グローバルIPアドレスリースシステム

YOSHIDA, Yutaka / FURUTA, Daisuke / 吉田, 裕 / 古田, 大輔

(出版者 / Publisher)
法政大学工学部
(雑誌名 / Journal or Publication Title)
Bulletin of the Faculty of Engineering, Hosei University / 法政大学工学部研究集報
(巻 / Volume)
38
(開始ページ / Start Page)
7
(終了ページ / End Page)
10
(発行年 / Year)
2002-03
(URL)
https://doi.org/10.15002/00004304

グローバルIPアドレス リースシステム

Global IP Address Lease System

古田大輔*、吉田裕**
Daisuke FURUTA and Yutaka YOSHIDA

The current internet protocol is IPv4, the capacity of which recently tends to be insufficient to respond to increase in global IP address assignment demand. Accordingly, several functionalities such as "Network Addresses Translation" and "IP Masquerade" are devised and utilized together with private address scheme. The functionality realized by the service, protocol, and system proposed here is similar to them, and is characteristic of that hosts are accessible from outside subnets usually operated by private address utilization.

Key Words : Lease System, Global IP Address, Private IP Address, IPv4

1．はじめに

現在インターネットで使用されているプロトコルはTCP/IPのIPｖ４である。急速な需要のため、グローバルIPアドレス（GA）が不足しつつあり、その将来的対策としてIPｖ６の適用が望まれるが、当面の対策としてプライベートIPアドレス（PA）の利用があげられる。

ただし、PA、GAを持つホスト間の通信を可能とする必要があり、NATやIPマスカレードによる方式[1]がPAホスト発、GAホスト着の形式で実現されている。本報告ではこの逆、GAホスト発、PAホスト着を可能とする一方式について述べる。

2．サービス

主としてPAにより運用中のサブネットにおいて、少数のGAを用いてサブネット外部のホストから内部のホストにアクセス可能とするサービスである（図１）。

ただし、サブネット内で利用可能な幾つかのGAを保有し、アクセスを要求する外部のホスト及びユーザは、予めサブネット内の特定のサーバに登録済みであることを前提条件とする。これは、システム利用上のセキュリティの向上のためである。さらに、通信を要求するホスト上においてもアカウントが登録済みであることを前提条件とする。

外部のホストが特定のサーバに相手ホスト名を指定して通信を依頼し、特定のサーバが幾つか手持ちのGAの中から一つを選んで指定されたサブネット内のホストにリースすることにより、一時的にサブネット内ホストとの通信が可能となる。

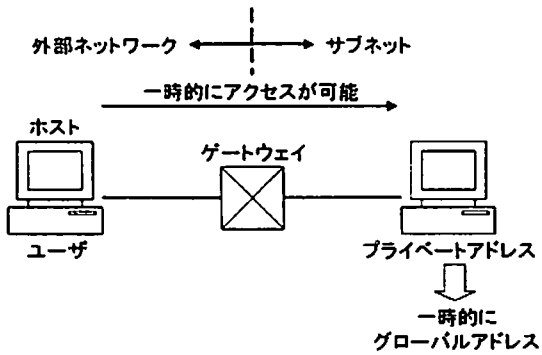


図１　実現するサービス

3．グローバルIPアドレスリースシステム

3．1　システム構成

最小構成は、サブネット内のリースクライアント（通常はPAを保有、以下単にクライアントと呼ぶ）、リースサーバ(このサーバ用のGAとリース用の幾つかのGAを保有)、サブネット外部のホストの３ホストである。当然サブネットと外部を接続するゲートウェイ（GAとPA両方を保有）も必須であり、複数種のコネクションを許す場合には、クライアント及び外部ホストが一般に複数となる。

●外部ホスト

- アクセスするホスト名、リースサーバのGAを知っており、このホスト上にアクセスを希望するユーザのアカウントがある。
- アクセス要求をリースサーバに送信し、認証を受けるための処理機能を持つ。

＊大学院情報電子工学専攻
＊＊電子情報学科

●リースサーバ
- アクセスを要求するためのユーザ情報（ユーザ名、パスワード）、クライアント情報（ホスト名とそのPA）、リースGAデータベースを管理する。
- 外部ホストからの要求を受け付け、ユーザ名とパスワードによる認証、サブネット内ホストに対するアドレス変更指示、クライアントからのアドレス返却によるサービスの終了と返却されたアドレスの解放。
- アクセス要求した外部ホストに対してクライアントのGAの通知。

●クライアント
- リースサーバからの要求に応じてGAを設定。
- サービス終了時のPAの設定。

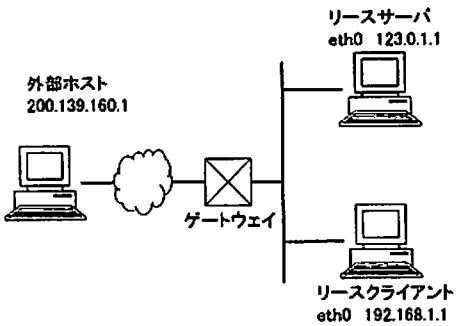


図2　システム構成

3．2　プロトコル[2)]

