(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3885573号
(P3885573)
(45)発行日　平成19年2月21日(2007.2.21)　(24)登録日　平成18年12月1日(2006.12.1)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	A
H04L 12/46	(2006.01)	H04L	12/46	E

請求項の数 3　(全 12 頁)

(21)出願番号　特願2001-369451 (P2001-369451)
(22)出願日　平成13年12月4日 (2001.12.4)
(65)公開番号　特開2003-169097 (P2003-169097A)
(43)公開日　平成15年6月13日 (2003.6.13)
審査請求日　平成16年11月29日 (2004.11.29)

前置審査

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　日高　稔
東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内
(72)発明者　長坂　充
東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内
(72)発明者　塚田　徳
神奈川県横浜市戸塚区戸塚町２１６番地
株式会社日立製作所通信事業部内

最終頁に続く

(54)【発明の名称】パケット処理方法および装置

(57)【特許請求の範囲】
【請求項１】
入力されたパケットから該パケットが構成するパケットフローの特性を示す識別情報を抽出する処理工程選択部と、
あらかじめ上記識別情報と上記パケットに施すべき処理の組をデータとして保有する処理選択テーブルと、
上記処理工程選択部で抽出された識別情報をキーとして上記処理選択テーブル情報を検索するテーブル検索部と、
上記テーブル検索結果に従って上記パケットに処理を施す複数のパケット処理部と、
上記処理されたパケットを送出する転送先選択部と
を有するパケット処理装置であって、
上記複数のパケット処理部は、パケットに施す処理毎に独立した複数種類のパケット処理部であり、
上記識別情報にトランスポート層の情報を含み、
上記処理工程選択部において、入力パケットのデータリンク層ヘッダ情報から入力データリンク層識別子を、ネットワーク層ヘッダに含まれる情報から入力ネットワーク層識別子を、トランスポート層ヘッダに含まれる情報から入力トランスポート層識別子を抽出し、上記入力ネットワーク層識別子および上記入力トランスポート層識別子を検索キーとして上記処理選択テーブルの検索を行うことで、出力ネットワーク層識別子、トランスポート層状態、パケット通過条件、処理識別子および出力データリンク層識別子を得、

上記トランスポート層状態は、上記入力トランスポート層識別子毎のトランスポート層パケットの到着履歴であること特徴とするパケット処理装置。
【請求項２】
上記パケットフローの入力された入力回線に基づいて、上記処理の選択を行うことを特徴とする請求項１記載のパケット処理方法。
【請求項３】
上記パケットデータに施される処理は、カプセル化、デカプセル化、暗号化、復号化、圧縮および伸張のうちから選択される少なくともいずれか一つであることを特徴とする請求項１記載のパケット処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本願発明は、通信網、特にパケット交換網を構成する通信機器に関する技術分野に関するものである。特に、通信網におけるパケット転送の際にオーバーヘッドなくパケットに処理を施しうる技術に関する。パケットに施される処理としては、情報を秘匿するための暗号化、圧縮、カプセル化などがある。
【０００２】
【従来の技術】
図10にパケット転送装置をノードとする通信網の構成例を示す。一般に通信網は、端末（T1,T2,T3,T11など）とノードにより構成される。図10の楕円は複数ノードからなる通信網を表現している。通信の端点として端末同士は通信を行う。通信は端点間をノードで連絡することで、直接接続されていない端末間でも行うことができる。ノードは端末あるいは他のノードとの通信を中継する。通信網の通信を中継する規約がIETF(Internet Engineering Task Force)が定めるインターネットプロトコルに従う通信網をインターネットINと呼ぶ。インターネットINでは、管理者が異なる通信網が相互に接続することにより構成されている。インターネットINのように、管理者が異なるノードからなる網上の通信が広く行われるようになり、管理上、安全性、あるいは運用性の面から端末が属する網の管理者のノードとそれ以外のノードを区別する必要がある。管理者が異なる網間を接続するノードを以下ではエッジノードあるいはエッジルータと呼ぶ。
【０００３】
インターネットINを構成する網は、専ら電気通信事業者が管理し不特定多数の利用者の接続を受け入れる網と、利用者が管理しあるいは管理権限を持ち利用者が接続する網がある。後者を以下プライベート網と呼ぶ。前者には専らインターネット接続サービスを利用者に提供する管理者の網と専ら回線接続サービスを利用者に提供する管理者の網とがある。インターネット接続サービスを利用者に提供する管理者の網を以下ISP網ISP1,ISP2などと呼ぶ。
回線接続サービスを利用者に提供する管理者の網を以下コア網CN1,CN2などと呼ぶ。以下では各網のエッジルータは、プライベート網エッジルータPE1,PE2、ISP網エッジルータER1,ER2、コア網エッジルータCE1,CE2のように呼ぶ。
プライベート網がインターネットに接続する形態は、プライベート網PN1のようにISP網ISP１に直接接続する形態と、プライベート網PN2のようにコア網CN1を介してISP網ISP2に接続する形態とがある。
以上のようなネットワーク上を、データはパケットの形で転送されている。パケット転送方式および装置において、データリンク層の情報、ネットワーク層の情報、トランスポート層の情報など、ネットワークモデル（International Standard Organizationの定めるOSI参照モデル）上で複数層にまたがる情報をパケット転送処理に利用している。
図４にパケットの例を示す。パケットは、トランスポート層データTL_DATAにトランスポート層ヘッダTLHを付加したものがネットワーク層データNL_DATAとなり、ネットワーク層データNL_DATAにネットワーク層ヘッダNLHを付加したものがデータリンク層データDL_DATAとなり、データリンク層データDL_DATAにデータリンク層ヘッダDLHとデータリンク層プ

