(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-175866
(P2005-175866A)
(43)公開日　平成17年6月30日(2005.6.30)

(51)Int.Cl.[7]	F I	テーマコード（参考）
H04L 12/56	H04L 12/56 400Z	5K030

審査請求 未請求　請求項の数 10　ＯＬ　（全 22 頁）

(21)出願番号　特願2003-412812(P2003-412812)
(22)出願日　平成15年12月11日(2003.12.11)

(71)出願人　000153465
株式会社日立コミュニケーションテクノロジー
東京都品川区南大井六丁目２６番３号
(74)代理人　100068504
弁理士　小川　勝男
(74)代理人　100086656
弁理士　田中　恭助
(72)発明者　村上　恭朗
神奈川県横浜市戸塚区戸塚町２１６番地
株式会社日立コミュニケーションテクノロジー内

最終頁に続く

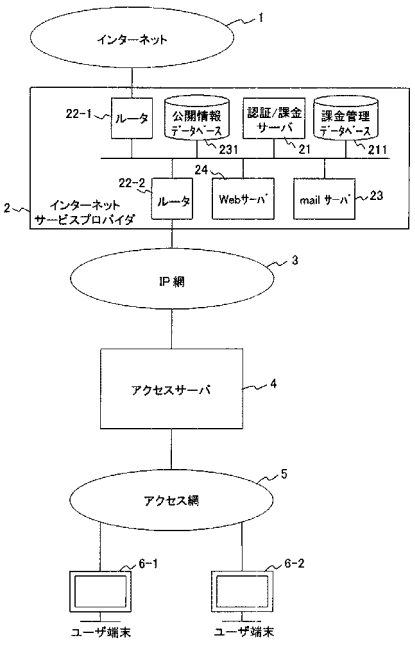
(54)【発明の名称】ネットワーク統計情報サービスシステムおよびインターネットアクセスサーバ

(57)【要約】

【課題】　インターネット利用者が所望する監視情報を自動的に収集して管理できるネットワーク統計情報サービスシステムおよびアクセスサーバを提供する。

【解決手段】ユーザ毎に統計データと統計情報収集条件とを記憶するデータベースを備えたサービスプロバイダシステム２と、ユーザ端末認証時にサービスプロバイダシステムから認証結果と要求元ユーザ識別子、統計情報収集条件および統計パラメータを示す応答パケットを受信し、認証結果に基づいてユーザ端末に応答するアクセスサーバ４とからなり、上記アクセスサーバが、上記応答パケットが示す統計情報収集条件と統計パラメータを記憶しておき、ユーザ端末がインターネットに接続中に、上記統計情報収集条件および統計パラメータに従ってユーザ毎に統計情報を収集し、更新された統計データをサービスプロバイダシステムに通知する。サービスプロバイダシステムは、アクセスサーバからの受信データに基づいて、データベースの統計データを更新しておき、ユーザ端末からの要求に応じて、データベースに蓄積された統計データの少なくとも一部を公開する。

図 1



【特許請求の範囲】
【請求項１】
ユーザ識別子と対応して、統計データとユーザが所望する統計情報収集条件とを記憶するためのデータベースを備えたサービスプロバイダシステムと、
アクセス網を介してユーザ端末から認証要求を受信した時、上記サービスプロバイダシステムに認証要求パケットを送信し、上記サービスプロバイダシステムから、認証結果と要求元ユーザの識別子、統計情報収集条件および収集すべき統計パラメータを示す応答パケットを受信し、該応答パケットが示す認証結果に基づいて上記ユーザ端末に応答するアクセスサーバとからなり、
上記アクセスサーバが、上記サービスプロバイダシステムからの応答パケットが示す統計情報収集条件と統計パラメータをユーザ識別子およびセッション識別子と対応して記憶するための管理テーブルと、上記ユーザ端末がインターネットに接続中に、上記管理テーブルが示す統計情報収集条件および統計パラメータに従って情報を収集し、上記管理テーブルの統計データを更新する統計データ更新手段と、上記更新された統計データを示す更新要求パケットを生成して、上記サービスプロバイダシステムに送信する更新要求生成手段とを有し、
上記サービスプロバイダシステムが、上記アクセスサーバから受信した更新要求パケットの内容に基づいて、上記データベースの統計データを更新しておき、ユーザ端末からの要求に応じて、該ユーザ端末のユーザ識別子と対応して上記データベースに蓄積された統計データの少なくとも一部を公開することを特徴とするネットワーク統計情報サービスシステム。
【請求項２】
前記更新要求生成手段が、ユーザ端末がインターネットに接続中に所定周期で定期的に生成した更新要求パケットと、インターネットへの接続終了に伴う上記ユーザ端末との間のセッション解放時に生成した更新要求パケットを前記サービスプロバイダシステムに送信することを特徴とする請求項１に記載のネットワーク統計情報サービスシステム。
【請求項３】
前記サービスプロバイダシステムが、前記データベースを管理し、前記アクセスサーバからの認証要求パケットおよび更新要求パケットに応答する統計情報管理サーバと、前記ユーザ端末からの要求に応答して統計データ公開のための処理を実行するＷｅｂサーバとからなることを特徴とする請求項１または請求項２に記載にネットワーク統計情報サービスシステム。
【請求項４】
前記更新要求生成手段が、前記統計情報収集条件で予め指定された特定のイベントの発生時に、その旨を示す更新要求パケットを生成して、前記サービスプロバイダシステムに送信することを特徴とする請求項２に記載にネットワーク統計情報サービスシステム。
【請求項５】
前記統計情報収集条件の１つが監視ＩＰアドレスと閾値とを指定しており、前記統計データ更新手段が、上記監視ＩＰアドレスを送信元とするパケット数をカウントし、上記パケット数が上記閾値以上となった時、前記更新要求生成手段が、その旨を示す更新要求パケットを生成して、前記サービスプロバイダシステムに送信することを特徴とする請求項４に記載にネットワーク統計情報サービスシステム。
【請求項６】
前記統計情報収集条件の１つが損失パケット数のカウントを指定しており、前記統計データ更新手段が、ネットワーク輻輳時に発生した損失パケット数をカウントし、前記更新要求生成手段が、輻輳回復時に、上記損失パケット数を示す更新要求パケットを生成して、前記サービスプロバイダシステムに送信することを特徴とする請求項４に記載にネットワーク統計情報サービスシステム。
【請求項７】
前記統計情報収集条件の１つがサービス中断時間のカウントを指定しており、前記統計

データ更新手段が、ネットワーク輻輳によるサービスの中断時間をカウントし、前記更新要求生成手段が、輻輳回復時に、上記サービス中断時間を示す更新要求パケットを生成して、前記サービスプロバイダシステムに送信することを特徴とする請求項４に記載にネットワーク統計情報サービスシステム。

【請求項８】

前記サービスプロバイダシステムが、前記データベースを管理し、前記アクセスサーバからの認証要求パケットおよび更新要求パケットに応答する統計情報管理サーバと、前記ユーザ端末からの要求に応答して統計データ公開のための処理を実行するＷｅｂサーバと、前記アクセスサーバから特定イベント発生に伴う更新要求パケットを受信した時、関係するユーザ端末に上記特定イベントの発生を通知するためのメールサーバとからなることを特徴とする請求項４～請求項７の何れかに記載のネットワーク統計情報サービスシステム。

【請求項９】

ユーザ端末から認証要求を受信した時、サービスプロバイダシステムに対して認証要求パケットを送信し、上記サービスプロバイダシステムから、認証結果と要求元ユーザの識別子、統計情報収集条件および収集すべき統計パラメータを示す応答パケットを受信した時、該応答パケットが示す認証結果に基づいて上記ユーザ端末に応答するインターネットアクセスサーバであって、

上記サービスプロバイダシステムからの応答パケットが示す統計情報収集条件と統計パラメータをユーザ識別子およびセッション識別子と対応して記憶するための管理テーブルと、

上記ユーザ端末がインターネットに接続中に、上記管理テーブルが示す統計情報収集条件および統計パラメータに従って情報を収集し、上記管理テーブルの統計データを更新する統計データ更新手段と、

上記更新された統計データを示す更新要求パケットを生成して、上記サービスプロバイダシステムに送信する更新要求生成手段とを有することを特徴とするインターネットアクセスサーバ。

【請求項１０】

前記更新要求生成手段が、ユーザ端末がインターネットに接続中に所定周期で定期的に生成した更新要求パケットと、インターネットへの接続終了に伴う上記ユーザ端末との間のセッション解放時に生成した更新要求パケットを前記サービスプロバイダシステムに送信することを特徴とする請求項９に記載のインターネットアクセスサーバ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワーク統計情報サービスシステムおよびインターネットアクセスサーバに関する。

【背景技術】

【０００２】

インターネットに代表されるＩＰ（Internet Protocol）ネットワーク上では、ＩＰプロトコルに従ってデータが転送される。ユーザ端末をＩＰネットワークに接続するためのインターネット接続サービスを提供する通信事業者は、インターネットサービスプロバイダ（ＩＳＰ：Internet Service Provider）と言われている。インターネット利用者がユーザ端末をインターネットに接続する場合、以前は、ダイアルアップによってＩＳＤＮ（Integrated Service Digital Network）／電話回線網経由でインターネットサービスプロバイダに接続していたが、近年のブロードバンドの急速な普及に伴い、ＦＴＴＨ（Fiber To The Home）、ＤＳＬ（Digital Subscriber Line）、ケーブルインターネット、無線（ＦＷＡ：Fixed Wireless Access）等の高速アクセス回線網を経由して、インターネットサービスプロバイダに接続することが可能となってきた。