主としてOSI参照モデルのアプリケーション層に追加する形で実現する（図3）。アプリケーション層のメッセージフォーマットは次の通り（図4）。ただし、送受信区間、ただし及び手順によって不要なデータも含まれるが、実装の簡単化のために統一したフォーマットとした。

3．2．1　メッセージフォーマット

● メッセージタイプ
リース要求、リース要求応答、ACK、NAK、リース通知、リース通知応答、リース、設定通知、終了

● ユーザ名、パスワード
リースサーバに登録してあるユーザ名とパスワード。

● リースクライアントのネーム
アクセスを要求する際のクライアントのホスト名。

● リースアドレス
クライアントにリースするGA。

● リースサーバアドレス
リースサーバのGA。

● リースクライアントアドレス
リースクライアントのPA。

● 外部ホストアドレス
外部ホストのGA。

3．2．2　手順

プロトコルの手順と状態遷移を示す（図5）。

● リースサーバへのアクセス要求
ユーザがクライアントへの通信をユーザ名とパスワード、クライアントのホスト名を送信し、依頼する。

● 認証
リースサーバは外部ホストから送信されたユーザ情報とクライアント情報を基にリースサーバのデータベース認証を行う。認証はアカウントの認証、クライアントのホスト名の認証を行う。不成立ならばNAKを外部ホストに返す。成立ならばクライアントへの通知へ遷移する。クライアントの認証においては指定されたクライアントに対して既にサービスが提供されていれば、そのことを通知して終了する。

● クライアントへの通知
リースサーバは認証が成立すれば、クライアントに外部ホストからアクセス要求が来たことを通知する。

● クライアントのネットワーク使用状況の診断
クライアントはリースサーバから通知を受けると、通信中であるかどうかを調べる。これは、既に確立している通信を優先させるためである。通信中であればNAKを返す。NAKを受け取ったリースサーバは依頼元の外部ホストに通信中であることを通知する。通信中でなければ、リース可能なことをリースサーバに通知する。

● GAのリース
リースサーバはクライアントからリース可能であることを通知されると、幾つか手持ちのGAの中から一つを選んでクライアントへリースする。

● アドレスの設定
クライアントはリースサーバからリースされたGAをインタフェースに設定する。次に設定が完了したことをリースサーバへ通知する。

● 通信可能状態の通知
リースサーバはクライアントが設定を完了したことを確認したら、依頼元の外部ホストへリースしたGAを通知する。

● 通信可能状態
リースサーバからクライアントのGAを通知されると、外部ホストはクライアントへの通信が可能な状態となる。

● 終了

サービスの終了は，外部ホストがクライアントへ終了メッセージを送信。終了メッセージを受け取ったクライアントはインターフェースに元のPAを設定する。クライアントはリースされていたGAを返却するために終了メッセージをリースサーバへ送信。終了メッセージを受け取ったリースサーバは返却されたGAを解放してサービスが終了する。

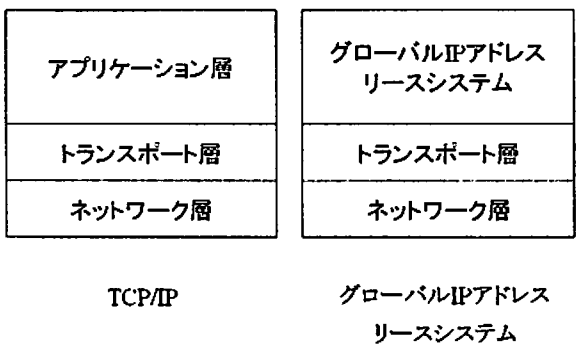


図３　実現するプロトコルの配置

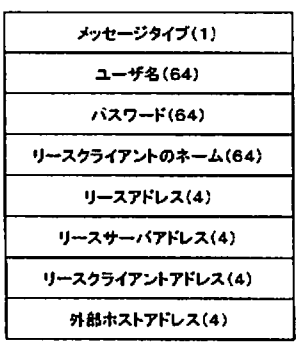


図４　メッセージのフォーマット

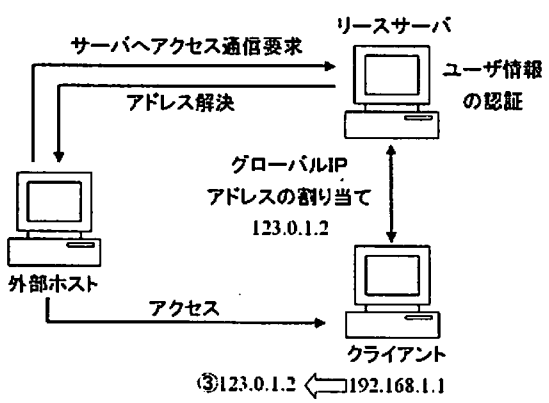


図５　手順

３．３　実装[3)]

