsabschnitt **32**, ob die Zustände des Puffers **34** und des Puffers **33** in dem Paketpuffer-Modus oder dem Paketdurchgang-Modus sind, und falls es der Paketpuffer-Modus ist, sendet der Schalter-Steuerungsabschnitt **32** ein Steuersignal zum Festsetzen des Modus in den Paketdurchgang-Modus an den Puffer **34** bzw. **33**. Dann, nach Empfang des Steuersignals, das eine Benachrichtigung anzeigen, dass der Modus von dem Puffer **34** bzw. **33** in den Paketdurchgang-Modus geändert wurde, sendet der Schalter-Steuerungsabschnitt **32** ein Steuersignal zum Umschalten der Schaltung des Schalters von SW1 auf SW2 an die Wippen-Schaltbox (SSWB). Außerdem, falls es sich um den Paketdurchgang-Modus handelt, sendet der Paketsteuerungsabschnitt **32** ein Steuersignal zum Umschalten der Schaltung des Schalters von SW1 auf SW2 an die Wippen-Schaltbox (SSWB) **35**.

**[0071]** Die obige Anforderung wird in den Schalter-Server **31** (Schaltsteuerung und Informationsempfangs- und -ursprungsserver) eingegeben durch den Schalter (SW2) der Wippen-Schaltbox (SSWB) und den Puffer **33**.

**[0072]** In dem Schalter-Server **31** beurteilt die Zentraleinheit (CPU) die Angemessenheit und den Zweck der Anforderung, die so eingegeben wurde, durch Verwendung eines Filterprogramms, und falls die Anforderung unrechtmäßig ist, verwirft die Zentraleinheit die Anforderung.

**[0073]** Falls die Anforderung angemessen ist, sendet die Zentraleinheit ein Steuersignal zum Umschalten der Schaltung des Schalters der Wippen-Schaltbox (SSWB) **35** von SW2 auf SW1 an den Schalter-Steuerungsabschnitt **32**.

**[0074]** Nach Empfang des Steuersignals sendet der Schalter-Steuerungsabschnitt **32** ein Steuersignal zum Festsetzen der Zustände des Puffers **34** und des Puffers **33** in den Paketpuffer-Modus an den Puffer **34** bzw. **33**. Dann, nach Empfang eines Steuersignals, das eine Benachrichtigung anzeigen, dass die Zustände von dem Puffer **34** bzw. **33** in den Paketpuffer-Modus geändert wurden, sendet die Zentraleinheit ein Steuersignal zum Umschalten der Schaltung

des Schalters von SW2 auf SW1 an die Wippen-Schaltbox (SSWB) **35**.

**[0075]** Dann, wenn die Wippen-Schaltbox (SSWB) **35** das Steuersignal empfängt, das von dem Schalter-Steuerungsabschnitt **32** gesendet wurde, schaltet die Zentraleinheit die Schaltung des Schalters von SW2 auf SW1 aufgrund der Operation des Flip-Flop-Elements (FF) um (siehe [Fig. 8](#)).

**[0076]** Der Schalter-Server **31** sendet eine Anforderung, die für den Zweck geeignet ist, an die Seite des internen Netzwerks **1**.

**[0077]** Dann, wie in [Fig. 9](#) gezeigt, sendet das interne Netzwerk **1** Daten als Reaktion auf die Anforderung, die von dem Schalter-Server **31** gesendet wurde.

**[0078]** Die Daten werden an den Schalter-Server **31** durch den Schalter (SW1) mit dem Kurzschlusszustand der Wippen-Schaltbox (SSWB) gesendet.

**[0079]** Der Schalter-Server **31** formt die Daten in ein entsprechendes Format, das für den Zweck geeignet ist. Die Formung der Daten wird durch die Zentraleinheit (CPU) auf Basis des Programms ausgeführt, das in dem externen Speicher installiert ist.

**[0080]** Dann sendet der Schalter-Server **31** ein Steuersignal zum Umschalten der Schaltung des Schalters der Wippen-Schaltbox (SSWB) von SW1 auf SW2 an den Schalter-Steuerungsabschnitt **32**, während die geformten Daten an den Puffer **33** ausgesendet werden, welcher in dem Paketpuffer-Modus ist.

**[0081]** Nach Empfang des Steuersignals von dem Schalter-Server **31** sendet der Schalter-Steuerungsabschnitt **32** das Steuersignal aus zum Umschalten der Schaltung des Schalters von SW1 auf SW2 an die Wippen-Schaltbox (SSWB) **35**. Nachfolgend sendet der Schalter-Steuerungsabschnitt **32** ein Steuersignal zum Festsetzen des Zustands des Puffers **33** in den Paketdurchgang-Modus an den Puffer **33** und empfängt ein Steuersignal, das eine Benachrichtigung anzeigen, dass der Zustand von dem Puffer **33** in den Paketdurchgang-Modus geändert wurde.

**[0082]** Dann, wie in [Fig. 10](#) gezeigt, werden Daten in den Puffer **34**, der in dem Paketpuffer-Modus ist, durch den Schalter (SW2) der Wippen-Schaltbox (SSWB) **35** hindurch von dem Puffer **33** eingegeben.

**[0083]** Nach Beendigung der Übertragung der Daten sendet der Puffer **33** das Benachrichtigungssignal (Puffer-leer-Signal) an den Schalter-Steuerungsabschnitt **32**. Nach Empfang des Puffer-leer-Signals sendet der Schalter-Steuerungsabschnitt **32** ein Steuersignal aus zum Festsetzen des Zustands in

den Paketdurchgang-Modus an den Puffer **34**, der in dem Paketpuffer-Modus ist.

**[0084]** Nach Empfang des Steuersignals setzt der Puffer **34** seinen Zustand in den Paketdurchgang-Modus und schickt ein Steuersignal, das eine Benachrichtigung anzeigen, dass der Zustand in den Paketdurchgang-Modus geändert wurde, an den Schalter-Steuerungsabschnitt **32** zurück.

**[0085]** Auf diese Weise werden die Daten an das externe Netzwerk **2** übertragen.

**[0086]** Dann wird ein angewendetes Beispiel dieser Ausführungsform beschrieben werden mit Bezug auf [Fig. 11](#).

**[0087]** In der Figur wird angenommen, dass ein Zertifizierungsakt für eine Personen-ID und das Benutzerattribut während des Internet-Shopping von einem Web-Server **1102**, der sich bei einem Provider befindet, angefordert wird von einem Datenserver (internes Netzwerk **1**), der sich innerhalb eines Unternehmens befindet.

**[0088]** Das externe Netzwerk **2** ist mit dem Internet **21** verbunden und das Internet **21** ist mit dem Web-Server **1102** des Providers durch einen Router **1101** verbunden. Der Web-Server **1102** ist mit dem Internet **22** durch den Router **1103** verbunden, und das Internet **22** ist mit einem Benutzerterminal **1104** verbunden.

**[0089]** In der Figur werden die Zertifizierungsergebnisse ausgegeben als Daten von dem internen Netzwerk **1** auf Basis der Zertifizierungsanforderung von dem externen Netzwerk **2**, und diese Operation wird realisiert wie oben mit Bezug auf [Fig. 7](#) bis [Fig. 10](#) beschrieben.

**[0090]** [Fig. 12](#) zeigt eine Struktur, in welcher die Terminal-Vorrichtung **11**, die sich innerhalb einer Privatwohnung befindet, was dem internen Netzwerk entspricht, eine Anforderung zum Herunterladen von Musikdaten an einen Web-Server **1203** des Providers sendet, was das externe Netzwerk ist, und die Musikdaten von dem Web-Server **1203** als Reaktion auf diese Anforderung empfängt.