【０００３】

電話回線を利用した従来のインターネット接続では、インターネットサービスプロバイダは、利用者に対してインターネット利用時間に応じて従量制の課金を行っていた。一方、ブロードバンド環境では、インターネットサービスプロバイダは、従来の電話回線を利用した従量制課金とは異なり、利用者に月毎に一定料金を課金する定額制課金を導入している。定額制課金の導入により、インターネット利用者は、料金を気にする必要がなくなり、ユーザ端末をインターネットに常時接続することが可能となってきた。

【０００４】

ところで、インターネットサービスプロバイダは、上述した各種の高速アクセス回線を収容するアクセスサーバを介して、利用者にインターネット接続サービスを提供する。この場合、アクセスサーバとユーザ端末との間の通信プロトコルとしては、ＰＰＰ（Point-to-Point Protocol）が広く利用されている。ＰＰＰは、元来、電話線や専用線などのシリアル回線上でＴＣＰ／ＩＰ等のリンクを提供するために提案されたプロトコルであり、Internet Engineering Task Force（ＩＥＴＦ）においてRequest for Comments（ＲＦＣ）１６６１として標準化されている。

【０００５】

ＰＰＰは、ＯＳＩ参照モデルのデータリンク層で動作するＬＣＰ（Link Control Protocol）と、ネットワーク層で動作するＮＣＰ（Network Control Protocol）とで構成されている。ＬＣＰは、文字通りリンクを制御するためのプロトコルであり、データサイズ、データ圧縮の有無、伝送速度などの通信条件に関するネゴシエーション（折衝）作業を経て２つの通信装置間にデータリンクを確立した後、データリンクの検査および解放のための制御を行なう。ＮＣＰは、ＬＣＰによるデータリンクの確立後に、ネットワーク層の上位プロコトルの選択や、ネットワークアドレスの割り当て／設定等を行なう。ＰＰＰは、ブロードバンド環境下でも広く利用されており、例えば、イーサネット（Ethernet：登録商標名）上で利用するＰＰＰプロトコルとして、ＲＦＣ２５１６で規定されたＰＰＰｏＥ（PPP Over Ethernet）が知られている。

【０００６】

インターネットサービスプロバイダは、利用者に関する情報および統計データを属性（アトリビュート）値としてデータベース化しておき、認証サーバと課金サーバで一元的に管理している。認証サーバと課金サーバは、一般的にＩＰ網を介してアクセスサーバと通信可能となっている。これらのサーバ間通信には、通常、ＲＡＤＩＵＳ（Remote Authentication Dial In User Service）が利用される。ＲＡＤＩＵＳに関する通信プロトコルは、例えば、ＲＦＣ２８６５、ＲＦＣ２８６６、ＲＦＣ２８６９として規定されている。

【０００７】

ＲＡＤＩＵＳは、サーバクライアント方式を採用しており、認証サーバと課金サーバをＲＡＤＩＵＳサーバ、アクセスサーバをＲＡＤＩＵＳクライアントとして動作させることによって、これらのサーバ間での利用者属性値の送受信を実現する。具体的には、ユーザ端末からインターネット接続要求を受信したアクセスサーバは、上記接続要求から抽出したユーザ名とパスワードをＲＡＤＩＵＳ認証プロトコルに従って送信することにより、認証サーバに要求元ユーザ端末が予め契約された正規ユーザか否かを問い合わせる。

【０００８】

認証サーバからユーザ認証の正常終了を示す応答を受信すると、アクセスサーバは、要求元ユーザ端末にインターネットへの接続を許可し、ユーザ端末との間にＰＰＰセッションを確立する。これによって、ユーザ端末は、インターネット上の各種サーバにアクセスすることが可能となる。アクセスサーバは、ユーザ端末にインターネットのアクセスを許可すると、該ユーザ端末（利用者）の課金情報（ネットワーク統計情報）の収集を開始し、ＲＡＤＩＵＳ課金プロトコルに従って、課金サーバに課金情報を送信する。課金サーバは、ユーザ名によって個々の端末利用者を識別し、利用者毎に課金情報を積算して管理する。

【０００９】

上述した課金情報を含む統計監視情報を通信フロー単位で収集するネットワーク監視シ

ステムについては、例えば、特開２００１－２５７７２２号公報に開示されている。
【００１０】
【特許文献１】特開２００１－２５７７２２号公報
【発明の開示】
【発明が解決しようとする課題】
【００１１】
現在、インターネットサービスプロバイダが課金サーバで管理している課金情報は、例えば、各利用者のインターネット接続時間、送受信パケット数、送受信データ量である。定額料金制の常時接続サービスにおいては、これらの課金情報は、ユーザに通知されることもなく、インターネットサービスプロバイダ自身によるネットワークの利用状況把握と、次期ネットワーク設計へのフィードバック情報としての利用に留まっている。
【００１２】
これは、現在のインターネット接続サービスの殆どが、最善を尽くすが、パケット転送に何の保証もしないベストエフォート型の通信サービスを前提としており、インターネットサービスプロバイダにとっては、例えば、インターネット接続サービス提供中に、ネットワーク上での輻輳による一時的なパケット損失が発生したとしても、各利用者に対してパケット損失の発生や損失パケット数の報告義務を負っていないためである。
【００１３】
近年、インターネット接続サービスの競争激化に伴って、インターネットサービスプロバイダは、他のプロバイダとのサービスの差別化を図るために、ＳＬＡ（Service Level Agreement：サービス品質保証制度）を導入するケースが増えている。ＳＬＡサービスとは、一定の通信品質レベルを保証した通信サービスの提供契約を意味しており、通信品質が予め保証した基準を下回った場合、例えば、利用者に対して保証金を支払うなど、利用者毎にきめ細かな契約を結んだインターネット接続サービスである。ＳＬＡサービスの具体的な契約メニューとしては、例えば、通信サービスに異常が発見された時、利用者に規定時間内にサービス障害を伝えることを保証するものや、一定時間（または一定割合［％］）のサービス時間割増を保証するもの等がある。
【００１４】
利用者にＳＬＡサービスを提供するためには、インターネットサービスプロバイダは、従来の課金情報のように、インターネット接続時間や送受信パケット数等の統計情報を管理するだけでは不十分であり、インターネット接続期間中に発生する損失パケット数やサービス中断時間など、従来よりも詳細な統計情報を収集し、これらの情報を利用者毎の新たなネットワーク利用情報として管理する機能が必要となる。
【００１５】
また、ブロードバンドアクセスが普及し、インターネットへの常時接続が恒常化したことに伴って、それまでＷｅｂサーバからコンテンツ情報を受信する立場にあったインターネット利用者の一部が、自らのＷｅｂサーバを所有する情報発信者に変化しつつある。こうした環境下では、インターネット利用者は、新たな統計情報として、インターネットから自分の端末（例えば、利用者が構築したＷｅｂサーバ）へのアクセス状況を示す情報を必要とする。しかしながら、利用者が自分の端末へのアクセス情報を個人的に収集し、管理しようとすると、ネットワークのオペレーションに関する高度のスキルと、専用のネットワーク監視装置の設置が前提となるため、実際には実現困難となる。
【００１６】
本発明の目的は、インターネット利用者が所望する統計情報を自動的に収集、管理し、利用者の公開できるネットワーク統計情報サービスシステムおよびアクセスサーバを提供することにある。
本発明の他の目的は、既存の課金システムの機能を拡張して、インターネット利用者が必要とする統計情報を通知サービスできるネットワーク統計情報サービスシステムおよびアクセスサーバをを提供することにある。
【課題を解決するための手段】

