分散システム／インターネット運用技術 15－1
（1999．9．24）

プライベートネットワークアドレスを利用する際の経路制御について

吉浦紀晃†、桜井成一朗†、坂本直志‡、藤本衛‡

† 東京工業大学 情報理工学研究科 計算工学専攻
‡ 東京工業大学 情報理工学研究科 数理・計算科学専攻

IPアドレスの枯渇やセキュリティーの問題からプライベートアドレスの広く利用されている。本稿では、パブリックネットワークアドレスを利用しているキャンパスネットワークにプライベートネットワークを併用し、双方で通信可能なネットワークとして運用する場合の特に経路制御の問題と運用例について述べる。この問題を解決するためには、プライベートネットワークとの通信の中継をするルータがすべて可変長サブネットマスクに対応していることと、サブネットマスクを伝搬する経路制御プロトコルを利用する必要がある。さらに、経路の爆発を防ぐためにプライベートアドレスの割り振り方や現在判明している問題について述べる。

Routing Control for a network including public address and private address networks

Noriaki Yoshiura†, Seichiro Sakurai†, Naoshi Sakamoto‡ and Kou Fujimoto‡

†Department of Computer Science, Tokyo Institute of Technology
‡Department of Mathematical and Computing Sciences, Tokyo Institute of Technology

Private network address is a temporary solution for exhaustion of the 32-bit IP address space. From the view of network security, private network addresses have been also used in many sites. This paper presents one example of administrating campus network in which public address networks and private address networks coexist. One of the problems in such an administration is control of routing and it is necessary for solving this problem that all routers for private address network deal with variable length subnet mask (VLSM) and routing protocol handling VLSM.

1 はじめに

現在、IP アドレスは、世界的に枯渇している。この問題に対する長期的な対策としては、IPv6[7] などがあるが、暫定的な解決策としては、プライベートアドレス [4] の利用が提案されている。

一方、ここ数年インターネットを利用して不正侵入を試みるという行為が頻発している。また、不正侵入されたサイトから更に他のサイトへの不正侵入も頻発している。プライベートアドレスはこのような試みを防止するという利点もある。

これらの点から、プライベートネットワークが広く利用されているが、プライベートネットワークと一般のパブリックネットワークとの通信を行なう場合には、NAT[2] や Proxy などのサーバが必要になる。

一方、大学などのネットワークでは、日常利用するコンピュータがある場所と実験を行なう場所が異なる建物にある場合がある。このような場合、実験を行なう建物に端末を置き、そこから、実際に利用するコンピュータへアクセスできれば十分である。よって、端末にはプライベートアドレスを割り当てれば十分であるが、この場合、大学内で利用しているパブリックネットワークとプライベートネットワークとが通信可能であることが必要である。

また、学内全体の Proxy サーバを利用する場合には、利用者の端末はプライベートネットワークでよいが、この場合も、プライベートネットワークから大学内で利用しているパブリックネットワークへの通信が必要になる。

そこで、本稿では、あるサイト内全体で利用可能なプライベートネットワークを用意し、そのサイト内では自由に通信可能となる運用について述べる。プライベートネットワークはパブリックネットワークの末端部分に利用されている場合が多いが、本稿で扱うプライベートネットワークの形態は、パブリックネットワークとプライベートネットワークとが混在しているネットワークであり、このような例はあまり見かけない。この形態のネットワークでは、経路制御が問題となる。

そこで、本稿では、以下では、2 章で、今回の運用例である東京工業大学におけるネットワークの状況を説明し、3 章で、議論のために必要な知識の説明を行う。4 章で、経路制御に関する問題とその解決策を述べ、5 章で、本稿をまとめる。

2 東工大のネットワークの状況

2.1 東工大のネットワーク構成

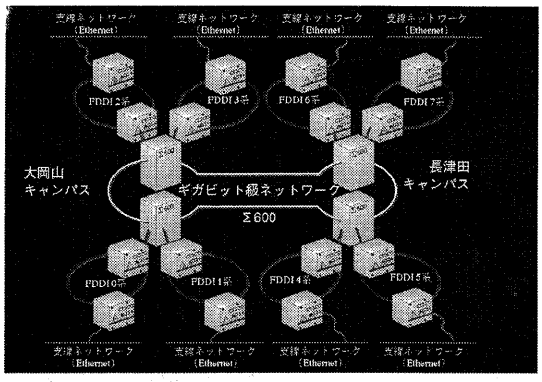

図 1: 東工大ネットワーク構成図

東工大のネットワークは、図 1 のような構成をしている。各建物にルータを配置し、これらのルータが 8 つの FDDI リングを構成しこれらの FDDI リングがバックボーンに接続するという構成である。以下では、この部分を幹線ネットワークと言う。この幹線ネットワークを東京工業大学 Network Operation Center(以下、NOC と略す) が管理している。一方、建物のルータに接続している建物内のネットワーク (以下では、支線ネットワークと言う) は、各専攻、学科、研究室が独自に構成し、管理している。よって、NOC は、建物内のネットワークトポロジーを管理しておらず、また、完全には把握していない。