**[0091]** In der Figur ist die Terminal-Vorrichtung **11** mit dem Internet **1201** durch den Router und eine Modular-Buchse **21** verbunden, und das Internet **1201** ist mit dem Web-Server **1203** des Providers durch den Router **1202** verbunden. Die Musikdaten für die Musiklieferung sind in dem Web-Server **1203** gespeichert.

**[0092]** In dem Musiklieferdienst wird die Übertragung der Musikdaten von dem Web-Server **1203** durch die Privat-Terminal-Vorrichtung **11** angefordert.

Wenn die Anforderung durch den Web-Server **1203** empfangen und durch ein Verfahren, das nicht gezeigt ist, zertifiziert worden ist, werden die Musikdaten durch das Steuer-Terminal **3** von dem Web-Server **1203** durch den Router und die Modular-Buchse **21** an dem Internet **1201** empfangen. Eine Prozedur vom Hervorbringen der Anforderung bis zum Empfang der Daten danach kann realisiert werden wie oben mit Bezug auf [Fig. 7](#) bis [Fig. 10](#) beschrieben. In der Beschreibung von [Fig. 7](#) bis [Fig. 10](#) sollten "Anforderung" und "Daten" vertauscht werden in "Daten" bzw. "Anforderung".

**[0093]** Außerdem kann zusätzlich zu den oben beschriebenen angewendeten Beispielen das vorliegende System angewendet werden auf ein LAN innerhalb eines Unternehmens, einen Provider, ein Datenzentrumsgeschäft, ein privates PC-Terminal und so weiter. Das heißt, die vorliegende Erfindung ist nicht beschränkt auf die oben beschriebenen Ausführungsformen und deren angewendeten Beispiele, sondern kann auf jeden Abschnitt in dem Netzwerk angewendet werden und kann die innere Sicherheit für jedes Netzwerk aufrechterhalten.

**[0094]** Die vorangehende Beschreibung der bevorzugten Ausführungsformen der Erfindung ist präsentiert worden für Zwecke der Veranschaulichung und Beschreibung. Sie ist nicht beabsichtigt, erschöpfend zu sein oder die Erfindung auf die genau offenbare Form zu beschränken, und Modifikationen und Variationen sind möglich im Licht der obigen Lehren oder können aus der praktischen Umsetzung der Erfindung erworben werden. Die Ausführungsformen wurden gewählt und beschrieben, um die Prinzipien der Erfindung zu erklären und deren praktische Anwendung, um es einem Fachmann zu ermöglichen, die Erfindung in verschiedenen Ausführungsformen und mit verschiedenen Modifikationen zu nutzen, wie sie für die jeweils betrachtete Verwendung geeignet sind. Es ist beabsichtigt, dass der Schutzmfang der Erfindung durch die hieran anliegenden Ansprüche und deren Äquivalente definiert wird.

**[0095]** Wo technische Merkmale, die in irgendeinem Anspruch erwähnt sind, von Bezugszeichen gefolgt werden, sind solche Bezugszeichen aufgenommen worden für den alleinigen Zweck, die Verständlichkeit der Ansprüche zu erhöhen.

### Patentansprüche

1. Eine Schalter-Schaltungssteuerungsvorrichtung **(3)** zum physikalischen Trennen eines internen Netzwerks **(1)** und eines externen Netzwerks **(2)**, welche zwischen dem externen Netzwerk **(2)** und dem internen Netzwerk **(1)** zwischengeschaltet ist, welche folgendes umfasst:  
einen ersten Schalter zum Kurzschließen und Freigeben des externen Netzwerks **(2)**;

einen zweiten Schalter zum Kurzschließen und Freigeben des internen Netzwerks **(1)**;  
**dadurch gekennzeichnet**, dass sie weiter einen Schalter-Steuerungsabschnitt **(32)** umfasst, der ohne Kontakt mit einem Datensignalweg, der das externe Netzwerk **(2)** und das interne Netzwerk **(1)** verbindet, angeordnet ist, wobei der Schalter-Steuerungsabschnitt **(32)** ein Steuersignal zum Kurzschließen entweder des ersten oder des zweiten Schalters ausgibt und zum gleichzeitigen Freigeben des anderen des ersten und zweiten Schalters, wobei der erste und zweite Schalter auf eine Wippenart zum Kurzschließen und Freigeben des externen Netzwerks **(2)** bzw. des internen Netzwerks **(1)** arbeiten.

2. Die Schalter-Schaltungssteuerungsvorrichtung **(3)** wie in Anspruch 1 beansprucht, die weiter folgendes umfasst:  
eine Hauptsteuerungsvorrichtung **(31)** zum Ausführen einer Zertifizierung und Steuerung von Daten; einen ersten Puffer **(34)**, der mit dem externen Netzwerk **(2)** verbunden ist; und einen zweiten Puffer **(33)**, der mit der Hauptsteuerungsvorrichtung **(31)** verbunden ist, zum Speichern einer Anforderung oder von Daten; worin der erste Schalter zum Kurzschließen und Freigeben des ersten Puffers **(34)** und des zweiten Puffers **(33)** auf dem externen Netzwerk **(2)** ist; der zweite Schalter zum Kurzschließen und Freigeben der Hauptsteuerungsvorrichtung **(31)** und des internen Netzwerks **(1)** ist; und der Schalter-Steuerungsabschnitt **(32)** das Steuersignal gemäß der Hauptsteuerungsvorrichtung **(31)** ausgibt.

3. Die Schalter-Schaltungssteuerungsvorrichtung **(3)** wie in Anspruch 2 beansprucht, worin der erste Puffer **(34)** Zertifizierungsmittel einschließt zum Verifizieren einer Richtigkeit der Anforderung oder von Daten von dem externen Netzwerk **(2)**.

4. Die Schalter-Schaltungssteuerungsvorrichtung **(3)** wie in Anspruch 2 definiert, worin die Hauptsteuerungsvorrichtung **(31)** Zertifizierungsmittel einschließt zum Verifizieren einer Richtigkeit der Anforderung oder von Daten von dem internen Netzwerk **(1)**.

5. Die Schalter-Schaltungssteuerungsvorrichtung **(3)** wie in Anspruch 2 definiert, die weiter folgendes umfasst:  
einen dritten Puffer **(37)**, der zwischen der Hauptsteuerungsvorrichtung **(31)** und dem zweitem Schalter angeordnet ist, zum Speichern einer Anforderung oder von Daten; und einen vierten Puffer **(36)**, der zwischen dem internen Netzwerk **(1)** und dem zweiten Schalter angeordnet ist, zum Speichern einer Anforderung oder von Daten.

6. Die Schalter-Schaltungssteuerungsvorrichtung (3) wie in Anspruch 5 beansprucht, worin der vierte Puffer (36) Filtermittel einschließt zum Beurteilen, ob unrechtmäßige Daten in der Anforderung von dem internen Netzwerk (1) vorhanden sind.