【００１７】
上記目的を達成するため、本発明によるネットワーク統計情報のサービスシステムは、ユーザ識別子と対応して、統計データとユーザが所望する統計情報収集条件とを記憶するためのデータベースを備えたサービスプロバイダシステムと、アクセス網を介してユーザ端末から認証要求を受信した時、上記サービスプロバイダシステムに認証要求パケットを送信し、上記サービスプロバイダシステムから、認証結果と要求元ユーザの識別子、統計情報収集条件および収集すべき統計パラメータを示す応答パケットを受信し、該応答パケットが示す認証結果に基づいて上記ユーザ端末に応答するアクセスサーバとからなり、
上記アクセスサーバが、上記サービスプロバイダシステムからの応答パケットが示す統計情報収集条件と統計パラメータをユーザ識別子およびセッション識別子と対応して記憶するための管理テーブルと、上記ユーザ端末がインターネットに接続中に、上記管理テーブルが示す統計情報収集条件および統計パラメータに従って情報を収集し、上記管理テーブルの統計データを更新する統計データ更新手段と、上記更新された統計データを示す更新要求パケットを生成して、上記サービスプロバイダシステムに送信する更新要求生成手段とを有し、上記サービスプロバイダシステムが、上記アクセスサーバから受信した更新要求パケットの内容に基づいて、上記データベースの統計データを更新しておき、ユーザ端末からの要求に応じて、該端末のユーザ識別子と対応して上記データベースに蓄積された統計データの少なくとも一部を公開することを特徴とする。
【００１８】
更に詳述すると、上記アクセスサーバが備える更新要求生成手段は、例えば、ユーザ端末がインターネットに接続中に所定周期で定期的に生成した更新要求パケットと、インターネットへの接続終了に伴う上記ユーザ端末との間のセッション解放時に生成した更新要求パケットを上記サービスプロバイダシステムに送信することを特徴とする。また、上記サービスプロバイダシステムは、上記データベースを管理し、アクセスサーバからの認証要求パケットおよび更新要求パケットに応答する統計情報管理サーバ（課金サーバ）と、ユーザ端末からの要求に応答して統計データ公開のための処理を実行するＷｅｂサーバとからなることを特徴とする。
【００１９】
本発明のネットワーク統計情報サービスシステムは、上記アクセスサーバの更新要求生成手段が、例えば、統計情報収集条件で予め指定された特定のイベントの発生時に、その旨を示す更新要求パケットを生成して、上記サービスプロバイダシステムに送信することを特徴とする。
具体的に言うと、本発明の１実施例では、上記統計情報収集条件の１つが、監視ＩＰアドレスと閾値とを指定しており、上記統計データ更新手段が、上記監視ＩＰアドレスを送信元とするパケット数をカウントし、パケット数が閾値以上となった時、上記更新要求生成手段が、その旨を示す更新要求パケットを生成して、サービスプロバイダシステムに送信する。
【００２０】
本発明の他の実施例では、上記統計情報収集条件の１つが損失パケット数のカウントを指定しており、上記統計データ更新手段が、ネットワーク輻輳時に発生した損失パケット数をカウントし、上記更新要求生成手段が、輻輳回復時に、損失パケット数を示す更新要求パケットを生成して、サービスプロバイダシステムに送信する。
本発明の更に他の実施例では、上記統計情報収集条件の１つがサービス中断時間のカウントを指定しており、上記統計データ更新手段が、ネットワーク輻輳によるサービスの中断時間をカウントし、上記更新要求生成手段が、輻輳回復時に、上記サービス中断時間を示す更新要求パケットを生成して、前記サービスプロバイダシステムに送信する。
【００２１】
本発明の１つの特徴は、上記サービスプロバイダシステムが、上述した統計情報管理サーバとＷｅｂサーバの他に、上記アクセスサーバから特定イベント発生に伴う更新要求パケットを受信した時、該当するユーザ端末に対して上記イベントの発生を通知するための

メールサーバを備えたことを特徴とする。

【００２２】

本発明によるインターネットアクセスサーバは、ユーザ端末から認証要求を受信した時、サービスプロバイダシステムに対して認証要求パケットを送信し、上記サービスプロバイダシステムから、認証結果と要求元ユーザの識別子、統計情報収集条件および収集すべき統計パラメータを示す応答パケットを受信した時、該応答パケットが示す認証結果に基づいて上記ユーザ端末に応答する機能を備え、上記サービスプロバイダシステムから受信した応答パケットが示す統計情報収集条件と統計パラメータをユーザ識別子およびセッション識別子と対応して記憶するための管理テーブルと、上記ユーザ端末がインターネットに接続中に、上記管理テーブルが示す統計情報収集条件および統計パラメータに従って情報を収集し、上記管理テーブルの統計データを更新する統計データ更新手段と、上記更新された統計データを示す更新要求パケットを生成して、上記サービスプロバイダシステムに送信する更新要求生成手段とを有することを特徴とする。

尚、上記アクセスサーバとサービスプロバイダシステムとの間では、例えば、ＲＡＤＩＵＳプロトコルにおけるアトリビュートを使用して、上述した統計情報収集条件と統計パラメータを送受信する。

【発明の効果】

【００２３】

本発明によれば、インターネット接続中のユーザ端末毎に、予め指定された統計情報収集条件に従ってパケット損失やサービス中断時間等の統計情報を収集し、これを利用者に公開することができ、利用者毎にきめ細かな契約を結んだインターネット接続サービスとネットワーク統計情報サービスが可能となる。

【発明を実施するための最良の形態】

【００２４】

以下、本発明によるネットワーク統計情報サービスシステムの１実施例を図面を参照して説明する。

図１は、本発明によるネットワーク統計情報サービスシステムを含むネットワーク構成図を示す。

【００２５】

図１において、アクセスサーバ４は、ＩＰ網３を介してインターネットサービスプロバイダ２を構成している認証サーバおよび統計情報管理サーバ（以下、課金サーバと言う）と通信可能である。ここでは、認証サーバと課金サーバを一つのサーバ（認証／課金サーバ）２１として示しているが、これらは２つのサーバに分離していても構わない。インターネットサービスプロバイダ２は、認証／課金サーバ２１の他に、インターネット１と接続するためのルータ２２－１と、ＩＰ網３と接続するためのルータ２２－２と、ｍａｉｌサーバ２３と、Ｗｅｂサーバ２４とを備えている。２１１は、認証／課金サーバが管理する課金管理データベース、２３１は、インターネット利用者のメールアドレスと利用者への公開情報となる統計データを蓄積するためのデータベースであり、ｍａｉｌサーバ２３とＷｅｂサーバ２４によって利用される。

【００２６】

ユーザ端末６（６－１、６－２）は、インターネットサービスプロバイダ２に所属する利用者の端末であり、インターネット１に接続する時は、アクセス網５を介してアクセスサーバ４に接続要求を送信する。ユーザ端末６とアクセスサーバ４との間では、ユーザ端末が使用するリンクの確立、ユーザ認証およびＩＰアドレス割当てのためのプロトコルとしてＰＰＰが使用される。アクセス網５としては、例えば、電話交換機網や、ＡＤＳＬ、ＦＴＴＨなどのブロードバンドアクセス網が使用される。

【００２７】

Ｗｅｂサーバ２４は、ユーザ端末からアクセス可能なサーバであり、データベース２３１に蓄積された公開用のネットワーク統計データ（パラメータ情報）をインターネット利用者に提供する。各インターネット利用者は、ユーザ端末６を用いてＷｅｂサーバ２４を

アクセスすることにより、自分の最新のパラメータ情報を取得することができる。Ｍａｉｌサーバ２３は、各インターネット利用者のメールアドレスを管理し、後述するように、特定イベントの発生時、または利用者からの要求に応じて統計データを電子メールで通知する。

【００２８】

図２は、図１に示したネットワーク統計情報のサービスシステムおいて、ユーザ端末６（６－１、６－２）とインターネット１上の目的サーバとがアクセスサーバ４を介して通信するために必要となる主信号系転送プロトコルスタックの１例を示す。

ユーザ端末６とアクセスサーバ４はＰＰＰによって接続されるため、ユーザ端末６のプロトコルスタック６０１とアクセスサーバ４のプロトコルスタック４０１にはＰＰＰが存在する。ＰＰＰより下位レイヤのプロトコルスタックは、アクセス網５のリンク層のタイプによって異なる。図２では、１例として、下位レイヤがイーサネット（Ｅｔｈｅｒｎｅｔ：登録商標名）網の場合のプロトコルスタックを示している。アクセスサーバから目的サーバまでは、プロトコルスタック４０２と１０１が示すように、ＩＰプロトコル（ＩＰｖ４／ＩＰｖ６）に従ってデータが転送される。

【００２９】

図３は、ユーザ認証情報や、統計情報収集条件、収集すべき統計パラメータなどの制御情報の通信に必要となる制御系転送プロトコルスタックの１例を示す。

プロトコルスタック６０２と４１１が示すように、ユーザ端末６とアクセスサーバ４の間では、制御情報がＰＰＰプロトコルによって通信される。一方、プロトコルスタック４１２と２１０１が示すように、アクセスサーバ４と認証／課金サーバ２１の間では、認証情報およびネットワーク統計情報がＲＡＤＩＵＳプロトコルに従って通信される。

【００３０】

ＲＡＤＩＵＳプロトコルでは、後述するように、ＲＡＤＩＵＳアトリビュート（属性値）が規定されており、アクセスサーバ４と認証／課金サーバ２１は、パケットのデータ部（ペイロード部）にそれぞれが必要とするアトリビュートを付与することによって、認証情報、統計情報収集条件、統計系パラメータ、統計データなど、ネットワーク統計情報処理に必要な制御情報を互いに送受信することが可能となる。

【００３１】

図４は、アクセスサーバ４のハードウェア構成の１例を示すブロック図である。

アクセスサーバ４は、サーバ全体の制御を行なう制御処理部４４と、パケットを所定の回線に出力するためのスイッチ（ＳＷ）部４３と、データリンク層やその上位層であるＩＰプロトコルを処理する複数のプロトコル処理部４２（４２－１～４２－ｎ）と、それぞれ接続回線の種別に応じた物理層終端機能を備えた複数の回線インタフェース（ＩＦ）４１（４１－１Ａ～４１－ｎＢ）とからなる。ここで、回線インタフェース４１－１Ａ、４１－２Ａ、…４１－ｎＡは入力回線用のインタフェース、回線インタフェース４１－１Ｂ、４１－２Ｂ、…４１－ｎＢは出力回線用のインタフェースを示している。