ロトコルによってはデータリンク層トレーラDLTを付加したものがデータリンク層パケットに成ると云うように入れ子構造に構成される。データリンク層パケットはフレームFLとも呼ばれる。
この入れ子構造をとることをカプセル化と呼ぶ。カプセル化とは一般に、階層化されたネットワークシステムの中で、ある層のプロトコルで扱うパケット、あるいはフレーム全体を、別のプロトコルのヘッダ情報を付加することで、ペイロードとして扱う手法をいう。逆にヘッダを削除し包まれたデータを取り出すことをデカプセル化と呼ぶ。
【０００４】
パケット転送を行う際の処理には、ノードが該当する層のヘッダ処理を行うだけでこと足りる場合とパケットデータ全体を処理する必要がある場合とがある。ヘッダ処理の例は、ネットワーク層の経路選択である。この場合、ネットワーク層ヘッダを処理することで出力先を決定できる。一方、パケット全体の処理を必要とする場合があり、その例は、パケットの暗号化、復号化、カプセル化あるいはデカプセル化などである。
【０００５】
また、プライベート網は、トンネリング技術を用いて仮想的に接続することもできる。ここでトンネリングの為のカプセル化を説明する。トンネリングとは、図１を例として説明すると、端末T１と端末T3が通信するパケットをエッジルータPE1とエッジルータPE3が通信するパケットにカプセル化することで、端末が通信するパケットは図１の破線で示した経路のエッジルータPE1とPE3間の経路を仮想的に接続された経路と見なす方式である。この仮想的に接続された経路はトンネルTN1と呼ばれる。トンネリングの具体的な方式は、新たなヘッダによりパケットをカプセル化することにより被カプセル化パケットの処理層の処理を新たなヘッダによる転送処理で行うことである。図１の例の場合、トンネリングとは、エッジルータPE1が、端末T1が送信したパケットに新たなネットワーク層ヘッダを付加し、その付加したネットワーク層ヘッダの情報による転送で到着するエッジルータPE3が、エッジルータPE1が付加したヘッダを削除し端末T1が送信したパケットを取り出すことである。
【０００６】
図５にネットワーク層のパケットをネットワーク層でカプセル化するパケット構成例を示す。カプセル化では、図４で示したネットワーク層ヘッダNLHを持つデータリンク層データDL_DATAであるパケットを新たなネットワーク層データT_NL_DATAとし、新たなネットワーク層ヘッダT_NLHを付加し、その部分が新たなデータリンク層データDL_DATA2と成る。このデータリンク層データDL_DATA2はデカプセル化されるまで、このネットワーク層ヘッダT_NLHの情報を基にしたネットワーク層のパケットとして処理される。デカプセル化では、このネットワーク層ヘッダT_NLHの情報を基にして到着した宛先ノードでネットワーク層ヘッダT_NLHが削除され、そのネットワーク層データT_NL_DATAがもとのネットワーク層のパケット、つまりもとのデータリンク層データDL_DATAとして復元される。復元されたデータは、ネットワーク層ヘッダNLHの情報でネットワーク層のパケットして転送される。
【０００７】
端末が通信する場合、トランスポート層より下位層で送受信するデータは個々のパケットであるが、セッション層より上位層で送受信するデータは連続したパケットから成るパケット群である。このパケット群を以下パケットフローと呼ぶ。
【０００８】
【発明が解決しようとする課題】
図１のネットワークを上記パケットフローが転送される際に、データの内容秘匿のための暗号化技術が重要となる。
【０００９】
従来、IETFが発行するRequest For Comments(RFC)2406 IP Encapsulating Security Payloadで行われているように、暗号化処理は、パケットフロー毎に端末上の応用プログラムが個別に処理したり、またはノードが暗号化を行っていた。暗号化にはパケットのデータ