この節では各ホストにおけるシステムの実装について述べ、プログラムインタフェース間のデータについて図６に示す。

● 外部ホスト

データ：メッセージタイプ
　ユーザ情報（ユーザ名、パスワード）
　クライアントのホスト名
　リースアドレス
　外部ホストアドレス

処理：ユーザ情報とクライアントのホスト名の入力しアクセス要求の送信。
　認証に対する応答メッセージの受信。
　リース完了によるクライアントのGAの受信。
　終了メッセージの送信

● クライアント

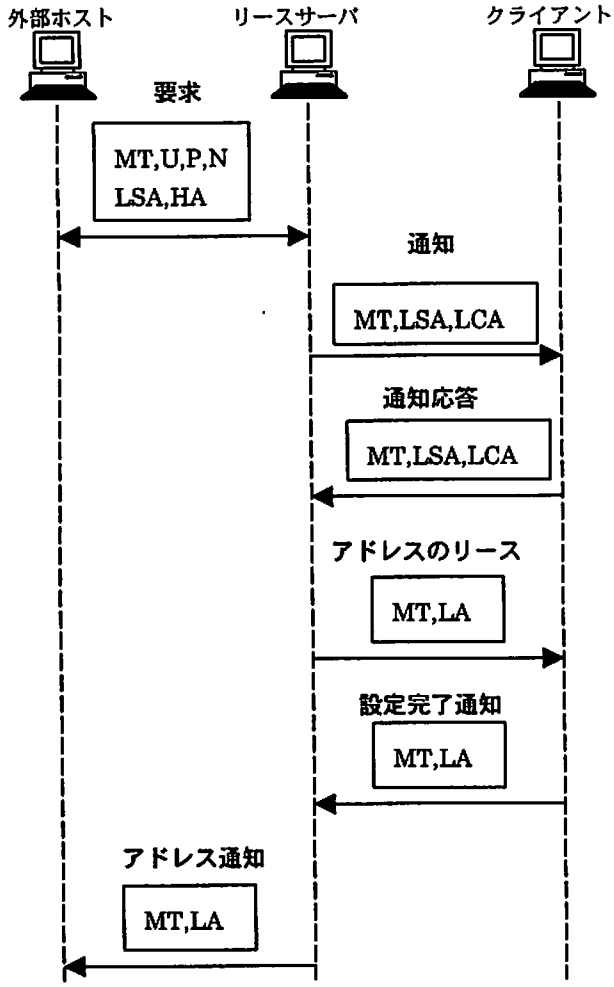
データ：メッセージタイプ
　リースサーバアドレス
　クライアントアドレス
　リースアドレス

処理：リースの受け付け。
　ネットワーク使用状況の診断。
　ネットワーク使用状況の通知
　リースアドレスの受信
　リースアドレスの設定
　設定完了の通知
　元のPAに設定
　アドレスの返却

● リースサーバ

データ：メッセージタイプ
　ユーザ情報（ユーザ名、パスワード）
　クライアントのホスト名
　クライアントアドレス
　リースサーバアドレス
　リースアドレス
　外部ホストアドレス

処理：アクセス要求の受け付け。
　ユーザ情報の認証（認証に対する応答）。
　クライアントのホスト名とそのPAの変換。
　クライアントへのリースアドレスの通知。
　データベースの更新。
　外部ホストへのクライアントアドレスの通知。
　サービス終了の受付。
　アドレスの解放。



MT：メッセージタイプ
U：ユーザ名
P：パスワード
N：クライアントのホスト名
LA：リースアドレスGA
LSA：リースサーバアドレス
LCA：クライアントアドレスPA
HA：外部ホストアドレス

図6　プログラムインタフェース間データ

4．機能拡張性

さらに幾つかの機能を追加することにより試作システムの機能拡張が可能である。

- サーバにNAT機能を持たせることによりサブネット内部からの通信も可能にする。
- サーバをマルチホーム（複数の物理ポートを持つホスト）にして、ファイアウォール機能を持たせたセキュリティの向上。
- リースクライアントをマルチホームにすれば、1個の物理ポートのみをグローバルアドレスに設定し、他のポートはプライベートアドレスのままとすることにより、クライアントの利便性が向上する。
- リース期間を設けることもできる。

5．おわりに

今回、アドレス枯渇問題対応策として外部ホストがリースクライアントへのアクセスをリースサーバへ依頼して、クライアントにグローバルIPアドレスを割り当てさせることにより、主としてプライベートアドレスで運用しているサブネット内クライアントに対して、外部ホストからアクセス可能とした。

参考文献

1）Linux magazine12月号，pp.78-80，株式会社アスキー，2001.
2）古田大輔：グローバルIPアドレスリースシステム，電子情報通信学会2001年通信ソサイエティ大会講演論文集2，pp105，2001.
3）W.リチャード・スティーブンス著，篠田陽一訳，UNIXネットワークプログラミング，株式会社トッパン，1999.