Es folgen 15 Blatt Zeichnungen

FIG. 1

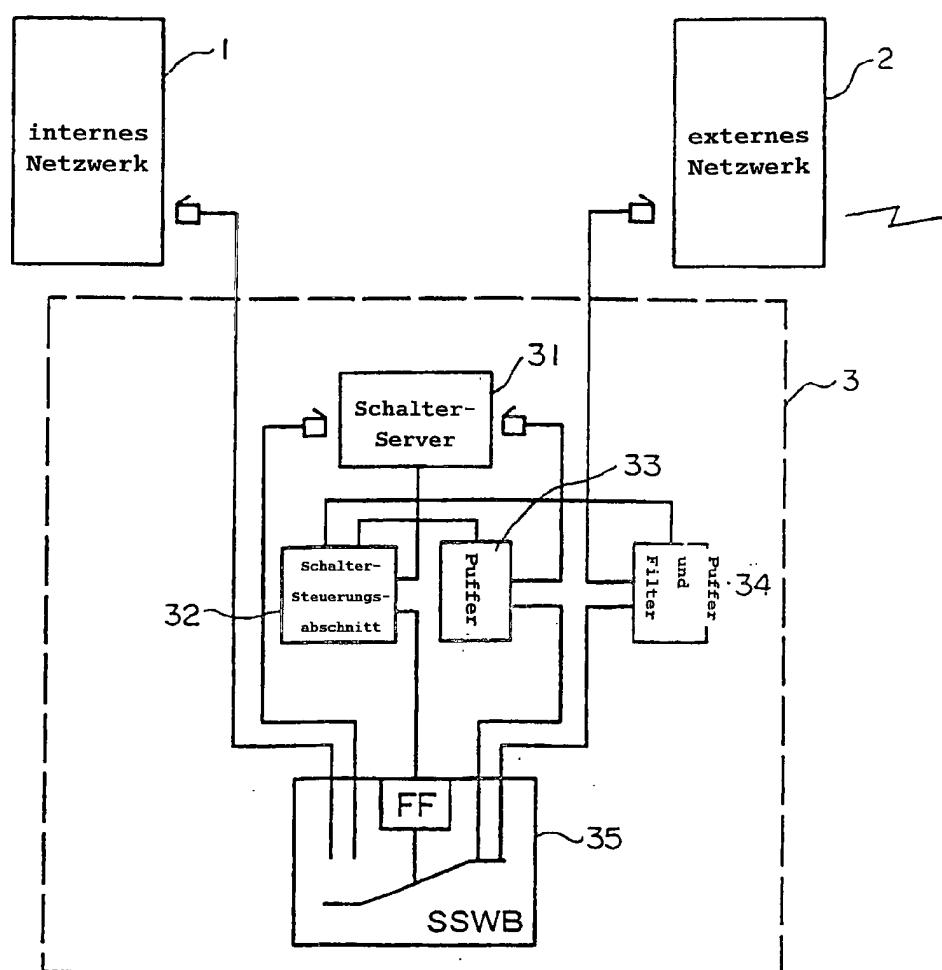


FIG. 2

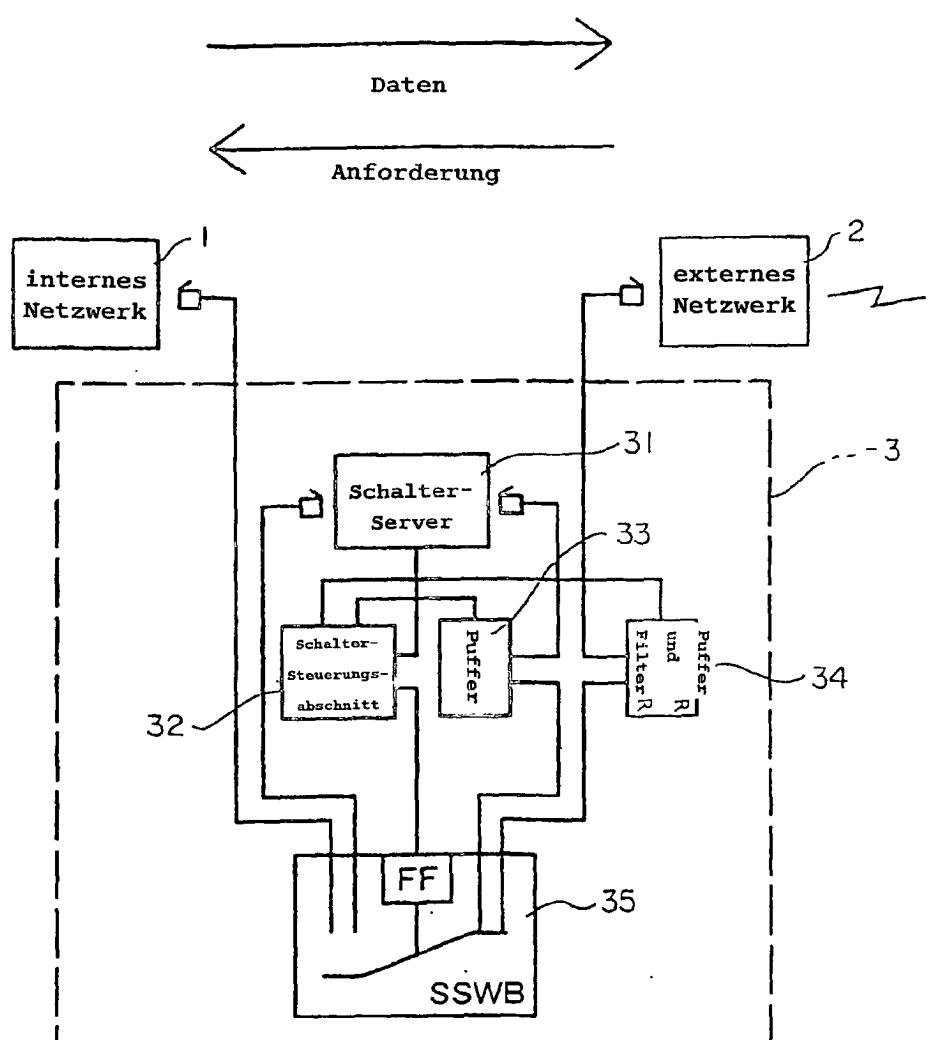


FIG. 3

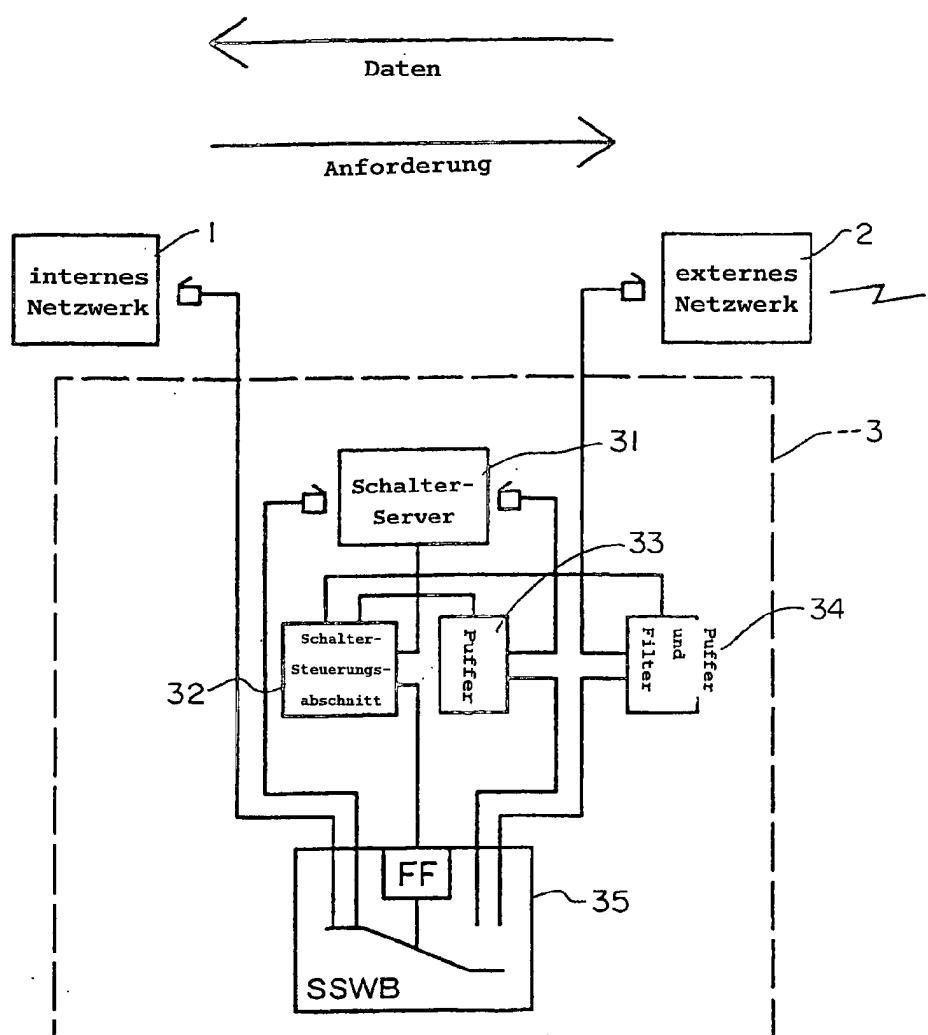


