

NAT (Network Address Translation)

平成 13 年 4 月 25 日
峯 肇史

1 NAT とは

プライベートアドレスしか持たないような内部ネット上のホストでは、通常はグローバルアドレスを持つ外部のマシンとは通信できない。プライベートアドレスは内部ネットだけで有効で、外部ネットでは、プライベートアドレスは意味を持たないためである。つまり外部のマシンと通信するには、グローバルアドレスが必要となる、そこで、すべてのマシンにグローバルアドレスを割り当てるとこの問題は解決できるが、この解決法は、IP アドレスの枯渇、セキュリティ上の望ましくない(外部から不正アクセスを受ける危険性がすべてのマシンに発生する) と言う点で現実的な解決法ではない。そこでプライベートアドレスを持つ内部マシンからでも、グローバルアドレスを持つ外部マシンと通信できるように IP アドレスの付け換えを行う技術が NAT (Network Address Translation) である。

例を上げると、NAT サーバーは、内部ネットのマシン (eric.4f.db.is.kyuhsu-u.ac.jp : 192.168.33.57) が外部にあるマシン (minako.db.is.kyuhsu-u.ac.jp : 133.5.18.160) に通信しようとする と eric から送信元アドレスが 192.168.33.57 で送信先アドレスが 133.5.18.160 であるパケットがまず送信される。このパケットは Defaultrouter である yumi/ami(192.168.33.1/133.5.18.197)(NAT サーバー) に送られ、ここで IP の付け換えが行われる。yumi が eric から受け取ったパケットの送信元アドレスを 133.5.18.197 に変更して、ami から送信されたパケットとして minako に送信する。このとき ami はこの変換をある一定期間覚えておき、minako からパケットが戻ってくると、それが先ほど NAT でアドレス変換したものであると確認されるとそのパケットの送信先アドレスを 192.168.33.57 に変更し eric に送信する。このような NAT サーバーの動作により内部ネットから外部へ通信が可能となる。

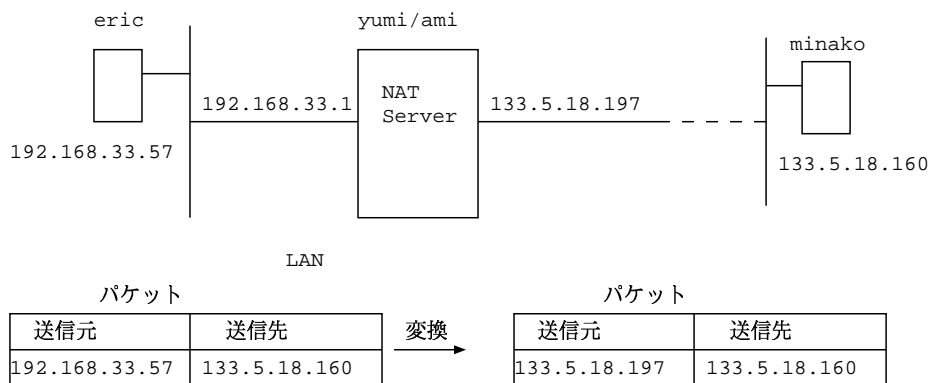


図 1: NAT での変換例

2 研究室の NAT サーバー

研究室では、NAT サーバは 4 階では yumi/ami , 3 階では yoda/luke が行っている。

3 NAT サーバーの設定

1. 以下の Option をつけてカーネルを再コンパイルする。
options IPFIREWALL
options IPDIVERT
2. /etc/rc.conf に以下の一行を加える。
gateway_enable="YES"
3. natd を立ち上げる。
% natd -interface tx0
ここで、tx0 は外部用のネットワークカードである。/etc/rc.conf に以下の行を加えておくと起動時に、natd を起動してくれる。natd_enable="YES"
natd_interface="tx0"
4. /etc/rc.firewall を以下のコマンドが実行されるように書き換える。
/sbin/ipfw -f flush
/sbin/ipfw add divert natd all from any to any via tx0
/sbin/ipfw add pass all from any to any
5. /etc/rc.conf に 以下の 1 行を追加。
firewall_enable=YES
この行を追加することにより、起動時に/etc/firewall に書いてあるスクリプトが実行される。

4 実習

NAT サーバーは、LAN を構築する必要もあるし、ネットワークカードも 2 枚必要なので、実習で NAT サーバを構築するのは大変です。そこで今回は、外部ネットワークに接続するときには、NAT サーバーを通して接続していることを確かめてください。以下のコマンドを実行します。

```
% traceroute minako
```

一度、yumi を経由して minako につながっているのがわかると思います。