【００３２】

図５は、制御処理部４４の１実施例を示すブロック図である。

制御処理部４４は、データプロセッサ（ＣＰＵ）４４１と、メモリ５０と、プロトコル処理部４２と通信するためのプロトコル処理部インタフェース（ＩＦ）４４３と、スイッチ部４３と通信するためのＳＷ部インタフェース４４４と、外部に設置された制御端末と通信するための制御端末インタフェース４４２とで構成される。ＣＰＵ４４１は、メモリ５０に用意されている各種のプログラムを実行する。

【００３３】

メモリ５０には、本発明に関係するプログラムとして、例えば、ＣＬＩ（Command Line Interface）処理ルーチン５１と、ルーティングプロトコル処理ルーチン５２と、警報監視処理ルーチン５３と、ＰＰＰプロトコル処理ルーチン５４と、ＲＡＤＩＵＳプロトコル処理ルーチン５５が記憶され、インターネット利用者毎に個別の統計情報を収集するために参照されるＰＰＰユーザ管理テーブル５６が形成されている。

【００３４】
ＣＬＩ処理ルーチン５１は、アクセスサーバ４を制御するためにシステム管理者が図示しない制御端末から入力した制御コマンドを処理するためのプログラムである。ルーティングプロトコル処理ルーチン５２は、各回線インタフェース４１からアクセスサーバ４に入力されたパケットを宛先アドレスに対応した他の何れかの各回線インタフェース４１に転送する際に必要となるルーティング情報を処理するためのプログラムである。
【００３５】
システム管理者が指定したルーティング情報は、ルーティングプロトコル処理ルーチン５２によって、各プロトコル処理部４２が備えるルーティングテーブル（図示せず）に設定される。各入力回線インタフェース４１－ｉＡ（ｉ＝１～ｎ）がネットワークから受信したパケットは、プロトコル処理部４２－ｉにおいて、例えば、パケットヘッダの宛先アドレスと対応したルーティング情報を含む内部ヘッダを付加した後、ＳＷ部４３に転送される。ＳＷ部４３は、各プロトコル処理部４２からの入力パケットを内部ヘッダが示すにルーティング情報に従って他の何れかのプロトコル処理部に転送する。各プロトコル処理部４２－ｊ（ｊ＝１～ｎ）は、ＳＷ部４３から受信したパケットから内部ヘッダを除去し、該パケットを出力回線インタフェース４１－ｊＢに出力する。
【００３６】
警報監視処理ルーチン５３は、アクセスサーバ４の内部で発生する警報信号を監視し、警報信号に応答した動作を行なうプログラムである。また、ＰＰＰプロトコル信号を処理するＰＰＰプロトコル処理ルーチン５４は、プロトコル処理部４２と連携して、ＲＦＣ１３３２、ＲＦＣ１６６１、ＲＦＣ１９９４などのＰＰＰに関するＲＦＣに従って、ＰＰＰ終端処理、ＬＣＰ処理、ＰＡＰ（Password Authentication Protocol）やＣＨＡＰ（Challenge Handshake Authentication Protocol）などの認証処理、ＩＰＣＰ（Internet Protocol Control Protocol）などのＮＣＰ処理を実行するためのプログラムである。
【００３７】
ＲＡＤＩＵＳプロトコル処理ルーチン５５は、ＲＦＣ２１３８、ＲＦＣ２１３９、ＲＦＣ２８６５、ＲＦＣ２８６６、ＲＦＣ３１６２などのＲＡＤＩＵＳプロトコルの全般を扱い、ＰＰＰ認証時には、ＰＰＰプロトコル処理ルーチン５４と連携して、認証／課金サーバ２１にユーザＩＤやパスワードなどの情報を転送する。
【００３８】
ユーザ認証に成功した場合、認証／課金サーバ２１は、認証されたユーザに関するアトリビュート情報として、例えば、該ユーザが使用すべきＩＰアドレスなどのネットワーク設定条件と、後述する損失パケット数の通知有無といった統計情報収集条件をアクセスサーバ４に通知する。アクセスサーバ４は、認証／課金サーバ２１から通知された各ユーザに関するアトリビュート情報を、ＰＰＰセッションが解放されるまでの間、ＰＰＰユーザ管理テーブル５６に記憶する。
【００３９】
認証に成功したユーザ端末６が、アクセスサーバ４との間にＰＰＰセッションを確立すると、アクセスサーバ４は、統計情報の収集処理を開始する。アクセスサーバ４は、ＰＰＰユーザ管理テーブル５６が示す統計情報収集条件に基づいて、例えば、接続時間、パケット通過量、損失パケット数などの各種パラメータが示す統計情報を収集する。本実施例では、統計情報をＰＰＰセッション単位に収集するために、ＰＰＰユーザ管理テーブル５６には、ユーザ識別子、セッション識別子と対応した統計データ（パラメータ情報）管理用の複数のエントリが登録される。
【００４０】
アクセスサーバ４は、ＰＰＰユーザのセッション確立を確認すると、ＲＡＤＩＵＳプロトコル処理ルーチン５５で課金（統計情報収集）処理の開始要求パケットを生成し、これを認証／課金サーバ２１に送信する。ＰＰＰユーザのセッションが解放された場合、アクセスサーバ４は、ＲＡＤＩＵＳプロトコル処理ルーチン５５で課金処理終了要求パケットを生成し、これを認証／課金サーバ２１に送信する。

【００４１】
アクセスサーバ４は、ＰＰＰセッションが継続中に、ＰＰＰユーザ管理テーブル５６が示す統計情報収集条件に基づいて、インターネット利用者が予めパラメータで指定した統計情報を収集する。アクセスサーバ４は、定期的またはネットワークにおける輻輳や障害の発生／回復などのイベントを契機として、ＲＡＤＩＵＳプロトコル処理ルーチン５５によって、収集された統計情報を示す課金処理中間パケットを生成し、これを認証／課金サーバ２１に送信する。
アクセスサーバ４から認証／課金サーバ２１に送信される課金処理開始要求パケット、課金処理終了要求パケット、課金処理中間パケットの詳細と、アクセスサーバ４と認証／課金サーバ２１との間の通信手順は、以下の説明から明らかになる。
【００４２】
図６～図８は、ユーザ端末６がアクセスサーバ４からインターネット接続サービスを受ける場合の通信シーケンスを示す。但し、ここに例示したシーケンス図は、説明を簡単にするため、本発明における主要なプロトコルメッセージを示したに過ぎず、実際の応用においてユーザ端末とアクセスサーバ間、アクセスサーバと認証／課金サーバ間で交信される全てのメッセージを正確に示している訳ではない。
【００４３】
図６に示すように、インターネット利用者のユーザ端末６は、アクセスサーバ４との間で、ＲＦＣ２５１６で示されるＰＰＰｏＥの初期化処理（Ｓ０１）を実行する。この処理は、特に、アクセス網５がＦＴＴＨ網で構成されている場合、Ｅｔｈｅｒｎｅｔ上に多重化されたＰＰＰフレームを識別するために必要となる。アクセスサーバ４では、例えば、プロトコル処理部４２－１～４２－ｎが、上記ＰＰＰｏＥ初期化処理を実行する。
【００４４】
ＰＰＰｏＥ初期化処理によってＰＰＰｏＥセッションが確立されると、アクセスサーバ４の制御処理部４４は、ＰＰＰプロトコル処理ルーチン５４によって、ＰＰＰのプロトコル信号処理を実行する。ＰＰＰｏＥセッションが確立されると（Ｓ０１）、制御処理部４４は、Link Control Protocol（ＬＣＰ）処理によってリンクレイヤを設定し（Ｓ０２）、ユーザ端末６からのユーザ認証要求（Ｓ０３）に応答して、例えば、ＲＦＣ１９９４に示されるChallenge Handshake Authentication Protocol（ＣＨＡＰ）に従って、認証／課金サーバ２１にユーザ認証を要求する。
【００４５】
本実施例では、認証／課金サーバ２１へのユーザ認証要求時に、制御処理部４４が、ＲＡＤＩＵＳプロトコル処理ルーチン５５を実行し、ＲＦＣ２８６５等に示されるＲＡＤＩＵＳプロトコルにより、ユーザＩＤやパスワード等を示すaccess requestパケットを認証／課金サーバ２１に送信する（Ｓ０４）。access requestパケットを受信した認証／課金サーバ２１は、認証要求元端末６のユーザが予め登録された正規利用者か否かを判定する。
【００４６】
access requestパケットを受信した認証／課金サーバ２１は、図７に示すように、受信パケットが示すユーザ名をキーとして、課金管理データベース（ＤＢ）２１１から要求元ユーザの契約サービス内容を検索し（Ｓ１７）、認証結果と契約サービス内容を示すaccess acceptパケット３００をアクセスサーバ４に返送する（Ｓ０５）。
【００４７】
課金管理データベース２１１は、例えば、図９（Ａ）に示すように、ユーザ名２１１－１と対応して、割当てＩＰアドレス２１１－２と、パスワード２１１－３と、接続時間２１１－４と、入力パケット数２１１－５と、出力パケット数２１１－６と、損失パケット数２１１－７と、中断時間２１１－８と、オプション番号２１１－９と、監視すべきパケットの送信元を示す監視アドレス２１１－１０と、上記監視アドレスに該当したパケット数２１１－１１と、閾値２１１－１２を示している。課金管理データベース２１１には、実際には、ユーザの住所、インターネット接続契約の種類、課金額、支払い口座など、課

