

細川 智康 小熊 寿 中山 泰一

電気通信大学 情報工学科

## 1 はじめに

現在、DHCP (Dynamic Host Configuration Protocol) を LAN 等のネットワーク上で用いる事が多くなってきている。DHCP とは、計算機がネットワークサービスを受けるために必要な IP アドレスなどの情報を動的に提供するプロトコルである[1]。

しかし、DHCP を利用したネットワークでは、DHCP を介さずにネットワークを利用する計算機を管理できない。そのため、サーバが管理する IP アドレスと衝突する可能性があり、DHCP クライアントに対するサービスが正しく提供できない。

本研究では、DHCP サーバが提供するアドレス空間を適切に管理するシステムを提案し、実現する。

## 2 DHCP サーバ

DHCP では、サーバは LAN 内の IP アドレスを管理し、クライアントからの要求が来た場合に、適切な IP アドレス情報の配布を行う。そして、配布した IP アドレスの使用状況を調べ、使用されていない IP アドレスの再配布を行っている。提供するアドレスに関しては、MAC アドレスを利用した接続制限を加える事が出来る。しかしこの制限は、プロトコルに従ってサービスを提供された計算機に対してのみ有効で、DHCP を介さない計算機に対しては無効である。つまり DHCP では、サーバはクライアントの計算機に対してのみ管理できるが、それ以外の計算機に対する管理ができない(図1)。

これは DHCP サーバの管理するアドレス情

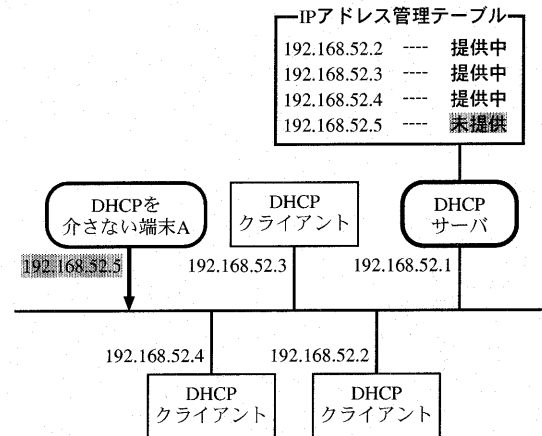


図1 DHCPにおけるアドレス管理

報は、プロトコルに従ったクライアントへの配布を想定し、それ以外での配布を考慮していないためである。この結果、実際にLAN内で利用されているアドレス情報とDHCPサーバの管理しているアドレス情報との間に差が生じる可能性がある。

## 3 アドレス空間管理システム

### 3.1 DHCP サーバによる未使用アドレスの占有

DHCP で IP アドレスを正確に管理するためには、DHCP を介さずにネットワークを利用する計算機に対し、任意の IP アドレスを利用できなくすればよい。この機能を実現するため本稿では、「DHCP サーバによるIPアドレスの一元管理」を行う(図2)。

サーバが提供する IP アドレスを一元管理するために、本研究では 2 つの機能を利用して実現する。

- IP エイリアス
- パケット・フィルタリング

以下本稿では、上記の 2 つの機能した管理システムの実現方法について述べる。

Design of the DHCP server for preventing illegal use of IP addresses

Tomoyasu HOSOKAWA, Hisashi OGUMA and Yasuichi NAKAYAMA

Department of Computer Science, The University of Electro-Communications

E-mail: hosoka-t@igo.cs.uec.ac.jp

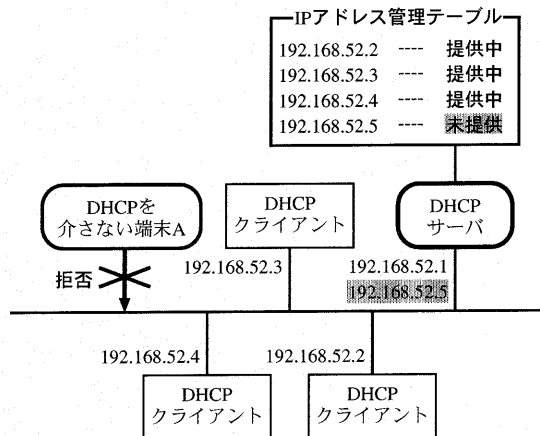


図2 提案するアドレス空間管理システム

### 3.2 実現方法

まず、提供されていないIPアドレスすべてを、DHCPサーバが保持し、提供すべきIPアドレスが勝手に利用されないようにする。

これはIPエイリアスを利用し、サーバの計算機が提供すべきIPアドレスすべてを保持することで実現できる。クライアントからサービス提供の要求が来た場合、サーバは自身が占有していたIPアドレスを開放し、クライアントにそのIPアドレスを与える。

しかしこの方法では、サーバが保持するIPアドレスに対する通信が生じた場合、本来存在しない計算機からの返答が生じる。この結果、ネットワーク内のアドレス情報を乱す事となる。

この問題を解決するために、IPルータでセキュリティのために利用されているパケット・フィルタリングの機能を利用し、サーバが保持しているIPアドレスに対するサービスを拒絶するようにする。

本研究ではフィルタリングツールとして、操作の容易性など理由から、IPファイアウォールを利用する[2]。

本研究で提案するシステムでは、これらの機能を既存のDHCPサーバ内に組み込み、UNIXが標準的に提供する機能を利用して実現する。そのため、クライアント・プログラムやDHCPのプロトコルを一切変更する必要がない。

本研究では、これらの機能をWIDE版DHCPのサーバ内で実現した。

```
# ifconfig r10 192.168.52.2 netmask 25
5.255.255.0
# Jan 13 17:52:49 balvino /kernel: arp
: 00:40:05:a7:f4:34 is using my IP add
ress 192.168.52.2!
# ping 192.168.52.1
PING 192.168.52.1 (192.168.52.1): 56 d
ata bytes
^C
--- 192.168.52.1 ping statistics ---
16 packets transmitted, 0 packets rece
ived, 100% packet loss
#
```

図3 DHCPを介さない計算機によるIP獲得の実験

### 4 評価

実際にDHCPを用いたLANを構築し、動作確認を行った。実験で利用したLANは、DHCPサーバ1台とクライアント1台で構成し、それぞれの計算機で動作するOSをFreeBSDとした。以上の環境にて、DHCPを介さない計算機によるIPアドレスの獲得の実験を行い、獲得できない事を確認した(図3)。

### 5 おわりに

本研究では、DHCPを利用したLAN内に、DHCPを介さない計算機が存在した場合に起きる問題の解決法として、アドレス空間管理法を提案・実現し、DHCPを介さない計算機によるIPの使用を禁止できることを確認した。

しかし、DHCPクライアントによって正しくリリースされなかったIPアドレスは、サーバによって回収されるまで放置されるため、DHCPを介さない計算機によって利用されてしまう可能性がある。このように何らかの理由で放置されてしまったIPアドレスに対する処理が遅れてしまう、という問題がある。どのようにしてIPアドレスの使用状況をリアルタイムで把握するかという事が、今後の課題として挙げられる。

### 参考文献

- [1] R. Droms.: Dynamic Host Configuration Protocol(DHCP), RFC 2131 (1997).
- [2] E. D. Zwicky, S. Copper and D. B. Chapman: *Building Internet Firewalls, 2nd Edition*, O'Reilly & Associates (2000).