東工大では、クラス B のアドレス (131.112/16) を 26 ビットサブネットマスクで利用しており、アドレスの割り当ては NOC が行っている。また、経路制御に関しては、幹線ネットワーク、支線ネットワークともに RIP[1][1]を利用している。

2.2 プライベートアドレスの利用方針

ネットワークの普及により、これまでネットワークを利用していなかった専攻や学科がネットワー

[1]現在は OSPF である。

クを利用し始め、学内においてもIPアドレスの枯渇という問題が起こっている。

この問題に対応するため、NOCでは、次の方針でプライベートアドレスの運用を開始した。

1. クラスAのプライベートアドレス(10.0.0.0/8)は当面利用しない。
2. クラスBのプライベートアドレス(172.16/12)は、学内プライベートアドレス、つまり、131.112/16や172.16/12と通信可能なアドレスとして利用し、サブネットマスクは、26ビットとする。利用する際には、アドレスを割り当てをNOCから受ける。
3. クラスCのプライベートアドレス(168.192/16)は、各支線ネットワークで自由に利用してもよい。

上記のように、172.16/12のアドレスは、東工大内部では自由に通信できるものであり、このため、131.112/16と172.16/12の26ビットサブネットマスクのサブネットが混在したネットワークにおいて任意のどのアドレス間も通信できるようにしなければならない。しかしながら、経路制御の問題があって、従来の運用では、172.16/12のネットワークと131.112/16のネットワークの間の通信が不可能であった。以下では、その問題点と解決策を述べるが、そのために必要な知識を説明する。

3 準備

ここでは、議論を展開するために必要な概念について説明をする。

3.1 RIP

RIPversion1は、広く利用されているrouting protocolである。RIPversion1では、各ルータが経路を知っているネットワークのアドレスをメトリックとともに伝搬する。しかし、そのネットワークのサブネットマスクを伝搬することはない。サブネットマスクを伝搬させることができる経路制御プロトコルとしては、RIPversion2[6]やOSPF[5]などがある。

3.2 Routing Table

ネットワークアドレスとルータ(ゲートウェイ)の組の列をルーティングテーブルと呼ぶ。このルーティングテーブルの構成は、BSD4.3以前とBSD4.4以降では異なる。

BSD4.3以前では、ルーティングテーブルは、ネットワークアドレスとルータ(ゲートウェイ)の組の列によって表現される。

一方、BSD4.4以降では、ルーティングテーブルは、ネットワークアドレスとネットマスクとルータ(ゲートウェイ)の組によって表現され、可変長サブネットマスクに対応している。

3.3 Packet Forwarding

ルータは、送られてきたパケットをその宛先をみて、どのルータ(ゲートウェイ)へ配送するかを決定する。この操作をPacket Forwardingと呼ぶ。BSD4.3以前では、Packet Forwardingは以下の手順によって行われる。

1. ルーティングテーブルに、宛先アドレスがあるならば、そのルータにパケットを送る。
2. ルーティングテーブルに、宛先アドレスがない場合、宛先アドレスが自分のインターフェイスのアドレスと同じネットワークアドレスに属するならば、そのインターフェイスのサブネットマスクから、宛先アドレスの属するサブネットを見つけ、そのサブネットがルーティングテーブルにある場合は、そのゲートウェイへパケットを送る。
3. 上記のいずれにも該当しない場合には、デフォルトゲートウェイへパケットを送る。

一方、BSD4.4以降では、Packet Forwardingは以下の手順で行なわれる。

1. ルーティングテーブルに、宛先アドレスがあるならば、そのゲートウェイにパケットを送る。
2. ルーティングテーブルに、宛先アドレスがない場合、ルーティングテーブルの各エントリの経路とマスクのビット積と宛先アドレスとマスクのビット積とが一致するものがあれば、そのエントリのルータへパケットを送る。一致するものが複数存在する場合には、マスク

が長いものを利用する。

3. 上記のいずれにも該当しない場合には、デフォルトゲートウェイへパケットを送る。

このようにBSD4.4では、ルーティングテーブルで、マスクを利用することができるため、可変長サブネットマスク (VLSM)[3] に対応できる。

4 プライベートネットワークアドレスの経路制御

4.1 問題点

パブリックアドレスとプライベートアドレスが混在したネットワークで、クラスBのプライベートアドレス172.16/12を、ナチュラルマスク以外で利用する場合には、例えば、26ビットサブネットマスクで利用するには、経路制御の問題が生じる。