部を暗号化する場合と、トンネリング（カプセル化）を行い、プライベート網内の転送情報であるネットワーク層ヘッダも含めたパケットデータ全体を暗号化する場合がある。パケットデータ全体を暗号化するのは、インターネットではパケットは管理者が特定できない経路を通過するため経路の安全性や経路情報の秘匿性を守る観点から、端末が属するプライベート網内のネットワーク層ヘッダ内の転送情報を、パケットが通過する経路のノード上でパケットを認識可能な者から秘匿する必要があるためである。

【００１０】

図5と図6を用いて、暗号化のためにパケットをカプセル化する例を説明する。図６に暗号化したトンネリングの為にネットワーク層ヘッダも含めて暗号化されたパケットの構成例を示す。カプセル化されたパケットT_NL_DATAがISP網をトンネルして通過するために必要な処理として、新たなネットワーク層ヘッダT_NLHがカプセル化ヘッダとしてパケットに付加される。暗号化の場合、カプセル化されるデータT_NL_DATAは、暗号化されたカプセル化データENCRYPTEDとして暗号化される。このようにプライベート網内のアドレス情報を持つネットワーク層ヘッダNLHは暗号化され、ISP網内で通過するノードでは暗号化されたデータENCRYPTEDとして転送されるので、第三者がネットワーク層ヘッダNLHの値を得ることは困難である。

【００１１】

パケットは、パケットフローとしてノードを通過する。従来のパケット転送装置で暗号化あるいは復号化を行う場合、対向パケット転送装置までの経路上を通過するパケットフロー毎に処理を行っている。またこの場合、エッジノードは、トンネル経路すなわちパケットを復号化する相手エッジノードまでの経路を通過するパケットを一様に暗号化していた。

このような従来のパケット転送装置においては、パケットフローを生成した端末を識別してパケットフロー中の暗号化あるいは復号化の要否を判断し、暗号化が必要なパケットのみに暗号化処理することは行っていない。

パケット転送装置をエッジノードとした場合、そのエッジノードが属する網のパケットフローが集中して通過する。エッジノードがパケットヘッダ処理に比較して計算量の多い暗号化処理を実行する場合、パケットフローが集中するノードでは計算による遅延でパケットの処理量が制限される。そこでパケットの処理量を効率化する必要がある。

【００１２】

【課題を解決するための手段】

そこで本発明のパケット転送装置では、パケットフロー毎に利用者あるいは処理内容を識別する識別手段を具備する。またパケットフロー状態を識別してパケットフローを構成するパケットデータへの処理を変更あるいは選択する手段を具備する。また暗号化などパケットに施す処理の要否を判断する手段を具備する。またパケット転送処理において、パケット情報、装置の内部状態に従って処理を変更することが可能な手段を具備する。

【００１３】

識別手段は、入力パケットが持つヘッダ情報から宛先情報等を抽出し、その入力パケットが構成するパケットフローの状態を把握する処理判別部と判別部の結果を保持したテーブル情報検索部とパケットに施す処理を決定する部分とパケットに施す処理ごとに専用処理部を有する。

【００１４】

より具体的には、本発明のパケット処理方法では、入力されたパケットフロー毎にパケットフローを構成するパケットデータに施される処理を選択し、パケットデータに選択された処理を施す。処理の選択は、パケットフローの入力された入力回線に基づいて、あるいは、パケットデータに含まれる識別子に基づいて、行うことができる。具体的には、パケットフローが入力される入力回線やパケットデータに含まれる識別子と、選択すべき処理内容とが対応付けされたテーブルを参照することにより、処理の選択を行う。パケットデータに施される処理は、例えばカプセル化、デカプセル化、暗号化、復号化、圧縮および伸張等種々の処理のうちから選択される一つ、あるいは、これらの組み合わせである。