FIG. 4

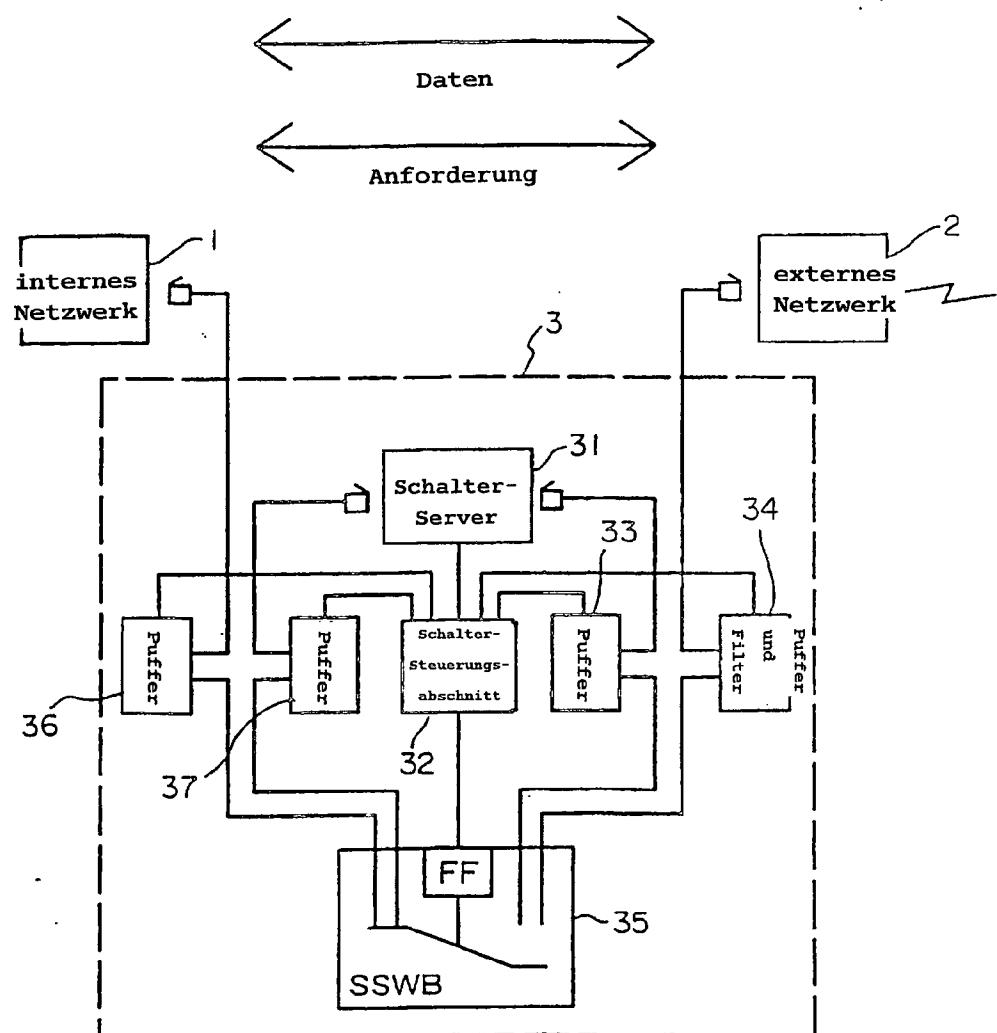


FIG. 5

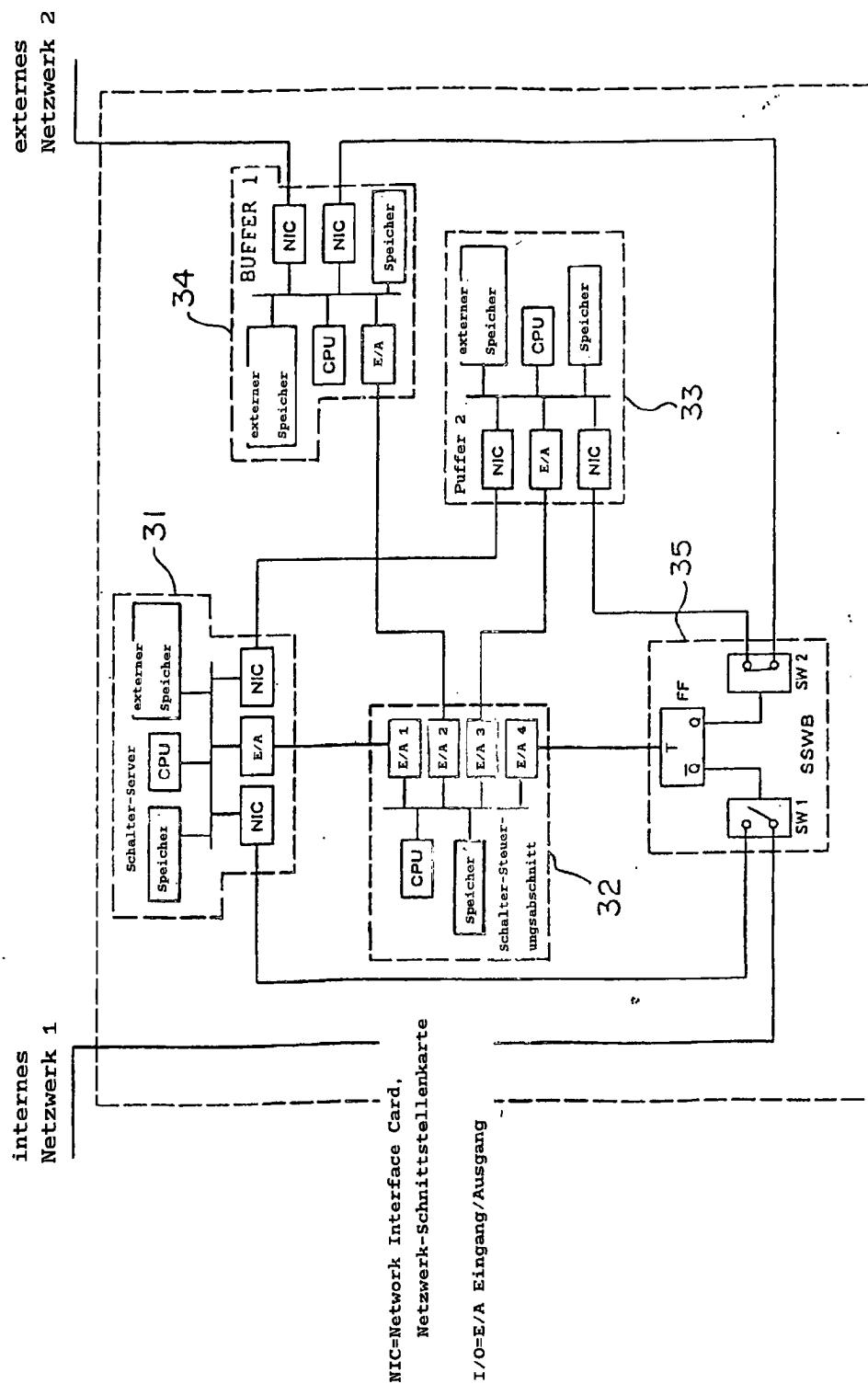
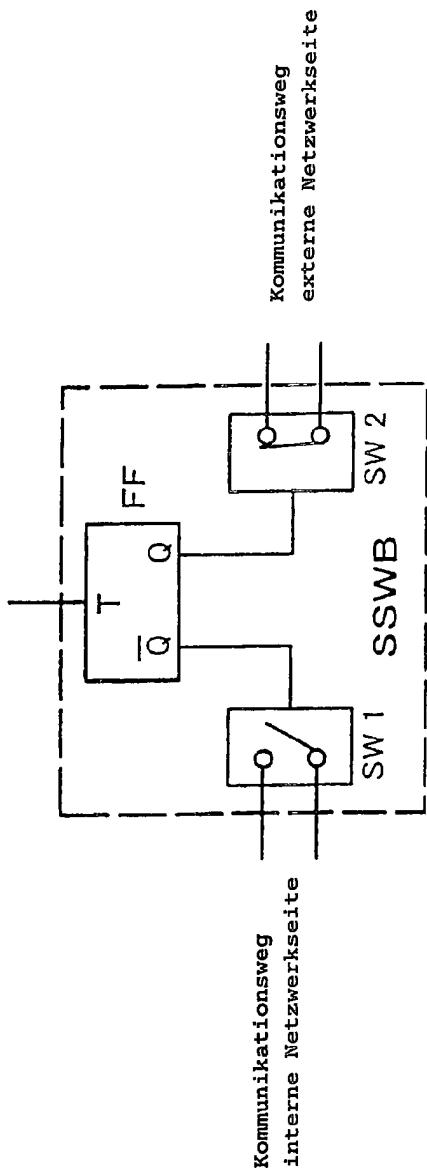


