高知地域指向疑似 IX の課題と解決法

西内 一馬, 杉山 道子, 廣瀬 崇夫
正岡 元, 菊池 豊

高知工科大学 情報システム工学科

概要

地域指向のインターネットトラフィック交換方式に PIX モデルがある。本モデルは、既に実験段階に入っている。実験を開始するにあたり、様々な課題がある事が判明した。

その一つが、プライベートアドレスの衝突である。もう一つは、既存のネットワークの上に別のアドレス空間を持つ PIX モデルを導入する際への問題である。本稿では、前者に NAT を後者に IP トンネリングを用いて解決する手法を提案する。また、実験ネットワーク PicoIX での具体例を示す。

Issues of design PIX and their solutions

NISHIUCHI Kazuma, SUGIYAMA Michiko, HIROSE Takao
MASAOKA Hajime, KIKUCHI Yutaka

Department of Information Systems Engineering, Kochi University of Technology

Abstract

PIX is a region oriented model for exchanging traffic of the Internet. This model already has been experimented on a real network named KPIX. When we started the experiment, various issues had turned out.

One is conflict of private addresses of connecting networks. The other is how to install a PIX independently on an existing network. This paper presents some solutions of the issues, which use NAT and IP tunneling respectively. We will show some examples of the solutions on our small experimental network called "PicoIX".

1 はじめに

著者らはインターネットトラフィック交換モデルである PIX モデルを提唱した [1]。また高知県において、地域情報化プロジェクトである Kochi 2001 Plan の下に、県内の産官学の共同で「KPIX 実験研究協議会」を 1997 年 7 月に組織し、実験を行っている [2]。KPIX とは、 "Kochi Pseudo Internet eXchange" の事である。

KPIX の設計を通して、ネットワークを構成する際にいくつかの課題がある事が判明した。

本稿では、まず第 2 節で PIX モデルの基本概念を述べる。次に、第 3 節で KPIX を実験する際に問題となった事例を挙げる。具体的には、一つはプライベートアドレスの衝突である。もう一つは、既存のネットワークの中に別のアドレス空間を持つ PIX モデルを導入する際の手法である。そして、第 4 節でその解決案を提案する。第 5 節では、第 4 節で挙げた問題点への解決法を実験ネットワーク PicoIX 上の具体的な設定例で説明する。第 6 節では、まとめを行う。

2 PIX モデルの基本概念

PIX (Pseudo Internet eXchange) モデルの簡単な特徴をここで述べる [1] 。

PIX モデルとは IX モデルに代わるインターネットトラフィック交換モデルのことである。PIX モデルでは、地域内に閉じたイントラネットを構成し、インターネットとイントラネットとのトラフィックの交換は全てアプリケーション層で行う。また、グローバル IP アドレスが必要な部分は、ISP とのゲートウェイのみである。他のホストはプライベートアドレスで構わない。

2.1 特徴

PIX モデルの特徴として、 IX と比較すると

- 管理者に要求される技術水準が低い
- 管理者間の協調・調整に対する労力の軽減
- 小さな地域コミュニティにも対応できる
- 影響が及ぶ範囲が小さい

ということが挙げられる。しかし、 PIX モデルでは

- 交換できないプロトコルが存在する
- DNS が複雑になり設定が難しい

といった欠点がある。

2.2 コンテンツの共有

PIX モデルは、地域におけるイントラネットの性格が強いため、同一ページの重複転送が多いと予想する。そして、HTTP コンテンツがインターネットトラフィックの大部分を占めているため、HTTP コンテンツを PIX 内で共有する。HTTP コンテンツを共有する事で、各 PIX 参加組織が独自でインターネットと繋がっている専用線への負荷を軽減する事ができる。

次の段階では HTTP キャッシュの様な蓄積型のアプリケーションだけでなく、ストリーム型のアプリケーションにも対応する。

2.3 インターネット側と IP の交換は行わない

PIX モデルを構成している場合、インターネット側から見ると、PIX モデルを構成している組織がそれぞれ ISP 経由でインターネットに接続されているようにしか見えない。同様に、PIX モデルの内側から見ると、いくつかの LAN が PIX モデルを使い、インターネットに繋がっているようにしか見えない。これにより、PIX モデル内での混乱が生じた場合、その影響が PIX モデルの外に伝搬する事は無い。