本発明によるネットワークシステムは、複数の通信網と、各通信網に属する端末と、通信も間を中継するエッジノードを有し、端末間をパケットフローがエッジノードを介して通信され、エッジノードはパケットフローの特性（例えば利用者、送信元、受信先、要求される処理など）に応じて、選択的にパケットフローに処理を施す。処理の典型例は、暗号化である。暗号化にはデータ部分のみの暗号化とカプセル化を含む。
さらに本発明になるエッジノードの構成としては、入力されたパケットからそのパケットが構成するデータフローの特性を示す識別情報を抽出する処理工程選択部と、あらかじめ識別情報とパケットに施すべき処理の組をデータとして保有する処理選択テーブルと、処理工程選択部で抽出された識別情報をキーとして処理選択テーブル情報を検索するテーブル検索部と、テーブル検索結果に従ってパケットに処理を施す独立したパケット処理部と、処理されたパケットを送出する転送先選択部を有するパケット処理装置を備える。入力されたパケットが持つヘッダ情報からそのパケットが構成するデータフローの特性を示す識別情報を抽出ができる。これは例えば、送信元アドレスや宛先アドレス等の利用者情報である。

【００１５】

別の例としては、入力されたパケットの発信元を判定する処理工程選択部と、あらかじめ識別情報とパケットに施すべき処理の組をデータとして保有する処理選択テーブルと、処理工程選択部で判定された発信元をキーとして処理選択テーブル情報を検索するテーブル検索部と、テーブル検索結果に従ってパケットに処理を施す独立したパケット処理部と、処理されたパケットを送出する転送先選択部を有するパケット処理装置である。ここで、パケットが入力された入力回線をパケットの発信元として判定したり、入力されたパケットが持つヘッダ情報からそのパケットの発信元を判定したりすることができる。

【００１６】

【発明の実施の形態】

図２により本発明を適用したパケット転送装置すなわちエッジノードの構成例を説明する。エッジノードとは例えば、図１のプライベート網エッジルータPE1,PE2、ISP網エッジルータER1,ER2、コア網エッジルータCE1,CE2などである。エッジノードは、装置外部から図5、図6に示すデータリンク層のパケットを受信する入力回線を収容した入力回線インタフェース30-1,30-nと装置外部へデータリンク層のパケットを送信する出力回線を収容した出力回線インタフェース50-1,50-nと、入力回線インタフェースが受信したデータリンク層のパケットを処理する入力処理部13-1,13-mと、入力処理部から出力処理部へ装置内でデータを転送するスイッチ部12と、送信するデータリンク層のパケットを処理する出力処理部14-1,14-mと、これらを制御する制御部11から成る。入力回線、出力回線、入力回線インタフェース、出力回線インタフェース、入力処理部、出力処理部、スイッチ部、制御部はパケット転送装置にそれぞれ複数備えることも可能である。

【００１７】

入力回線インタフェース30-1,30-nは、入力回線から入力された物理信号をデータリンク層パケット認識し、データリンク層パケットを入力パケット処理部20へ転送する。

【００１８】

入力パケット処理部20は入力されたデータリンク層パケットを処理し、処理したパケットをスイッチ部12に転送する。スイッチ部12は入力パケット処理部20から転送されたパケットを出力パケット処理部40へ転送する。出力パケット処理部40はスイッチ部12から転送されたパケットを処理し、データリンク層パケットとして出力回線インターフェース50-1,50-nへ転送する。

【００１９】

出力回線インタフェース50は、出力パケット処理部40から転送されたデータリンク層パケットを受信し出力回線へ適した物理信号に変換して出力する。

【００２０】

図３により入力パケット処理部20と出力パケット処理部40の構成例を説明する。入力パケット処理部20は、少なくとも一つの演算装置CPUと記憶装置MSと複数の入出力装置205から

なる。入出力装置205は、演算装置CPU1、演算装置CPU2等、あるいは記憶装置MSと、入出力回線インターフェース、スイッチ部あるいは制御部とを、バスあるいはクロスバースイッチにより接続する。本実施例の入力パケット処理部20と出力パケット処理部40は類似の構成であり、連携してパケットを処理する。