金管理に必要な他の項目情報を含んでいるが、これらの情報は、本発明には直接的には関係しないため、図面からは省略してある。

【００４８】

オプション番号２１１－９は、例えば、図９の（Ｂ）に示すように、予めオプション内容２１１－２０としてアクセスサーバ４で実行すべきデータ収集サービス（契約サービス）の内容を特定している。ここで、例えば、access requestパケットのユーザ名が「tanaka」の場合、認証／課金サーバ２１は、access requestパケットが示すパスワードが、課金管理データベース２１１にユーザ名「tanaka」で登録されたパスワード「aaaa」に一致するか否かをによって、要求元ユーザが正規の利用者か否かを判定する。パスワードが一致した場合、ユーザ名「tanaka」のエントリから、要求元ユーザ端末に割当てるべきＩＰアドレス２１１－２（「100.100.10.12」）と、オプション番号２１１－９（「１」）を取得する。

【００４９】

認証／課金サーバ２１は、ユーザ認証に成功した場合、アクセスサーバ４に、図１０に示すaccess acceptパケット３００を返信する（Ｓ０５）。上記access acceptパケット３００には、課金管理データベース２１１から取得したユーザ割当てＩＰアドレスと、契約サービス内容を特定するオプション番号が設定されている。

【００５０】

図１０は、access acceptパケット３００のフォーマットの１例を示す。

本実施例のaccess acceptパケット３００は、ＩＰヘッダ３１０とＵＤＰヘッダ３２０をもつＩＰパケットのペイロード部に、このパケットがaccess acceptパケットであることを示すRadius Code３３０と、Radiusアトリビュート５００を含む。

【００５１】

Radiusアトリビュート５００は、ユーザ端末の識別子となるユーザ名を示すUser-Nameアトリビュート５０１と、ユーザ端末への割当てＩＰアドレスを示すFramed-IP-Addressアトリビュート５０８と、Vendor-Specificアトリビュート５２６を含む。

【００５２】

図１０のRadiusアトリビュートにおいて、末尾に括弧で示した数字は、規約で定義されたアトリビュート番号を示しており、例えば、User-Nameアトリビュート５０１は、アトリビュート番号「１」と、後続するデータ長と、ユーザ名との組み合せによって記述される。Vender-Specificアトリビュート５２６は、規約で定義されたアトリビュート番号をもつ一般的なアトリビュートでは指定できない特殊機能を実現するために使用される。

【００５３】

図１１に、本実施例においてVender-Specificアトリビュート５２６として使用されるVender Typeと定義内容との関係を示す。ここに示した例では、Vender Typeとして「１」～「７」の７種類が用意され、Vender Type毎に予めオプション種別やパラメータ種類などの属性が定義されている。上述したユーザ名「tanaka」のaccess acceptパケット３００の場合、Vender-Specificアトリビュート５２６では、Vender Type（１）＝「１」と指定することによって、アクセスサーバ４に対して、ユーザ名「tanaka」の端末に関しては、オプション番号「１」で定義されたパラメータ（損失パケット数と中断時間）の情報収集サービスを実行すべきことを指示する。

【００５４】

認証／課金サーバ２１からaccess acceptパケット３００を受信したアクセスサーバ４は、受信パケットのアトリビュートを解析し、ＰＰＰユーザ管理テーブル５６に、要求元ユーザの識別子と対応して、統計情報収集条件と統計データを示す新たなエントリを登録する（Ｓ１８）。

【００５５】

図１２に、ＰＰＰユーザ管理テーブル５６に登録される情報の１例を示す。

ＰＰＰユーザ管理テーブル５６の各エントリは、ユーザ名５６－１と、割当てＩＰアドレスを示すFramed IP Address５６－２と、接続中のＰＰＰセッションをアクセスサーバ

４内で一意に識別するためのSession ID５６－３と、ＰＰＰセッションが接続時間を示すSession Time５６－４と、ＰＰＰセッション中の入力データパケット数を示すInput Packets５６－５と、出力データパケット数を示すOutput Packets５６－６と、損失パケット数を示すLoss Packets４５－７と、パケット損失によるサービス中断時間を示すCongestion Time５６－８と、監視すべきパケットの送信元アドレス（監視アドレス）を示すMonitored Address５６－９と、上記監視アドレスに該当する監視パケット数を示すMonitored Packets５６－１０と、閾値５６－１１とを含む。

【００５６】

上述したユーザ名「tanaka」の場合、最初のaccess acceptパケット３００の受信直後には、ユーザ名５６－１＝「tanaka」、Framed IP Address５６－２＝「100.100.100.12」、Session ID５６－３＝「ｗｗ」、Session Time５６－４＝「00:00:00」、Input Packets５６－５＝「０」、Output Packets５６－６＝「０」、Loss Packets４５－７＝「０」、Congestion Time５６－８＝「０」のエントリがＰＰＰユーザ管理テーブル５６に登録されることになる。

【００５７】

アクセスサーバ４は、ＰＰＰユーザ管理テーブル５６へのエントリ登録（Ｓ１８）が終わると、要求元ユーザ端末６にユーザ認証応答を送信する（Ｓ０６）。ユーザ端末６は、上記ユーザ認証応答を受信すると、ＲＦＣ１３３２に示されるＩＰＣＰ（IP Control Protocol）によって、アクセスサーバ４との間でＩＰレイヤ設定のための通信手順を実行する（Ｓ０７）。ユーザ端末６に対するＩＰアドレスの設定と、プロトコル信号処理によるＰＰＰセッションの設定が終了すると、ユーザ端末６はインターネット１への接続が可能となる。

【００５８】

アクセスサーバ４は、ユーザ端末６との間のＰＰＰセッションの設定が完了すると、課金（統計情報収集）処理を開始する。この時、本発明では、アクセスサーバ４の制御処理部４４がＲＡＤＩＵＳプロトコル処理ルーチン５５を実行し、ＰＰＰユーザ管理テーブル５６に追加された新たなエントリ情報に基づいて、課金処理開始要求パケットであるaccounting request（start）パケット３０１を作成し、これを認証／課金サーバ２１に送信する（Ｓ０８）。

【００５９】

図１３は、accounting request（start）パケット３０１のフォーマットを示す。

accounting request（start）パケット３０１は、Radiusアトリビュート５００として、ユーザ名を示すUser-Nameアトリビュート５０１と、ユーザ端末割当てＩＰアドレスを示すFramed-IP-Addressアトリビュート５０８と、課金処理要求パケットの種別を示すAcct-Status-Typeアトリビュート５４０と、ユーザ端末とアクセスサーバ間のＰＰＰセッション識別子を示すAcct-Session-IDアトリビュート５４４を含む。Acct-Status-Typeアトリビュート５４０は、accounting requestが課金処理の開始要求か、終了要求か、中間的なアカウンティング要求かの区別を示しており、パケット３０１では、課金処理の開始要求“start”であることを示すコード「１」が設定されている。

【００６０】

ユーザ名「tanaka」の例では、Radiusアトリビュート５００に、User-Nameアトリビュート５０１＝「tanaka」、Framed-IP-Addressアトリビュート５０８＝「100.100.100.12」、Acct-Session-IDアトリビュート５４４＝「ｗｗ」が設定される。

【００６１】

認証／課金サーバ２１は、アクセスサーバ４から上記accounting request（start）パケット３０１を受信すると、応答パケット（accounting response）を返信し（Ｓ０９）、受信パケットで指定されたユーザ名をもつインターネット利用者について統計情報の収集動作を開始する。

【００６２】

次に、図８を参照して、ユーザ端末６がインターネットに接続されている間に実行され

る課金（統計情報収集）処理動作について説明する。
ユーザ端末６がインターネット１に接続されている間、アクセスサーバ４は、図７のステップＳ１８でＰＰＰユーザ管理テーブル５６に登録されたエントリ情報に基づいて、ユーザ端末毎に、例えば、入出パケット数や損失パケット数などのパラメータが示す統計情報を収集し、ＰＰＰユーザ管理テーブル５６を周期的に更新する（Ｓ１９）。Session Time５６－４は、ＰＰＰユーザ管理テーブル５６の更新の都度、前回の更新時点からの経過時間が加算される。

【００６３】
ユーザ名「tanaka」のユーザ端末の場合、上記周期的更新によって、ＰＰＰユーザ管理テーブル上で、例えば、Session Time５６－４＝「00:05:00」、Input Packets５６－５＝「２２５０」、Output Packets５６－６＝「２５６７」、Loss Packets４５－７＝「１００」、Congestion Time５６－８＝「３０」の如く、統計データの値が変化する。

【００６４】
アクセスサーバ４は、ＲＡＤＩＵＳプロトコル処理ルーチン５５によって、課金処理中間要求パケットであるaccounting request（interim-update）パケット３０２を周期的に生成し、これを認証／課金サーバ２１に送信する（Ｓ１０）。accounting request（interim-update）パケット３０２には、ＰＰＰユーザ管理テーブル５６が示す統計データの値が設定される。

【００６５】
図１４は、accounting request（interim-update）パケット３０２のフォーマットを示す。accounting request（interim-update）パケット３０２は、アトリビュート５００として、図１３に示したaccounting request（start）パケット３０１と同様に、ユーザ名を示すUser-Nameアトリビュート５０１と、ユーザ端末割当てＩＰアドレスを示すFramed-IP-Addressアトリビュート５０８と、課金処理要求パケットの種別を示すAcct-Status-Typeアトリビュート５４０と、ＰＰＰセッション識別子を示すAcct-Session-IDアトリビュート５０４を含む。Acct-Status-Typeアトリビュート５４０には、このパケットが中間アカウンティング“interim-update”用のものであることを示すコード「３」が設定される。