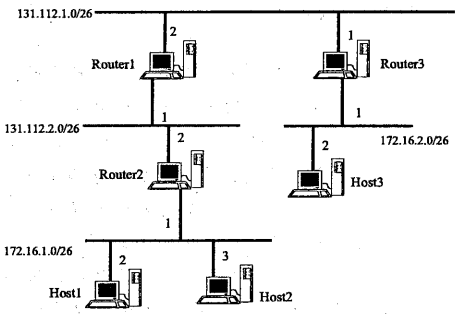

図2: プライベートネットワーク間の通信がうまくいかない場合

図2のようなネットワークでは、Router1、Router2、Router3がVLSM対応ではなく、ルーティングプロトコルとしてRIPversion1を利用している場合、各ルータのルーティングテーブルは、表1のようになる[2]。

Router1から、172.16.2.2へ通信を行おうとすると、Router1は、ルーティングテーブルから次の作業により、配送先を決定する。

1. 172.16.2.2が自らがもつnetwork interfaceのIPアドレスと同じネットワークに属するかどうか調べ、そうではないと判断する。
2. 172.16.2.2は、172.16.2.2の属するネットワークのサブネットマスクを知らないので、ナチュラルマスクをサブネットマスクとして利用する。
3. 172.16.2.2にサブネットマスクをかけたものである。172.16.0.0をルーティングテーブル上に探す。
4. サブネットマスクを利用して172.16.2.2とマッチするものを2つ見つけ出す。いずれも同一ホップ数であるため、上位にある131.112.2.2へパケットを送る。

Router1のルーティングテーブル

目的地	ゲートウェイ	ホップ数
172.16.1.0	131.112.2.2	1
172.16.2.0	131.112.1.1	1
131.112.1.0	直接接続	0
131.112.2.0	直接接続	0

Router2のルーティングテーブル

目的地	ゲートウェイ	ホップ数
131.112.1.0	131.112.2.1	1
131.112.2.0	直接接続	0
172.16.2.0	131.112.2.1	2
172.16.1.0	直接接続	0

Router3のルーティングテーブル

目的地	ゲートウェイ	ホップ数
131.112.1.0	直接接続	0
131.112.2.0	131.112.1.2	2
172.16.1.0	131.112.1.2	2
172.16.2.0	直接接続	0

表1:

このようにして、Router1はどのルータへパケットを送るかを決定するが、131.112.2.2の方面には、172.16.2.2のホストは存在しないので、通信を行うことはできない。このことから、172.16.1.0/26と172.16.2.0/26の間の通信が不能となる。

これは、Router2からRouter1へ、そして、Router3からRouter1へ送られるRIPversion1による経路情報にサブネットマスクが含まれていないこと、そして、Router1がルーティングテーブ

[2]この点は、実装によって異なるが、どの場合でも、パケットフォワードはうまくいかない。

ルにサブネットマスクを持っていないことが原因である。

4.2 解決策

上記のように、プライベートアドレスとパブリックアドレスとを混合して利用する場合には、上記のような2つの問題を解決する必要がある。

そのためには、

- ルータをVLSM対応とすること
- ルーティングプロトコルとして、サブネットマスクを伝搬させるものを利用すること。

の2点があげられる。

VLSM対応OSとしては、FreeBSD2.2.7、Linux, Windows NT4.0, Solaris2.6がある。しかしながら、現状のネットワークを構成しているマシンは、すべてがVLSM対応OSとはかぎらず、また、管理組織が異なるので、すべてのリプレースは無理である。しかし、幹線ネットワークのルータはすべてVLSM対応している。

サブネットマスクを伝搬させるルーティングプロトコルとしては、RIPversion2やOSPFがあり、いずれを使ってもよい。ただ、現在幹線ネットワークを構成しているルータには、RIPversion2を利用できないものもあるので、OSPFを利用することとした。これにより、172.16/12のネットワークの経路情報を幹線ルータで交換することとした。

また、支線ネットワークとの経路交換は現状のままRIPversion1を利用するしかないので、建物にある幹線ルータで、静的に経路を設定し、プライベートネットワークに直接接続しているルータと建物ルータの間にあるルータは全てVLSM対応となっている場合に、プライベートネットワークの利用を認めた。

4.2.1 運用方法

運用方法をまとめると次のようになる。

1. プライベートネットワークを利用したい場合は、NOCへ申請する。
2. NOCでは、そのプライベートネットワークとそのネットワークがある建物の幹線ルータまでの間の通信で通過するルータが全てVLSM対応のルータであるかどうかを確認し、そうである場合は、NOCはアドレスを割り当てる。
3. そのプライベートネットワークが存在する建物にある幹線ルータで、プライベートネットワークへの経路を静的に設定する。
4. 静的に設定した経路は幹線ネットワークにOSPFで配送し、支線ネットワークへはプライベートネットワークの経路を配送しない。
5. 建物にある幹線のルータからプライベートネットワークまでの間のルータでは、静的にまたはRIPversion2などでプライベートネットワークへの経路情報を設定する。