【００２１】

図９に本発明を適用したパケット転送装置の論理構成図を示す。これらの構成は、図３の一つあるいは複数のCPU1，CPU2上のデータ処理及び記憶装置MSによって実現することができる。しかし、すべてハードウエア構成とすることもできる。本方式は、入力インタフェース部あるいはスイッチ部から入力されたパケットが持つヘッダ情報を抽出し、そのパケットが構成するデータフローの状態を把握する処理工程選択部100とテーブル情報の更新の管理を行うテーブル管理部101とテーブル情報を検索するテーブル検索部102と通信網内の認証サービスとの間で行う認証処理結果をテーブル管理部へ伝える認証処理部103とテーブル104とテーブル検索結果によりパケットに施す処理毎のパケット処理部300とスイッチ部あるいは出力インタフェース部へパケットを転送する転送先選択部400を有する。

【００２２】

処理工程選択部100では、入力パケットのデータリンク層ヘッダDLH、あるいはトレイラDLTに含まれる情報からデータリンク層識別子IN12を得る。また、ネットワーク層ヘッダNLHに含まれる情報からネットワーク層識別子IN21を得る。また、トランスポート層ヘッダTLHに含まれる情報からトランスポート層識別子IN22を得る(図4、図5、図７、図８参照)。例えばデータリンク層識別子は、データリンク層の送信元アドレス、宛先アドレス、およびセッション識別子である。例えば、RFC2516で示されるPPP over Ethernetでは、入力パケットのデータリンク層ヘッダDLHからセッション識別子が得られる。またネットワーク層識別子はネットワーク層の送信元アドレス、宛先アドレス、上位層プロトコル識別子である。ネットワーク層ヘッダの例は、RFC791で示されるInternet Protocol(IP)である。またトランスポート層で抽出する情報はトランスポート層アドレスやトランスポート層状態フラグである。トランスポート層ヘッダの例は、RFC793で示されるTCPやRFC768で示されるUDPである。入力パケットを発信した端末は、入力回線IN11、データリンク層識別子IN12あるいはネットワーク層識別子IN21により特定する。

【００２３】

テーブル検索部102では、入力処理工程選択部100が入力パケットから抽出した入力情報IN1あるいは入力情報IN2を検索キーにして出力情報を記録したテーブルを検索する。

処理工程選択部100は、テーブル検索部102から得た検索結果すなわち出力情報OUT1と出力情報OUT2に応じ、パケット処理部300へデータ処理を指示する。

【００２４】

図7にデータリンク層ヘッダの情報をパケットフロー識別に利用するテーブルの例を、図８にネットワーク層ヘッダの情報とトランスポート層ヘッダの情報の一方または両方をパケットフロー識別に利用するテーブルの例を示す。

図7の例では、入力パケットから得られた入力回線IN11や入力データリンク層識別子IN12から入力情報IN1が構成される。入力情報IN1を検索キーとし図7に示したテーブルの検索を行うことで出力情報OUT1を得る。出力情報OUT1は、パケットが出力される出力回線OUT11、出力データリンク層識別子OUT12、データリンク層（DL）状態OUT13、パケット通過条件OUT14から構成する。また、処理識別子OUT15によりパケットに行う処理が指定される。

図8の例では、入力パケットから得られた入力ネットワーク（NL）層識別子IN21や入力トランスポート（TL）層識別子IN22から入力情報IN2が構成される。入力情報IN2を検索キーとし図8に示したテーブルの検索を行うことで出力情報OUT2を得る。出力情報OUT2は、出力ネットワーク層（NL）識別子OUT11、トランスポート層（TL）状態OUT22、パケット通過条件OUT23、処理識別子OUT24、および出力データリンク層識別子OUT25から構成する。

図1のプライベート網エッジルータPE1は、入力パケットの発信端末を、入力データリンク層識別子IN12で識別できる。図７の例では、端末T1の通信するパケットであることは、入力処理工程選択部がパケット抽出した入力情報IN1を検索キーとして図7に示したテーブル

を検索することで判断できる。すなわち端末T1の発信したパケットは、入力データリンク層識別子IN12が0002であり、端末T11の発信したパケットは入力データリンク層識別子IN12が0010であるので発信端末が識別できる。
また、図7の例では、端末T1のパケットフローは、認証処理部103が利用者識別した入力回線IN11、入力データリンク層識別子（セッション識別子）IN12毎に、テーブルエントリのDL状態OUT13をデータ通信に変更することで判断できる。出力回線がどの網に接続しているかはテーブルエントリに保持された出力データリンク層識別子（セッション識別子）OUT12から識別する。同様に端末T11の通信するパケットであることも識別できる。そこで端末に応じた処理識別子OUT15を割り当てることにより暗号化の要否の判断を行うことが出来る。