FIG. 6

## Steuersignalweg von Schalter-Steuerungsschnitt



Wahrheitstabelle für Trenn-Flip-Flop-Element,  
das SW1 und SW2 steuert

T	$Q$	$\overline{Q}$
0	keine Änderung	
1	invertiert	

FIG. 7

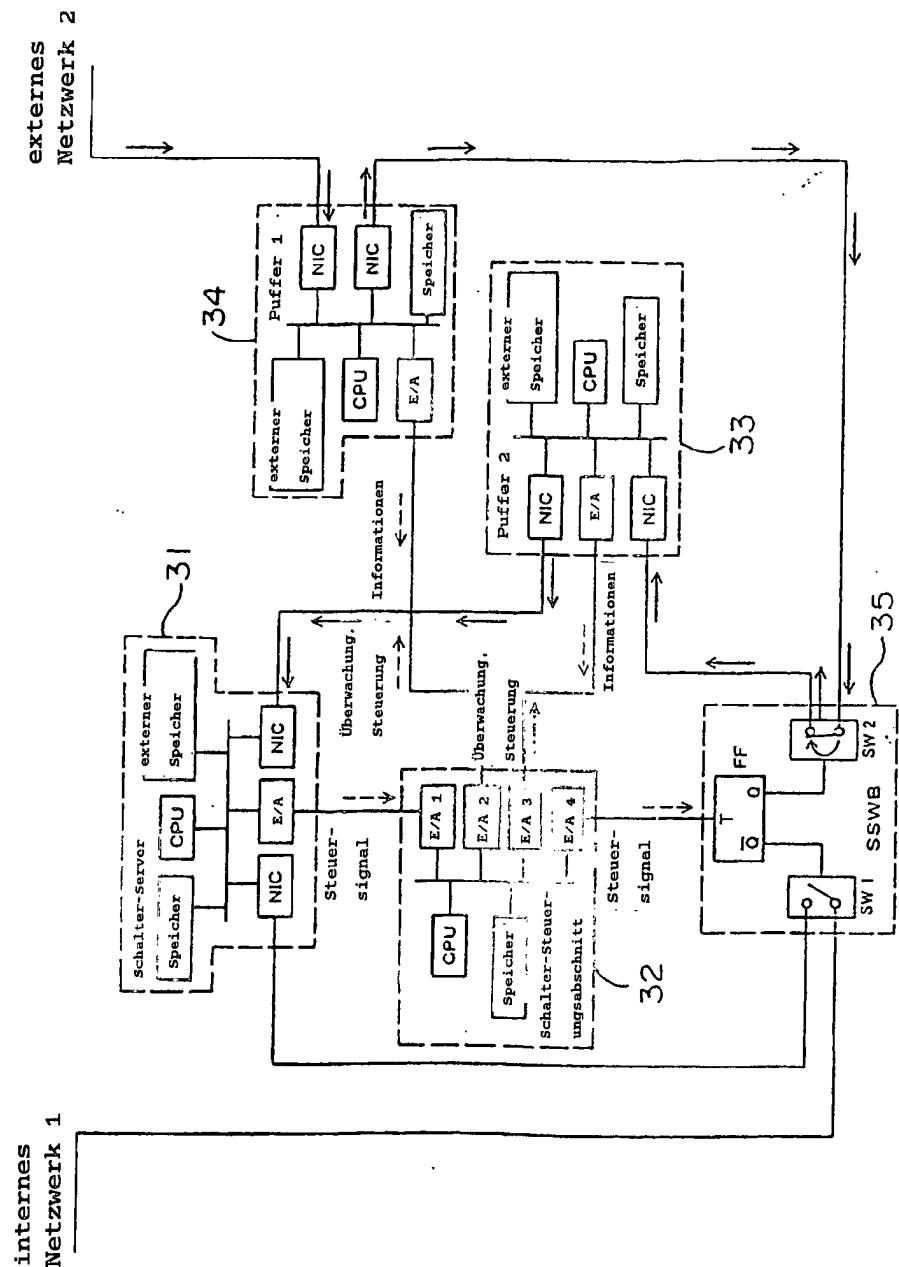


FIG. 8

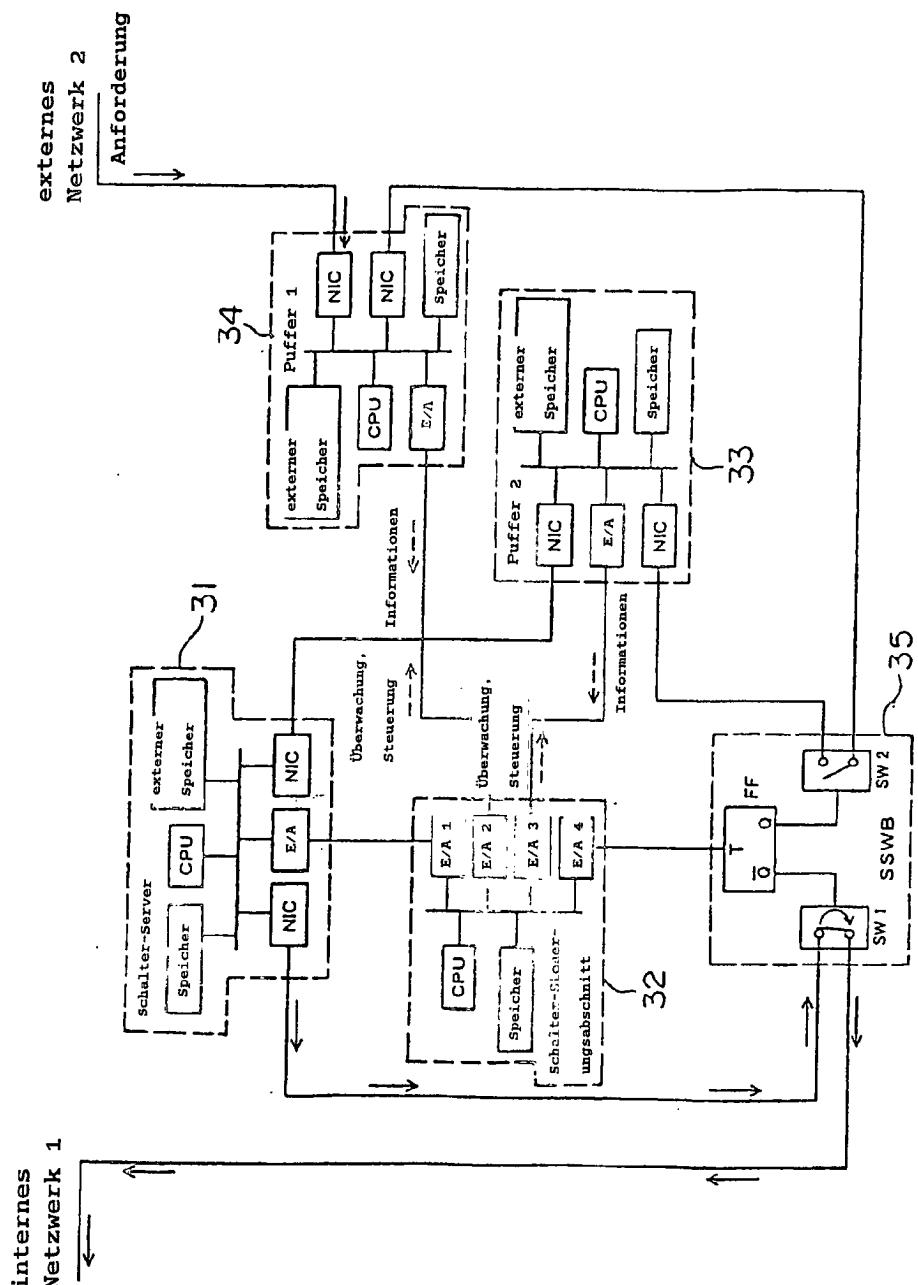


FIG. 9