【００６６】
accounting request（interim-update）パケット３０２は、上記アトリビュートの他に、ＰＰＰセッションの接続時間を示すAcct-Session-Timeアトリビュート５４６と、入力パケット数を示すAcct-Input-Packetsアトリビュート５４７と、出力パケット数を示すAcct-Output-Packets５４８と、Vendor-Specificアトリビュート５２６を含む。この他にも、例えば、accounting request（interim-update）パケット３０２の生成時刻を示すEvent-Timestampアトリビュート（５５５）などが含まれるが、図面では省略してある。

【００６７】
ユーザ名「tanaka」のユーザ端末の場合、ＰＰＰユーザ管理テーブル５６が示すLoss Packets５６－７＝「１００」、Congestion Time５６－８＝「３０」等の統計データは、図１１に示したVender Type定義に従って、例えば、Vender Type（４）＝１００、Vender Type（５）＝３０の如く、Vendor-Specificアトリビュート５２６として設定される。

【００６８】
認証／課金サーバ２１は、アクセスサーバ４からaccounting request（interim-update）パケット３０２を受信すると、図８に示すように、受信パケットが示すRadiusアトリビュート５００の内容に従って、課金管理データベース２１１のUser Name５０１に該当するのエントリにおける統計データの値を更新し（Ｓ２０）、更新された統計データをＷｅｂサーバ２４に通知すると共に、アクセスサーバ４に応答パケット（accounting response）を送信する（Ｓ１１）。
Ｗｅｂサーバ２４は、上記統計データに従って、データベース２３１の公開用パラメータ情報を更新する（Ｓ２１）。従って、インターネット利用者は、上記Ｗｅｂサーバ２４をアクセスすることによって、自分のパラメータ情報をリアルタイムに閲覧、取得するこ

とが可能となる。

【００６９】

ユーザ端末６の利用者が、インターネット接続を終了すると、図６に示すように、ユーザ端末６とアクセスサーバ４との間で、ＩＰＣＰのターミネーション処理（Ｓ１２）、ＬＣＰのターミネーション処理（Ｓ１３）、ＰＰＰｏＥセッションの解放処理（Ｓ１４）が実行される。アクセスサーバ４は、ＰＰＰｏＥセッションの解放処理が完了すると、課金処理終了要求パケットである図１５に示すaccounting request（stop）パケット３０３を生成し、これを認証／課金サーバ２１に送信する（Ｓ１５）。

【００７０】

accounting request（stop）パケット３０３は、図１４に示したaccounting request（interim-update）パケット３０２と同様のフォーマットを有し、Acct-Status-Typeアトリビュート５４０には、このパケットが課金処理の終了“stop”用のものであることを示すコード「２」が設定され、Radiusアトリビュート５００には、ＰＰＰユーザ管理テーブル５６の最新の統計データ値が設定される。

【００７１】

認証／課金サーバ２１は、上記accounting request（stop）パケット３０３を受信すると、統計データの最後の更新処理（図８のステップＳ２０）を実行し、アクセスサーバ４にaccounting Responseを返送する（Ｓ１６）。この時、Ｗｅｂサーバ２３も公開用パラメータ情報の最後の更新処理（図８のステップＳ２０）を実行する。

【００７２】

次に、図１６のシーケンス図を参照して、ネットワーク上での輻輳によってパケット損失が発生し、インターネット接続サービスが一時的に中断した場合の課金処理動作について説明する。

アクセスサーバ４は、ネットワーク上の輻輳を検出すると（Ｓ２３）、ＰＰＰユーザ管理テーブル５６で指定されている統計情報収集条件に従って、ユーザ（セッション）毎に、輻輳時間や損失パケット数といったパラメータの値を計数し、ＰＰＰユーザ管理テーブル５６の統計データを更新する（Ｓ２４）。上記計数動作によって、前述したユーザ名「tanaka」の場合、例えば、図１２に示したように、Session Time５６－４＝「00:05:30」、Input Packets５６－５＝「２２５０」、Output Packets５６－６＝「２５６７」、Loss Packets４５－７＝「１００」、Congestion Time５６－８＝「３０」の如く統計データの値が更新される。

【００７３】

アクセスサーバ４は、ネットワーク上での輻輳回復を検出すると（Ｓ２５）、ＲＡＤＩＵＳプロトコル処理ルーチン５５によって、図１４に示したVendor-Specificアトリビュートを含むaccounting request（interim-update）パケット３０２を生成し、ＰＰＰユーザ管理テーブル５６が示す統計データを認証／課金サーバ２１に送信する（Ｓ１０）。例えば、ユーザ名「tanaka」の場合、Loss Packets４５－７の値はVender Type（４）＝「１００」、また、Congestion Time５６－８の値はVender Type（５）＝「３０」として、認証／課金サーバ２１に通知される。

【００７４】

認証／課金サーバ２１は、上記accounting request（interim-update）パケット３０２を受信すると、課金管理データベース２１１の受信パケットUser Name５０１が示すエントリにおいて、受信パケットのVendor-Specificアトリビュートの内容に応じたデータ更新を実行する（Ｓ２６）。この後、ｍａｉｌサーバ２３に対して、User Nameと、輻輳によって発生した損失パケット数やサービス中断時間等の統計データを通知する（Ｓ２６０）と共に、アクセスサーバ４に対して、上記accounting request（interim-update）パケット３０２の受信応答となるaccounting responseパケットを送信する（Ｓ１１）。

【００７５】

ｍａｉｌサーバ２３は、認証／課金サーバ２１からの通知内容に従ってデータベース２３１を更新（Ｓ２７）した後、利用者のメールアドレスに対して、統計情報（この例では

輻輳情報）を送信する（Ｓ２８）。以上のシーケンスによって、インターネット利用者毎に、パケット損失数やサービス中断時間等、予めパラメータで指定された統計情報のリアルタイム配信が可能となる。

【００７６】

次に、図１７に示すシーケンス図を参照して、例えば、特定ＩＰアドレスを送信元とするパケット通信量をアクセスサーバ４で監視しておき、パケット通信量が予め利用者との間の契約値をオーバーした時、利用者にその旨を電子メールで通知するようにした本発明に特有の統計情報公開サービスについて説明する。

【００７７】

アクセスサーバ４は、ＰＰＰユーザ管理テーブル５６に監視アドレス５６－９として登録されている特定のＩＰアドレスを送信元とするパケット数（通信量）を監視し、該当パケットの個数を監視パケット数５６－１０としてカウントする（Ｓ２９）。アクセスサーバ４は、監視パケット数を予め指定されている閾値５６－１１と比較し、閾値を超えた時（Ｓ３０）、その旨を示すaccounting request（interim-update）パケット３０２を認証／課金サーバ２３に送信する（Ｓ１０）。このaccounting request（interim-update）パケット３０２は、図１６のステップＳ１０で送信されるaccounting request（interim-update）パケットと比較して、Vender-Specificアトリビュート情報のみが異なる。

【００７８】

例えば、図７の課金管理データベース２１１でユーザ名「yamada」のエントリが示すように、ユーザ「yamada」が、予めインターネットサービスプロバイダ２との間で、監視アドレス２１１－１０（「10.1.1.0/24」）から自端末宛への送信パケット数が、閾値２１１－１２として指定した「1000」を超えた時、メールでその旨を通知するという契約をしていたと仮定する。この場合、ユーザ名「yamada」のユーザ端末からインターネット接続要求があった時、認証／課金サーバ２１は、access requestパケット３００のVender-Specificアトリビュート５２６で、Vender Type（１）＝「２」、Vender Type（２）＝「10.1.1.0/24」、Vender Type（３）＝「1000」と指定することによって、上記契約条件をアクセスサーバ４に通知する。

【００７９】

アクセスサーバ４は、上記契約条件をＰＰＰユーザ管理テーブル５６のユーザ名「yamada」のエントリに記憶して、監視パケット数５６－１０のカウント（Ｓ２９）と、閾値オーバーの判定（Ｓ３０）を実行する。ユーザ名「yamada」の監視パケット数が閾値を越えた時、アクセスサーバ４は、ＲＡＤＩＵＳプロトコル処理ルーチン５５によって、例えば、Vendor-SpecificアトリビュートがVender Type（６）＝「1001」、Vender Type（７）＝「設定値オーバ」を指定したaccounting request（interim-update）パケット３０２を生成し、これを認証／課金サーバ２１に送信する（Ｓ１０）。

【００８０】

認証／課金サーバ２１は、上記accounting request（interim-update）パケット３０２を受信すると、課金管理データベース２１１におけるユーザ名「yamada」のエントリの統計データを更新する（Ｓ３１）。この後、ｍａｉｌサーバ２３に対して、ユーザ名「yamada」のメールアドレスに監視パケット数オーバー通知のメール送信を要求する（Ｓ３１０）と共に、アクセスサーバ４に対して、accounting request（interim-update）パケット３０２の受信応答となるaccounting responseパケットを送信する（Ｓ１１）。