4.2.2 通信の方法

このような状況での通信の仕方を述べる。あるプライベートネットワークから学内のパブリックネットワークへの通信は、パブリックネットワークの経路が支線に送られているのでその経路を利用してパケットが配送される。

一方、支線ネットワークへはプライベートネットワークの経路情報を送っていないので、パブリックまたはプライベートネットワークからプライベートネットワークへの通信は次のように行われる。

1. プライベートネットワーク宛の場合、支線ネットワークへは経路がないので、デフォルトの経路を通って、建物の幹線のルータへパケットが届く。
2. 建物の幹線のルータはOSPFによって経路交換しているので、宛先であるプライベートネットワークのある建物の幹線ルータへパケットを送る。
3. 幹線ルータでは、静的にプライベートアドレスの経路が設定されているので、その経路へプライベートネットワーク宛のパケットを送る。

具体的には、図3のようになる。

4.2.3 IPアドレスの割り振り方

172.16/12のプライベートアドレスと26ビットサブネットマスクで利用すると、最大で、16384個のサブネットを利用することが可能であり、この場合、各ルータのルーティングテーブルもこの大きさになる。現在利用しているルータが非常に非

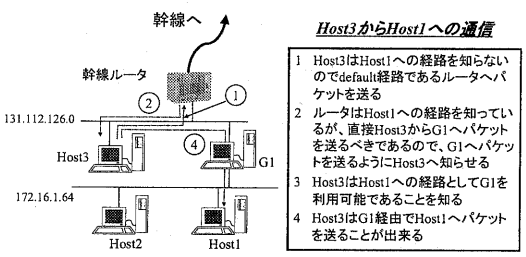

図 3: プライベートネットワークへの通信の流れ

力であることを考えるとルーティングテーブルの大きさを極力小さく押える必要がある。よって、以下のようにIPアドレスの割り振り方を次のように工夫し、経路集約を行った。

1. 各FDDIリング単位で利用するクラスBのプライベートネットワークアドレスを割り振る。
2. 各建物単位で利用するネットワークアドレスを24ビットサブネットマスク単位で割り振る。
3. バックボーンには、これらの集約した経路情報を流す。

これにより、各FDDIリング内には、プライベートアドレスに関して、最大で256個の経路情報が流れ、バックボーンには、8つの経路情報が流れる。

4.2.4 運用の際の問題点

現在判明している問題としては、RIPとOSPFの変換による問題がある。上記の運用では、幹線ネットワークから受け取ったOSPFの経路情報を、支線ネットワーク側へはRIPversion1を流すことになっているが、支線側で、split-horizonを実装していない経路制御デーモン、例えば、BSD4.4のroutedなどが稼働している場合、あのネットワークが落ちている場合、split-horizonを実装していないデーモンはその経路を幹線側へ流してしまう。さらに、この経路を受け取った幹線ルータはOSPFとして伝搬させてしまう。この場合、消えた経路が永久に残ってしまう。

この問題に対しては、支線ネットワークにデフォルトの経路のみをRIPで送る、支線から来るRIPの経路にフィルターをかける、支線内にBSD4.4のroutedを廃止するなどの方法があるが、デフォルトの経路をのみをRIPで送るが最も良い解決策である。

5 おわりに

今後、VLSM対応のOSが増加することが考えられるので、それに伴い順次、プライベートアドレスの経路を静的に設定しているが、これを動的なものに変えることが可能になると考えられる。今回示した運用方法はあくまでも、古いルータやOSが新しいものになるまでの暫定的なものであり、理想的には、すべてのルータ(ゲートウェイ)がVLSM対応で、RIPversion2やOSPFを利用できることである。

また、セキュリティのことを考えると、徐々にプライベートネットワークへの移行を行い、大学のネットワークにあるパブリックアドレスを極力少なくしていくことが望ましい。よって、そのための移行方法の一つであるとも考えられる。

参考文献

[1] C.L. Hedrick. , Routing Information Protocol., RFC1058, (1988).

[2] K. Egevang & P. Francis., The IP Network Address Translator (NAT)., RFC1631, (1994).

[3] T. Pummill & B. Manning., Variable Length Subnet Table For IPv4., RFC1878, (1995).

[4] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot & E. Lear., Address Allocation for Private Internets., RFC1918, (1996).

[5] J. Moy., OSPF Version 2., RFC2328, (1998).

[6] G. Malkin., RIP Version 2., RFC2453, (1998).

[7] S. Deering, R. Hinden. December 1998., Internet Protocol, Version 6 (IPv6) Specification., RFC2460, (1998).