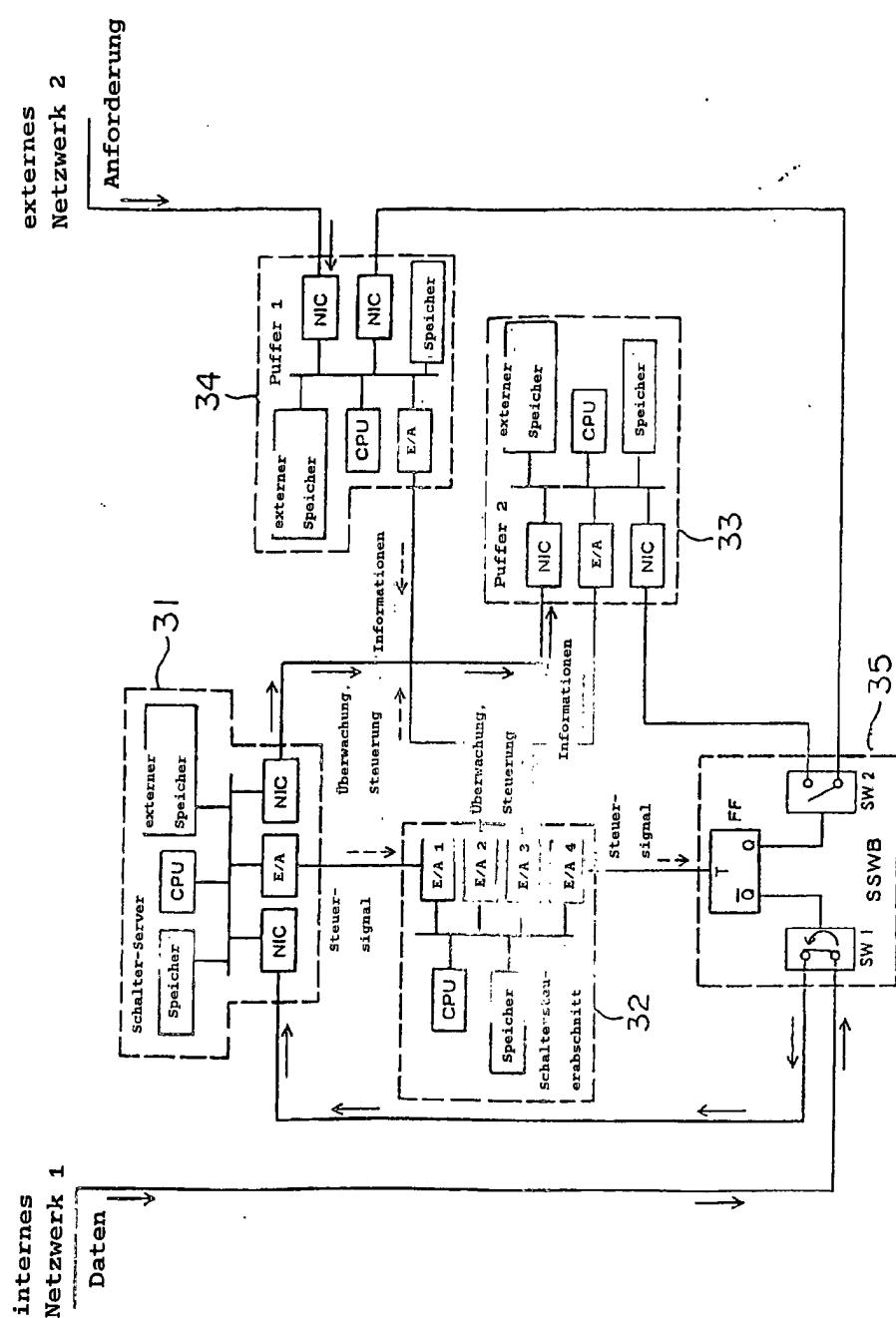


FIG. 10

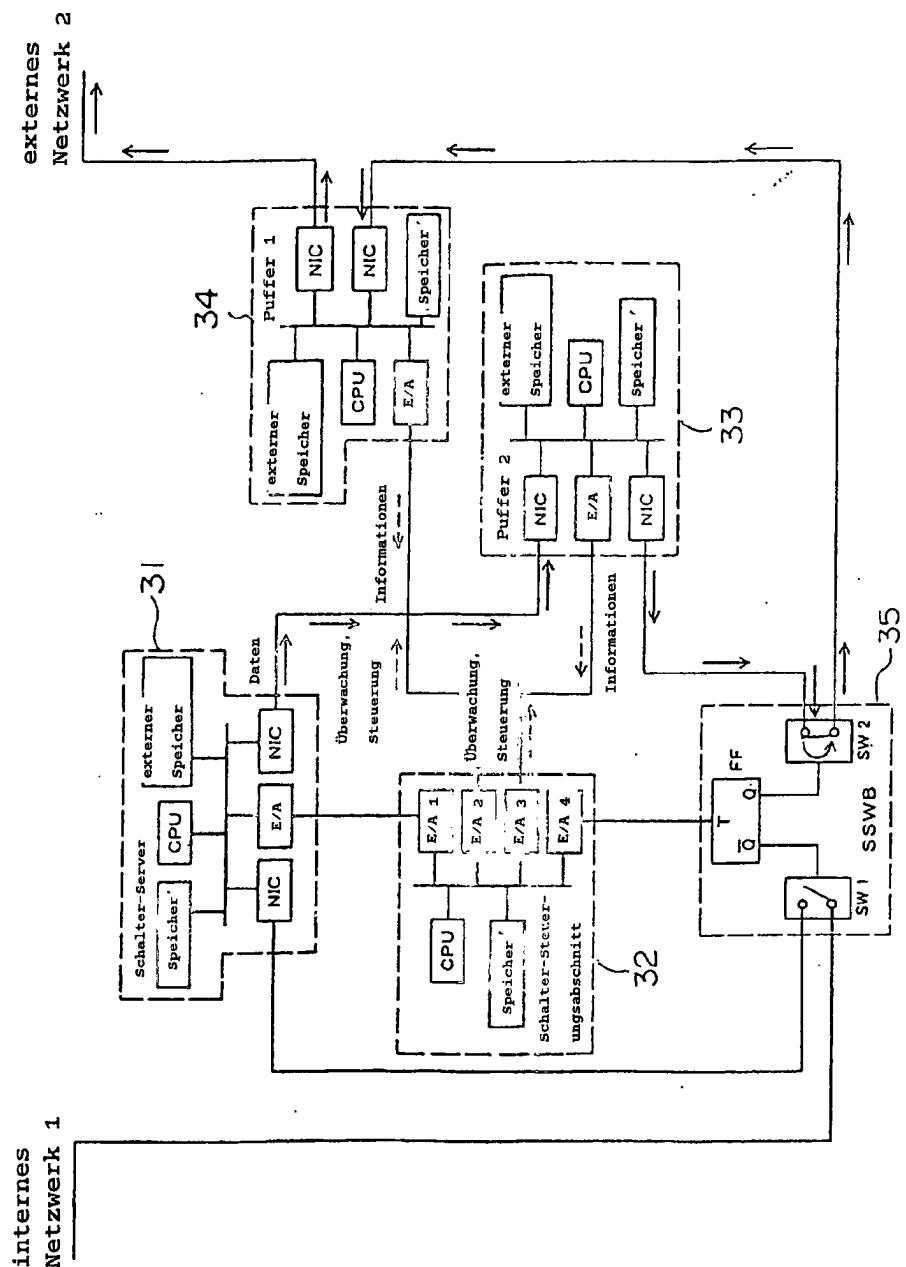


FIG. 11

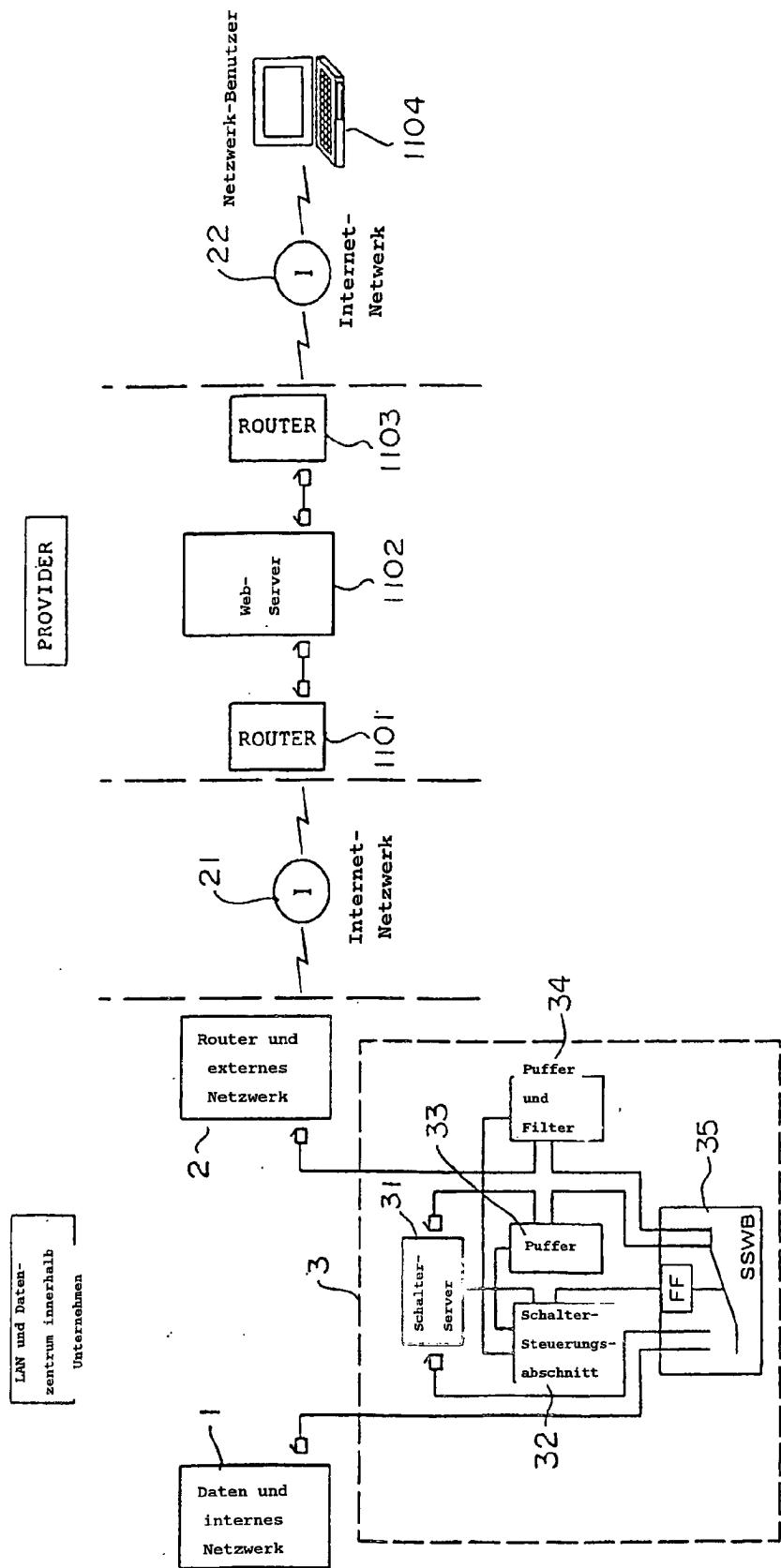


FIG. 12