【００８１】

ｍａｉｌサーバ２３は、認証／課金サーバ２１からの通知内容に従ってデータベース２３１を更新（Ｓ３２）した後、指定された利用者のメールアドレスに対して、監視パケット数のオーバー通知のメールを送信する（Ｓ３３）。以上のシーケンスによって、インターネット利用者は、予め指定したＩＰアドレスからのパケット通信量が指定値をオーバーしたことをリアルタイムに知ることが可能となる。

【００８２】

以上の実施例においては、予め利用者とインターネットサービスプロバイダとの間の契

約条件として、パケット損失数と指定ＩＰアドレスからのパケット通信量をそれぞれ別々のパラメータとして指定したが、例えば、複数の監視ＩＰアドレスを指定する、パケット損失数を特定ＩＰアドレスからのパケットに限定するなど、監視サービスで収集すべき統計情報の種類と指定形式には、実施例以外の種々の変形が許容される。

【００８３】

また、実施例では、アクセスサーバ４と認証／課金サーバ２１の間の交信パケットにおいて、Vendor-Specificアトリビュート内のVender Typeによって各種パラメータ情報を指定したが、ＲＦＣ２８６６でreservedとして規定されているアトリビュートを使用してもよい。

【図面の簡単な説明】

【００８４】

【図１】本発明によるネットワーク統計情報サービスシステムを含むネットワーク構成図。

【図２】図１のネットワークに適用される主信号系転送プロトコルスタックの１例を示す図。

【図３】図１のネットワークに適用される制御信号系転送プロトコルスタックの１例を示す図。

【図４】図１に示したアクセスサーバのハードウェア４の詳細を示すブロック図。

【図５】図４のアクセスサーバ４における制御処理部４４の詳細を示すブロック図。

【図６】本発明によるネットワーク統計情報サービスシステムの動作を示すシーケンス図。

【図７】図６におけるステップＳ０４～Ｓ０６の詳細動作を示すシーケンス図。

【図８】図６におけるネットワーク統計情報の更新ステップＳ１０の詳細と、ユーザ端末によるネットワーク統計情報の参照動作を示すシーケンス図。

【図９】認証／課金サーバ２１が備える課金管理データベースの１例を示す図。

【図１０】図１の認証／課金サーバ２１からアクセスサーバ４に送信されるaccess acceptパケットのフォーマットを示す図。

【図１１】図１の認証／課金サーバ２１とアクセスサーバ４との間で交信されるVender Specificアトリビュートの内容を説明するための図。

【図１２】図５のＰＰＰユーザ管理テーブル５６の１例を示す図。

【図１３】図１のアクセスサーバ４から認証／課金サーバ２１に送信されるaccounting request（start）パケットのフォーマットを示す図。

【図１４】図１のアクセスサーバ４から認証／課金サーバ２１に送信されるaccounting request（interim-update）パケットのフォーマットを示す図。

【図１５】図１のアクセスサーバ４から認証／課金サーバ２１に送信されるaccounting request（stop）パケットのフォーマットを示す図。

【図１６】本発明のネットワーク統計情報サービスシステムにおけるネットワーク輻輳検出時の動作を示すシーケンス図。

【図１７】本発明のネットワーク統計情報サービスシステムにおける監視パケット閾値超過時の動作を示すシーケンス図。

【符号の説明】

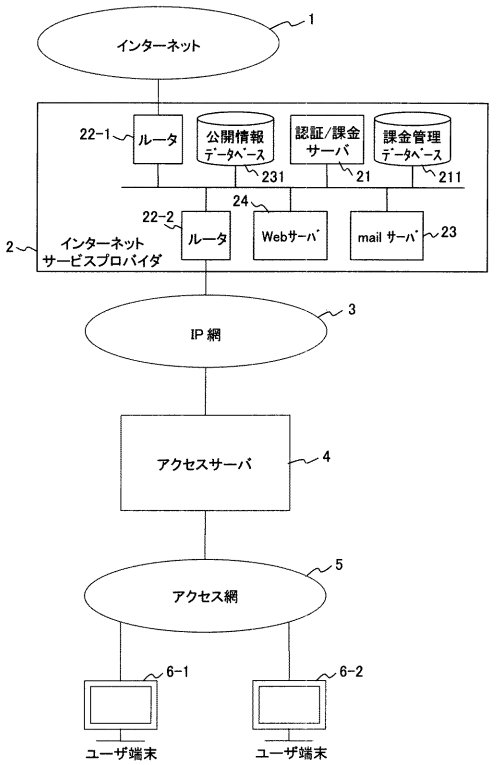
【００８５】

１：インターネット、２：インターネットサービスプロバイダ、３：ＩＰ網、
４：アクセスサーバ、５：アクセス網、６：ユーザ端末、２１：認証／課金サーバ、
２１１：課金管理データベース、２２：ルータ、２３：ｍａｉｌサーバ、
２３１：公開情報用データベース、２４：Ｗｅｂサーバ、
４１－１～４１－ｎ：回線インタフェース、４２－１～４２－ｎ：プロトコル処理部、
４３：スイッチ部、４４：制御処理部、４４１：ＣＰＵ、
４４２：制御端末インタフェース、４４３：プロトコル処理部インタフェース、
４４４：スイッチ部装置制御処理部、５０：メモリ、５１：ＣＬＩ処理ルーチン、

５２：ルーティングプロトコル処理処理ルーチン、５３：警報監視処理ルーチン、
５４：ＰＰＰプロトコル処理処理ルーチン、
５５：ＲＡＤＩＵＳプロトコル処理ルーチン、５６：ＰＰＰユーザ管理テーブル。