【００２５】
テーブル管理部102は、処理工程選択部100が抽出した情報からデータリンク層状態の変更、パケット通過条件変更を判定し、テーブルエントリに設定する。また、暗号化等の処理の要否を判定し、処理識別子をテーブルエントリに設定する。図7の例では、テーブルエントリのデータリンク層（DL）状態OUT11は、入力データリンク層識別子IN12毎のデータリンク層パケットの到着履歴である。また、図８の例では、トランスポート層(TL)状態OUT21は、入力トランスポート層識別子IN22毎のトランスポート層パケットの到着履歴である。

【００２６】
認証処理部103は、パケット転送装置外部の認証サービス、あるいは図示していないパケット転送装置内部の認証サービスと通信し利用者の認証を行う。入力パケットはそのパケットを生成した利用者情報を含む。利用者情報は、データリンク層識別子やネットワーク層識別子やトランスポート層データに含まれる上位層の情報である。そこで認証処理部は、その利用者情報を認証サービスに送信し、認証結果を受信する。認証処理部は認証結果に従いそのパケットが属するパケットフローのテーブルエントリを登録、抹消、パケット通過条件OUT14の変更の要否をテーブル管理部に通知する。テーブル部はエントリとしてその情報を保持する。

【００２７】
パケット処理部300は、処理識別子により選択されて実行される。
本発明のパケット転送装置をエッジルータとして用いた網の構成例である図1を用いて、パケット処理部300を説明する。第一のプライベート網PN1のエッジルータPE1と第三のプライベート網PN3のエッジルータPE3はコア網CN1を介して第一のISP網ISP1のエッジルータER1と接続し、第二のプライベート網PN2のエッジルータPE2はコア網CN2を介して第二のISP網ISP２のエッジルータER5と接続する。また、プライベート網PN1とプライベート網PN2はトンネルTN2で接続されている。プライベート網１とプライベート網PN3はトンネルTN１で接続されている。

【００２８】
図1を再度参照して、広域ネットワークに於ける本願発明の動作を説明する。図１のプライベート網エッジルータPE1が送信するパケットは、図８のテーブルを用いると、通信相手が図の破線すなわち契約ISP内の暗号化が不要な経路(トンネルTN1)で接続される端末T3である場合、処理識別子OUT15によりトンネリングの為のカプセル化処理301が選択される。通信相手が図の一点鎖線すなわちインターネットINを通過し暗号化が必要な経路（トンネルTN２）で接続される端末T2である場合、処理識別子により暗号化処理部303が選択され、さらにトンネリングの為のカプセル化処理301が選択される。
一方プライベート網エッジルータPE1が受信するパケットは、図８のテーブルを用いると、通信相手が図の破線すなわち契約ISP内の暗号化が不要な経路(トンネルTN1)で接続される端末T3である場合、処理識別子OUT15によりトンネリングの為のデカプセル化処理302が選択される。通信相手が図の一点鎖線すなわちインターネットINを通過し暗号化が必要な経路（トンネルTN２）で接続される端末T2である場合、処理識別子によりトンネリングの為のデカプセル化処理302が選択され、さらに複号化処理部304が選択される。また、パケ

ットにデータ圧縮伸張処理が必要な場合には、圧縮処理部305あるいは伸張処理部306へパケットが転送される。必要な処理が終了するとパケット処理部300は転送先選択部400にパケットデータを送信する。転送先選択部400では、パケットデータをスイッチ部12または出力回線インタフェース50へ転送する。また、処理工程選択部100では、スイッチ部12から転送されたパケットの場合も同様な処理を行う。

【００２９】

図１１により、本発明のパケット転送装置を用い、ISP網側のエッジルータにより、仮想プライベート網VPNを構成する場合の実施例を説明する。この場合、プライベート網内のパケットは、ISP網のエッジルータER２によりカプセル化されトンネル用のパケットとなる。ISP網のエッジルータER２は、ISP網を通過するために必要な新たなネットワーク層ヘッダT_NLHをカプセル化ヘッダとしてパケットに付加する。接続契約しているプライベート網PN1のエッジルータPE1からのパケットはデータリンク層識別子とネットワーク層識別子により端末T1からのパケットであることを認識できる。同様に端末T11からのパケットであることも認識できる。暗号化は、テーブルに保持した処理識別子に従って行う。この場合、インターネット接続サービスを行う事業者は、その事業者の管理するISP網ISP1に接続する利用者に代わって暗号化したトンネリング等の付加価値サービスを行うことが出来る。