3 PIX の問題点

ここでは、 KPIX の設計の際に問題となった 2 つの課題について述べる。

3.1 プライベートアドレス枯渇問題

PIX モデルはプライベートアドレスを用いて各参加組織をつなぐ。そのため、全参加組織が使用

していないプライベートアドレスを見つけだすことが必要となってくる。全参加組織が使用していないプライベートアドレスがある場合は、そのプライベートアドレスを使用すれば問題なく PIX モデルに移行できる。しかし、プライベートアドレスは各組織毎、自由に使用しているため、参加組織が使用しているプライベートアドレスが重複する場合がでてくる。また重複していない場合でも、空きがいわゆる「虫食い」状態になっていて必要な大きさの空間を確保できない場合がある。

3.2 既存のネットワークと管理を独立にする

現在、運営している IP ネットワークがあり、そのネットワークを PIX モデルで使用としたとする。この時、IP ネットワークと PIX が構成するネットワークのポリシーが異なるなどの理由で管理上互いに独立のネットワークにしたい場合がある。

4 PIX における問題点への解決法

ここでは前節で述べた問題点に対する解を与える。

4.1 プライベートアドレス枯渇問題への解決法

NAT (Network Address Translation) とは、IP アドレス空間においてグローバルアドレス空間とプライベートアドレス空間を接続するための技術である。

この技術を用いて、各参加組織が使用していないプライベートアドレスと PIX 用のプライベートアドレスを「1 対 1」静的対応させる事で、PIX 内からはある一つのプライベートアドレスを使用しているかのように見せる事ができる。

また、分散しているプライベートアドレスを NAT を用いて整理する事で管理が容易になる、大きなプライベートアドレス空間を作る事ができる、といった特徴もある (図 1)。

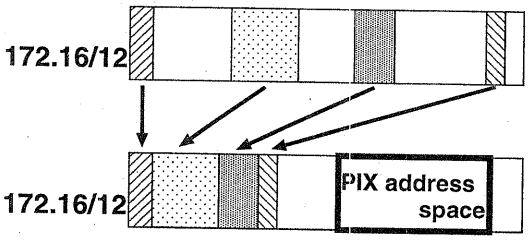

図 1: プライベートアドレス空間の整理

4.2 他の IP ネットワークを PIX モデルのデータリンクにする方法

IP トンネリングとは、パケットをカプセル化して間に挟むネットワークを暗号化トンネルとする技術である。

既存のネットワークを利用して、PIX モデルを構築しようとした場合、ルータの持つ IP トンネリング機能を用い、既存のネットワークを PIX のデータリンクとして使う事が可能である。

トンネリングをすると、パケットをカプセル化するため、IP パケットの通路となるネットワークを意識せずに使用できる。そのため、あたかも一つのルータで PIX のネットワーク同士が繋がっているかのように見せる事ができる (図 2)。

5 実験ネットワーク

第 4 節で挙げた、NAT によるプライベートアドレスの整理, トンネリングインタフェースによる異なるアドレス空間を共存させるための設定を実際に行い、この様な実装が可能であるか確認する為、実験ネットワークを構築した。

これを、“ PicoIX ” と呼ぶ。Pico IX はネットワークを 4 つ、ルータ 3 つを持ち、100baseTX で繋がっている。ネットワークは SW-HUB のみで構成されている。各ルータは RIP を用いて経路情報のやりとりをおこなう。