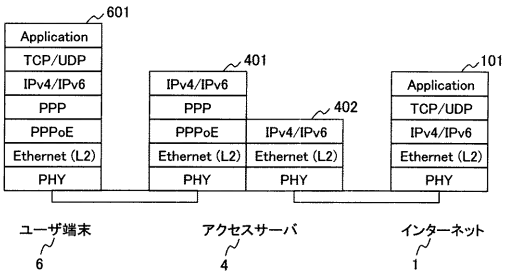
【図１】

図 1



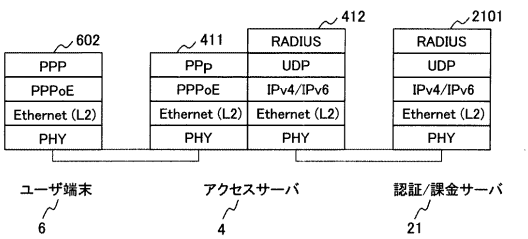
【図２】

図 2



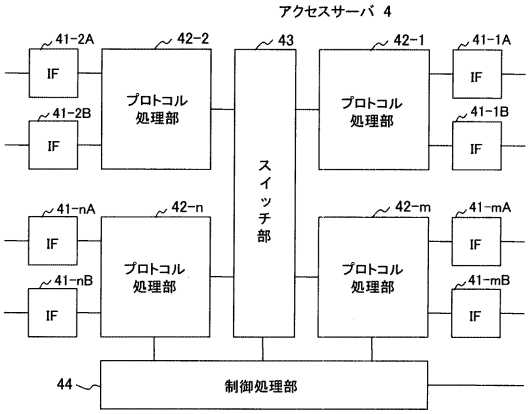
【図３】

図 3



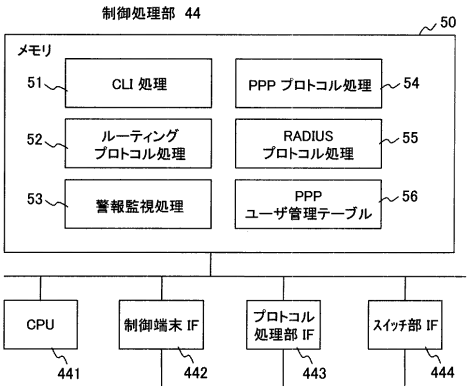
【図４】

図 4



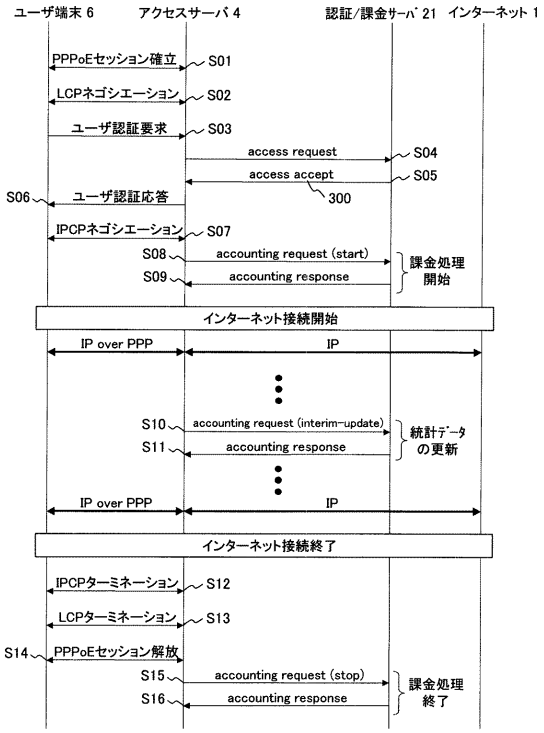
【図５】

図 5



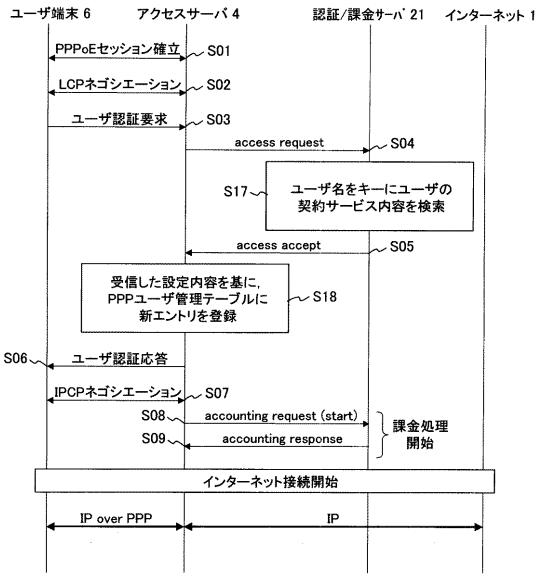
【図６】

図 6



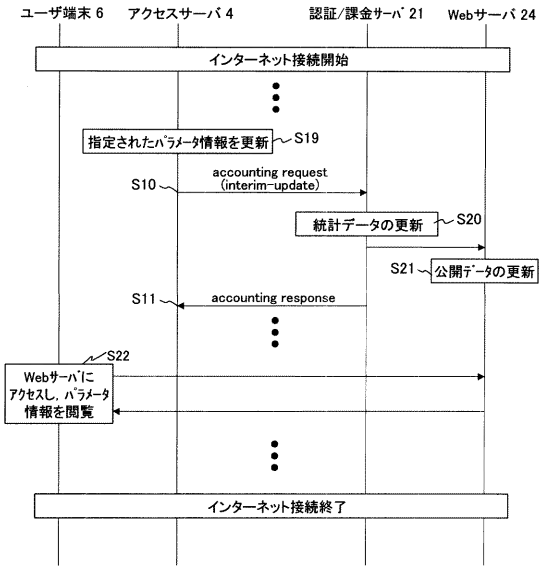
【図７】

図 7



【図８】

図 8



【図９】

図 9

課金管理データベース 211

211-1 ユーザ名	211-2 割当てIP	211-3 パスワード	211-4 接続時間	211-5 入力パケット数	211-6 出力パケット数	211-7 損失パケット数	211-8 中断時間
tanaka	100.100.10.12	aaaa	00:05:00	2250	2567	100	30
wada	100.100.5.3	bbbb	-	-	-	-	-
suzuki	10.0.0.1	xxxx	00:20:15	1010	258	-	-
sato	10.1.1.5	yyyyy	05:35:25	3455	6853	1652	2052
yamada	10.5.2.2	zzzz	00:48:12	4582	3962	-	-
kato	10.15.25.3	cccc	-	-	-	-	-

(A)

211-9 オプション

オプション番号	211-10 監視Address	211-11 監視パケット数	211-12 閾値
1	-	-	-
1	-	-	-
0	-	-	-
1	-	-	-
2	10.1.1.0/24	1001	1000
3	10.15.0.0/24	-	500

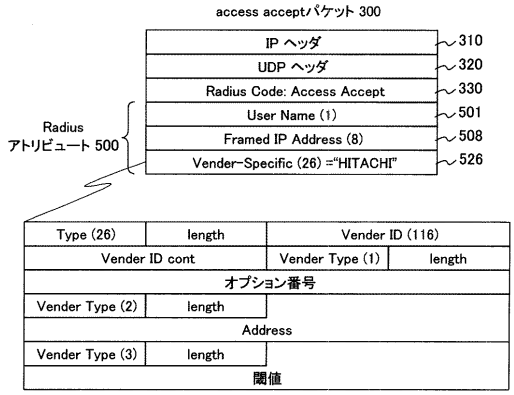
211-20 オプション内容

211-9 オプション番号	オプション内容
0	オプション無し
1	損失パケットならびに中断時間をカウントする
2	特定のパケットをカウントする
3	オプション1との両方を選択

(B)

【図１０】

図 10



【図１１】

図 11

Vender Specific アトリビュート 526

Vender Type	定義内容
1	オプション種別
2	カウントしたいAddress値
3	閾値
4	損失パケット数
5	中断時間
6	指定されたAddress値からの流入パケット数
7	閾値オーバ／範囲内

【図１２】

図 12

PPPユーザ管理テーブル 56

56-1 ユーザ名	56-2 Framed IP Address	56-3 Session ID	56-4 Session Time	56-5 Input Packets	56-6 Output Packets	56-7 Loss Packets	56-8 Congestion Time	56-9 Monitored Address	56-10 Monitored Packets	56-11 閾値
tanaka	100.100.10.12	ww	00:05:00	2250	2567	100	30	-	-	-
suzuki	10.0.0.1	xx	00:20:15	1010	258	-	-	-	-	-
sato	10.1.1.5	yy	05:35:25	3455	6853	1652	2052	-	-	-
yamada	10.5.2.2	zz	00:48:12	4582	3962	-	-	10.1.1.0/24	1001	1000
•••										

【図１３】

図 13

accouting request (start) パケット 301

	IP ヘッダ	310
	UDP ヘッダ	320
	Radius Code: Accounting Request	330
Radius アトリビュート 500	User Name (1)	501
	Framed IP Address (8)	508
	Acct Status Type (40) = "start"	540
	Acct Session ID (44)	544

【図１４】

図 14

accounting request (interim-update)パケット 302

	IP ヘッダ	310
	UDPヘッダ	320
	Radius Code: Accounting Request	330
	User Name (1)	501
	Framed IP Address (8)	508
Radius アトリビュート 500	Acct Status Type (40) = " interim-update"	540
	Acct Session ID (44)	544
	Acct Session Time (46)	546
	Acct Input Packets (47)	547
	Acct Output Packets (48)	548
	Vender -Specific (26) ="HITACHI"	526

Type (26)	length	Vender ID (116)
Vender ID cont	Vender Type (4)	length
Loss Packets		
Vender Type (5)	length	
Congestion Time		
Vender Type (6)	length	
Address Packets		
Vender Type (7)	length	
閾値オーバ／範囲内		

【図１５】

図 15

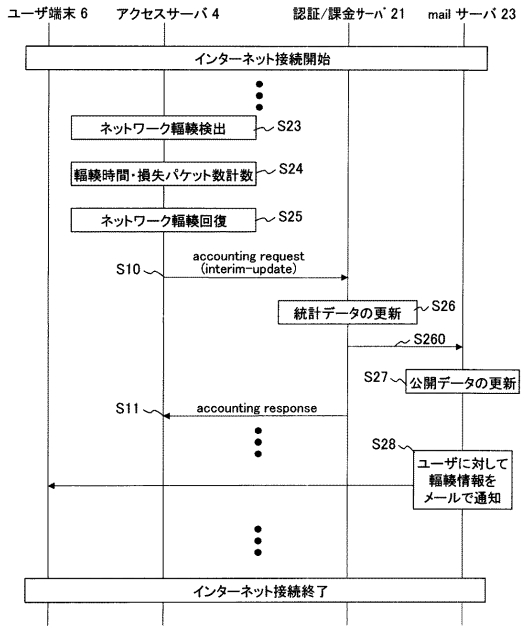
accounting request (stop) パケット 303

	IP ヘッダ	310
	UDP ヘッダ	320
	Radius Code: Accounting Request	330
	User Name (1)	501
	Framed IP Address (8)	508
Radius アトリビュート 500	Acct Status Type (40) = "stop"	540
	Acct Session ID (44)	544
	Acct Session Time (46)	546
	Acct Input Packets (47)	547
	Acct Output Packets (48)	548
	Vender-Specific (26) = " HITACHI "	526

Type (26)	length	Vender ID (116)
Vender ID cont	Vender Type (4)	length
Loss Packets		
Vender Type (5)	length	
Congestion Time		
Vender Type (6)	length	
Address Packets		
Vender Type (7)	length	
閾値オーバ／範囲内		

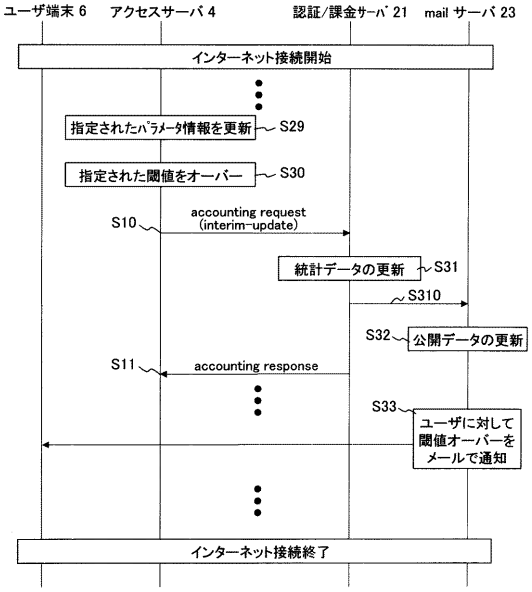
【図１６】

図 16



【図１７】

図 17



フロントページの続き

(72)発明者　和田　光弘
神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立コミュニケーションテクノロジー内

Ｆターム(参考) 5K030 HA08 HC01 JA10 JT02 MA01 MA04 MB09

【要約の続き】
【選択図】　図１