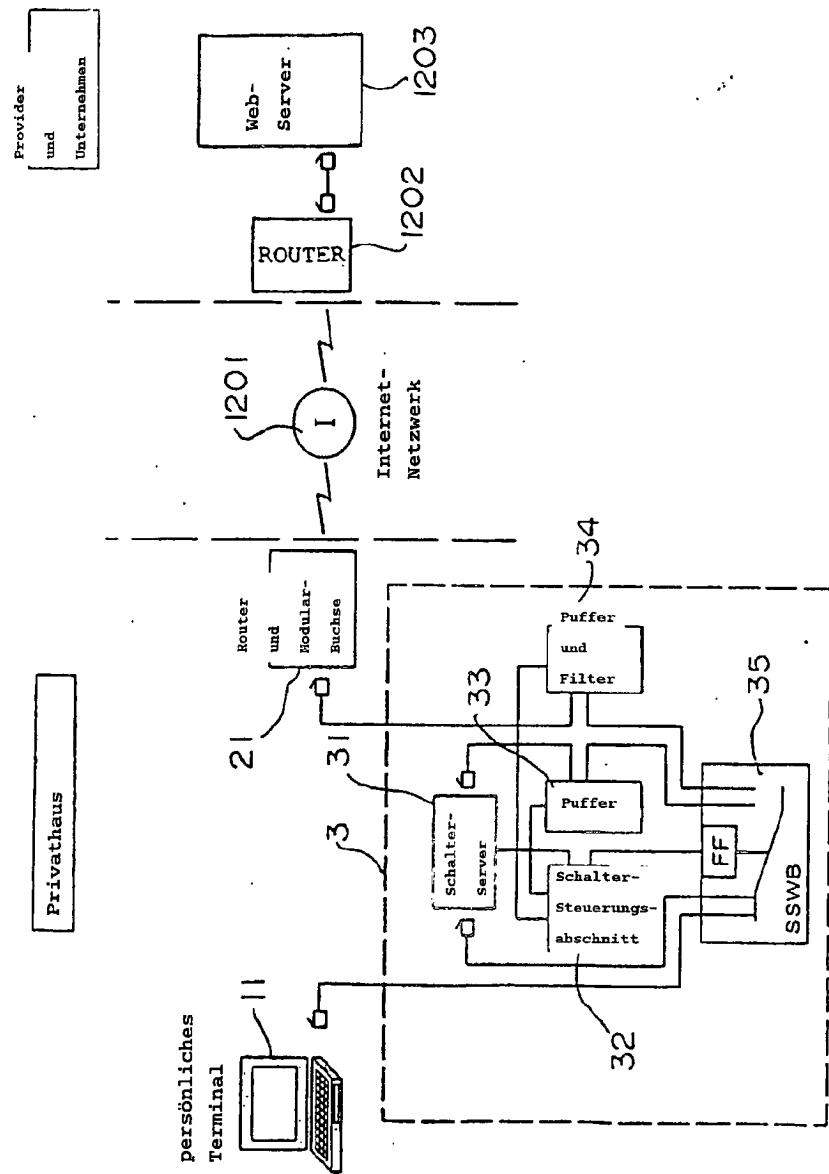


FIG. 13

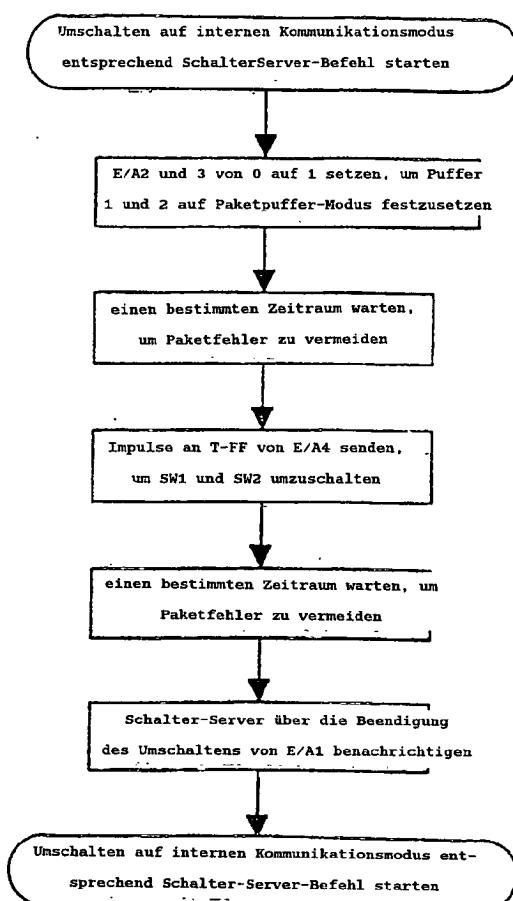


FIG. 14

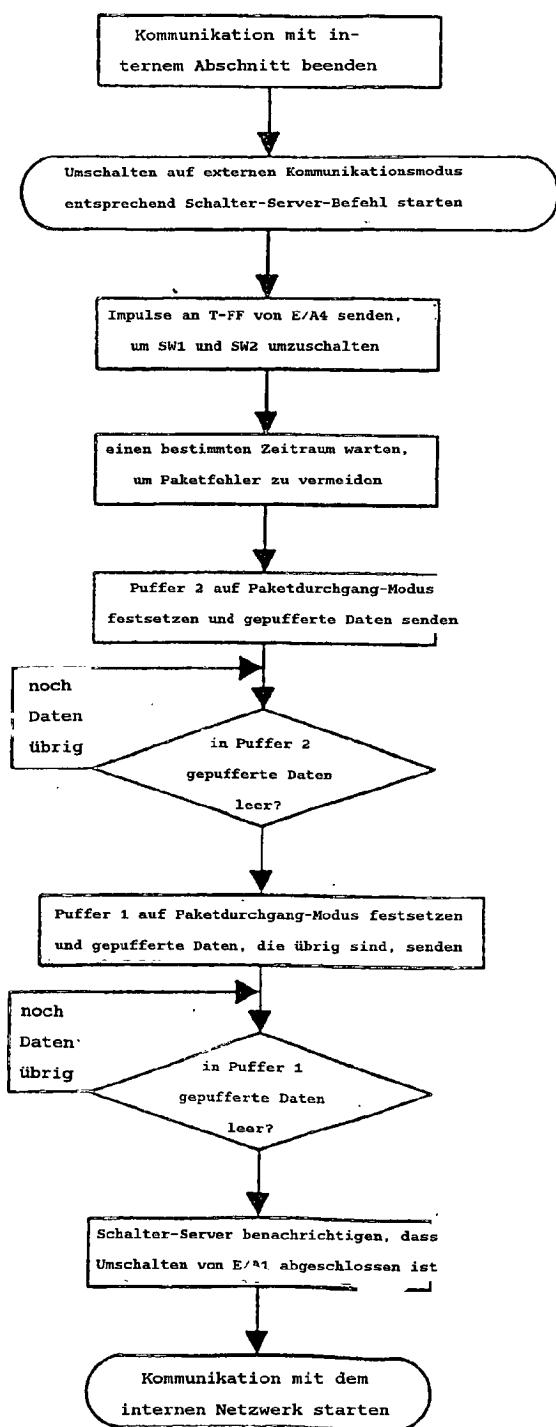


FIG. 15