線形に 3 つのルータで繋がったネットワークの名前を左から P, I, C, O とする。ルータの名前を

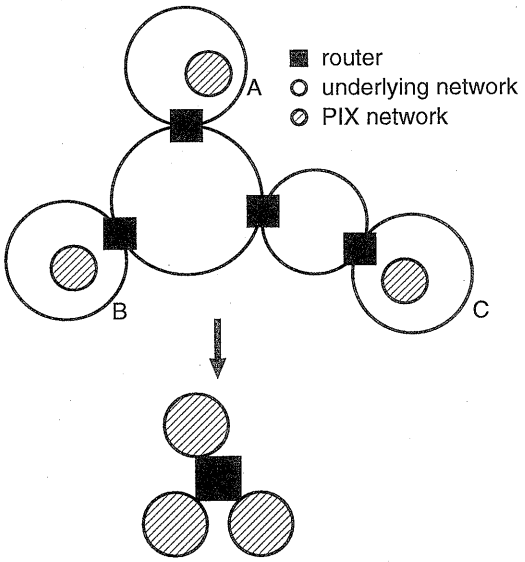

図 2: 既存のネットワークをデータリンクとして用いる

左から Upper, Middle, Lower とする (図 3)。

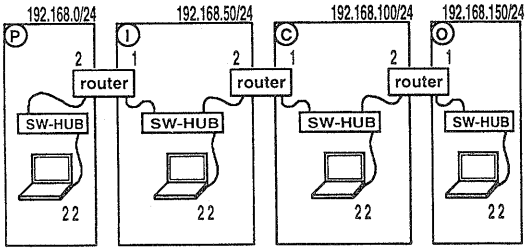

図 3: PicoIX の構成

5.1 NAT 機能を使うための設定例

中央にあるルータ Middle の設定例を挙げる。なお、ここで挙げるコマンドは YAMAHA のルータ独自のコマンドである [3]。

ここでは、ネットワーク I のホスト群 192.168.50.22 – 31 を 192.168.1.22 – 31 と見えるようにし、ネットワーク C のホスト群 192.168.100.22 – 31 を 192.168.2.22 – 31 と見えるように設定をした (図 4)(図 5)。

種類	メーカ	名前
router	YAMAHA	RT140e
SW-HUB	Allied Telesis	FS708 FS708XL

表 1:

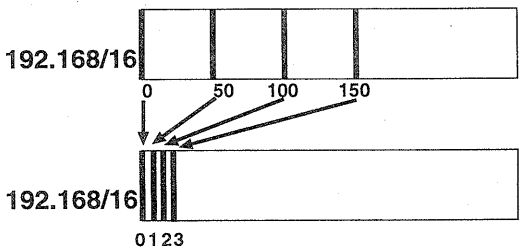

図 4: NAT アドレス空間

［ルータ Middle の設定］

1. ip lan1 address 192.168.100.1/24
2. ip lan1 nat descriptor 1
3. ip lan2 address 192.168.50.2/24
4. ip lan2 nat descriptor 2
5. nat descriptor type 1 nat
6. nat descriptor address outer 1 192.168.1.22
7. nat descriptor address inner 1 192.168.50.22
8. nat descriptor static 1 1 192.168.1.22 = 192.168.50.22 10
9. nat descriptor type 2 nat
10. nat descriptor address outer 2 192.168.2.22
11. nat descriptor address inner 2 192.168.100.22
12. nat descriptor static 2 1 192.168.2.22 =

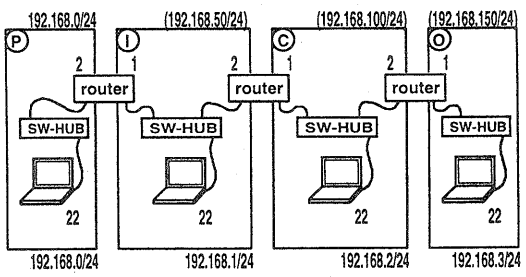

図 5: PicoIX + NAT

192.168.100.22 10

［ルータ Middle の設定解説］

1. ルータの lan1 のアドレスを 192.168.100.1 に、繋がるネットワークを 192.168.100/24 にする
2. lan1 の NAT ディスクリプタ番号を 1 にする
3. ルータの lan2 のアドレスを 192.168.50.2 に、繋がるネットワークを 192.168.50/24 にする
4. lan2 の NAT ディスクリプタ番号を 2 にする
5. NAT ディスクリプタのタイプを NAT ディスクリプタ番号に設定
6. ルータの外側 IP アドレスを選択
7. ルータの内側 IP アドレスを選択
8. IP の対応を決定する。ここでは、10 台のホストが静的 NAT 対応する
9. NAT ディスクリプタのタイプを NAT ディスクリプタ番号に設定
10. ルータの外側 IP アドレスを選択
11. ルータの内側 IP アドレスを選択
12. IP の対応を決定する。ここでは、10 台のホストが静的 NAT 対応する

5.2 トンネル機能を使うための設定例

PicoIX をデータリンクとして、その上に仮想的に FemtoIX を構成する。図 6 で破線で描いてあるホストは FemtoIX のホストである。

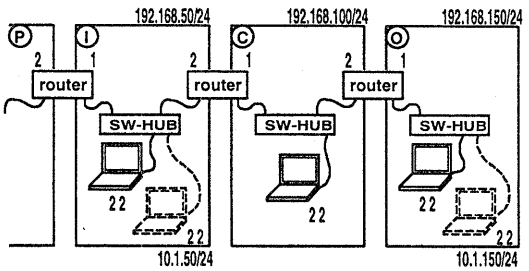

図 6: PicoIX + IP tunneling

ここでは、ネットワーク I の中に新たに 10.1.50/24 というネットワーク、ネットワーク O の中に新たに 10.1.150/24 というネットワークを構成し、その新たに構成されたネットワーク (FemtoIX) 同士をトンネリングインタフェースを用いて接続する例を挙げる。この時、ネットワーク C から FemtoIX のパケットは、暗号化されているため読む事ができない [4]。