【００３０】

【発明の効果】

本発明により、入力パケットの発信端末あるいは利用者を認識することが可能であり、送信先の判定も可能であるので、利用者あるいは処理内容を識別してパケットの処理を変更し、パケットフローを構成するパケット処理を変更しエッジノードを通過するパケットの処理を差別化することが可能である。また、利用者が暗号化を行いたいパケットを選択的に暗号化することができ、利用者毎に暗号化が必要な経路を通過するパケットのみを暗号化することができる。従って、エッジノードで暗号化等の比較的計算量の多い処理を選択的に行うことが可能となる。高速回線を収容したパケット転送装置によりデータフローの暗号化処理を行うことが可能となることで、パケットがプライベート網の管理者以外の管理する網を通過する場合にもプライベート網内の宛先情報が秘匿されるので、プライベート網内の宛先にサービス不能攻撃などの悪意あるアクセスが行い難くなる。

本方式を具備したパケット転送装置の管理者は、利用者毎にパケット処理を差別化したサービスを提供することが可能である。

【図面の簡単な説明】

【図１】本発明によるエッジノードを用いた網の構成例を説明する概念図である。

【図２】本発明によるエッジノードの構成例を説明するブロック図である。

【図３】本発明によるエッジノードのパケット処理部の構成例を説明するブロック図である。

【図４】パケットの構成例を説明する概念図である。

【図５】カプセル化されたパケットの構成例を説明する概念図である。

【図６】カプセル化されデータ部を暗号化したパケットの構成例を説明する概念図である。

【図７】本発明による処理工程選択に用いるテーブル構成を説明する表図である。

【図８】本発明による処理工程選択に用いるテーブル構成を説明する表図である。

【図９】本発明によるエッジノードのパケット処理部の論理構成例を説明するブロック図である。

【図１０】本発明によるエッジノードを用いた網の構成例を説明する概念図である。

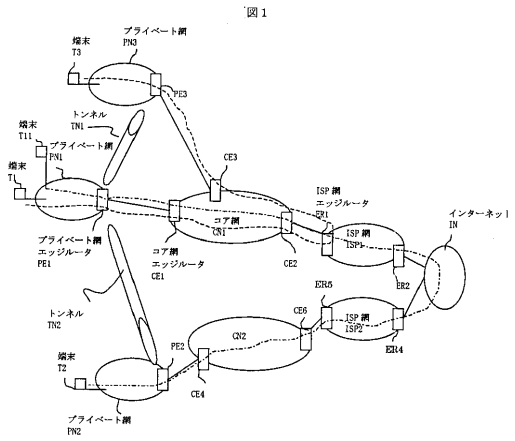
【図１１】本発明によるエッジノードを用いた網の構成例を説明する概念図である。

【符号の説明】

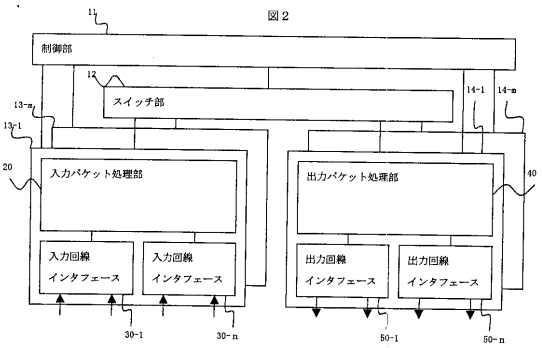
T1…端末、DT1…ダイアルアップ端末、PN1…プライベート網、ISP1…ISP網、CN1…コア網、PE1…プライベート網エッジルータ、ER1…ISP網エッジルータ、CE1…コア網エッジルータ、IN…インターネット、TN1…トンネル、11…制御部、12…スイッチ部、13…入力処理

部、14…出力処理部、20…入力パケット処理部、30…入力回線インタフェース、40…出力パケット処理部、50…出力回線インタフェース、100…入力処理工程選択部、101 DLH…データリンク層ヘッダ、DLT…データリンク層トレーラ、DL_DATA…データリンク層データ、NLH…ネットワーク層ヘッダ、NL_DATA…ネットワーク層データ、T_NLH…ネットワーク層ヘッダ、T_NL_DATA…ネットワーク層データ、TLH…トランスポート層ヘッダ、TL_DATA…トランスポート層データ、FL…データリンク層パケットまたはフレーム。