設定時の注意として、ルータが 2 つ以上のネットワークを繋いでいる場合が挙げられる。この場合、事前共有鍵や IKE (Internet Key Exchange), SA [1](Security Association) の届け先は、経由する組織の中から見た最も到達地点に近いゲートウェイとなる。トンネルのルートには、トンネリングインタフェースを通過して到達させたいネットワークアドレスを指定する。

この例では、ルータ Middle には 192.168.100.2 を指定し、ルータ Lower には 192.168.100.1 を指定すればよい。

［ルータ Middle の設定］

1. ip lan1 address 192.168.100.1/24
2. ip lan2 address 192.168.50.2/24
3. ip lan2 secondary address 10.1.50.2/24
4. ipsec auto refresh on
5. ipsec pre-shared-key 192.168.100.2 text picoix
6. ipsec ike remote address 1 192.168.100.2
7. ipsec sa policy 78 192.168.100.2 esp des-cbc md5-hmac
8. tunnel select 1
9. ip tunnel route add net 10.1.150.0/24 1
10. ipsec tunnel 78
11. tunnel enable 1

［ルータ Middle の設定解説］

1. ルータの lan1 のアドレスを 192.168.100.1 に、繋がるネットワークを 192.168.100/24 にする
2. ルータの lan2 のアドレスを 192.168.50.2 に、繋がるネットワークを 192.168.50/24 にする
3. ルータの lan2 のセカンダリアドレスを 10.1.50.2 に、繋がるネットワークを 10.1.50/24 にする
4. SA を自動更新する
5. 相手側セキュリティゲートウェイに対する事

[1]鍵に関する情報を集めたもの

前共有鍵の設定. この場合、 picoix となる
6. 鍵交換要求を受け付けるセキュリティゲートウェイを設定する
7. 相手側のセキュリティゲートウェイに対するSA のポリシーを設定する
8. トンネルインタフェース番号の選択
9. 相手側のセキュリティゲートウェイが接続しているLAN への static なトンネル経路情報を設定する
10. 使用する SA のポリシーを選択する
11. トンネルインタフェースを有効にする

[ルータ Lower の設定]

1. ip lan1 address 192.168.150.1/24
2. ip lan1 secondary address 10.1.50.1/24
3. ipsec auto refresh on
4. ipsec pre-shared-key 192.168.100.1 text picoix
5. ipsec ike remote address 1 192.168.100.1
6. ipsec sa policy 78 192.168.100.1 esp des-cbc md5-hmac
7. tunnel select 1
8. ip tunnel route add net 10.1.50.0/24 1
9. ipsec tunnel 78
10. tunnel enable 1

[ルータ Lower の設定解説]

設定の方法は、ルータ Middle の場合と同様である。

6 まとめ

PIX モデルにおける課題と NAT と IP トンネリングを用いた解決法、さらにその設定例について述べた。今後は、これを KPIX に応用した設定をしていきたい。

今回は、 PicoIX を用いて NAT ・ IP トンネリングの実験をおこなった。これにより小規模なネットワークで実現性を示す事ができた。しかし、これを大規模な KPIX に用いた場合にうまく機能するのか、NAT と併用して使用する事による弊害はあるのか、などの課題が残されている。

また、複雑になると分かっている DNS をどのように設定するのか、HTTP コンテンツをキャッシュする squid をどのように設定すれば最も効率の良い結果が期待できるか、といった課題もある。後者については [5] で発表する予定である。

参考文献

[1] 菊池豊, 菊地時夫. 応用層によるインターネットトラフィック交換モデル. コンピュータソフトウェア, Vol. 16, No. 4, pp. 46–58, July 1999.

[2] 菊池豊, 菊地時夫ほか. 高知応用層交換所の構築. 情報処理学会研究報告, pp. 49–54. 分散システム運用技術研究会, may 2000. ISSN0919-6072.

[3] RT シリーズの資料庫/文書庫. http://www.rtpro.yamaha.co.jp/RT/docs/.

[4] Elizabeth Kaufman and Andrew Newman. IPsec 導入の手引き. 翔泳社, 2000.

[5] 正岡元, 杉山道子, 西内一馬, 廣瀬崇夫, 菊池豊, 菊地時夫. 高知地域指向疑似 IX における WWW サーバ群の構成. 情報処理学会研究報告. 分散システム運用技術研究会, dec 2000. ISSN0919-6072, to appear.