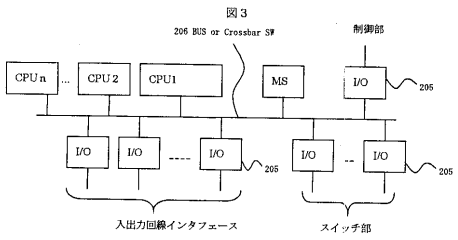
【図１】



【図２】

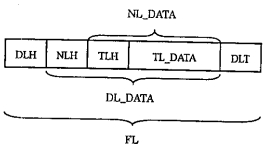


【図３】



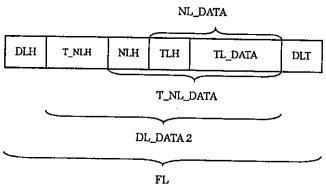
【図４】

図４



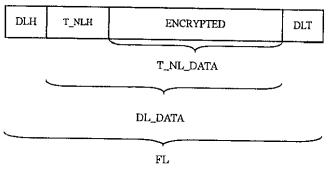
【図５】

図５



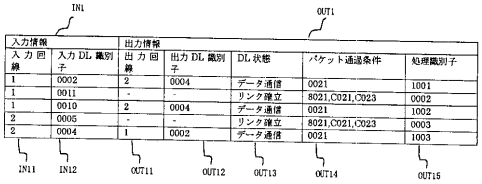
【図６】

図６



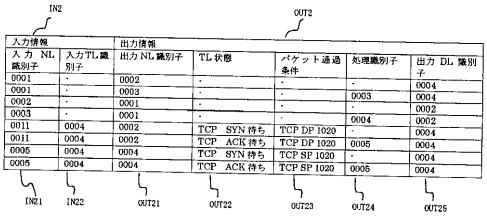
【図７】

図７



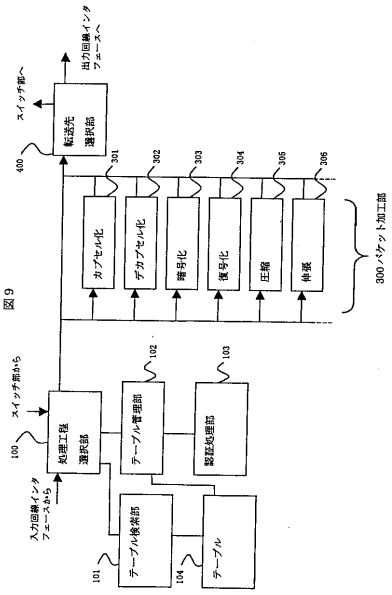
【図８】

図８



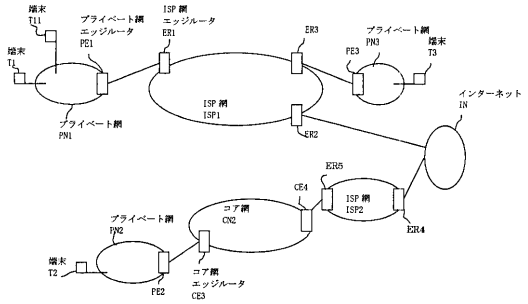
【図９】

図９



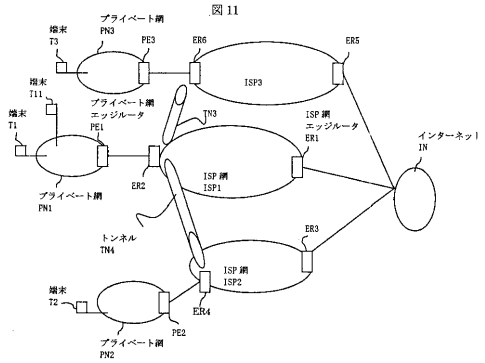
【図１０】

図10



【図１１】

図11



フロントページの続き

審査官　清水　稔

(56)参考文献　特表２００２－５０４２８５（ＪＰ，Ａ）
特開平１１－３３１２６８（ＪＰ，Ａ）
国際公開第９８／０５７４６４（WO，Ａ１）
特開２００１－３２６６９３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/66
H04L 12/46