社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－ＱＡＩ－21（10）
2006／10／24

公衆無線インターネットみあこネット3に対応したブロードバンドルータの実装

藤川 賢治† 古村 隆明†† 岡部 寿男††

†† 京都大学 〒606-8501 京都市左京区吉田本町
† ルート株式会社 〒141-0031 東京都品川区西五反田7-21-11 第2 TOC ビル8F
E-mail: †fujikawa@root-hq.com, ††{komura,okabe}@media.kyoto-u.ac.jp

あらまし 我々は、公衆無線インターネットプロジェクト、「みあこネット」を推進している。みあこネットプロジェクトでは、誰もが何処に居ても自由にそして安全にインターネットを利用できる環境を作ることを目的としている。みあこネットでは、これまでの実検・運用を踏え、現在、VPNサーバを分散化させた、「みあこネット3」方式を展開している。本稿では、無線ブロードバンドルータとVPNサーバ機能とを併持ったみあこネット3方式対応ルータの実装に関して述べる。
キーワード 無線インターネット, みあこネット, みあこネット3, VPN, PPTP

Implementation of A Broadband Router Supporting Public Wireless Internet MIAKO.NET 3

FUJIKAWA KENJI†, KOMURA TAKAAKI††, and OKABE YASUO††

†† Kyoto University Yoshida-Honmachi, Sakyo-ku, Kyoto, 600-8501 Japan
† ROOT INC. 2nd TOC Bldg., 7–21–11, Nishi-GoTanda, Shinagawa-ku, Tokyo, Japan
E-mail: †fujikawa@root-hq.com, ††{komura,okabe}@media.kyoto-u.ac.jp

Abstract We have been promoting a wireless Internet project *MIAKO.NET*, under which anyone can have access to the Internet anywhere without restriction and with security. After the past experiences of experiments and management of MIAKO.NET, we are now developing the *MIAKO.NET 3* method, which locatess VPN servers distributedly. This paper shows an implementation of a router, which supports the MIAKO.NET 3 method, and has the functions of a broadband router and a VPN server.
Key words Wireless Internet, MIAKO.NET, MIAKO.NET 3, VPN PPTP

1. はじめに

我々は、公衆無線インターネットプロジェクト、みあこネットプロジェクトを推進している。[1] みあこネットプロジェクトでは、誰もが何処に居ても自由にそして安全にインターネットを利用できる環境を作ることを目的としている。みあこネットでは、これまでの実検・運用を踏え、現在、VPNサーバを分散化させた、みあこネット3方式を展開している。(図1) [2]

本稿では、無線ブロードバンドルータとVPNサーバ機能とを併持った、みあこネット3方式対応ルータであるHome Residential Gateway (HomeRG) の実装に関して述べる。HomeRGはSOHO用の無線ブロードバンドルータとしても活用可能である。

以下、2章でみあこネット3方式の特長をごく簡単に述べ、3章でIXP425アーキテクチャ上でのHomeRGの実装について述べる。

2. みあこネット3方式

サーバを分散配置可能にする、みあこネット3方式は次のような特長を有す。

- 無線区間のSSIDを"MIAKO"に設定
- Comunity Area Network (CAN) の提供
- VPNプロトコルのみを通すフィルタ
- VPNサーバの分散配置

これらの機能を盛込むことを決定するまでの比較・検討の経緯は、[2] を参照されたし。

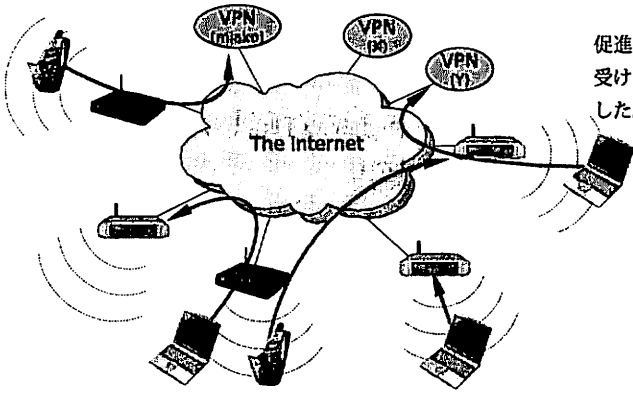

図1 みあこネット3

3. みあこネット3方式対応ブロードバンドルータの設計と実装

基地局を家庭や職場のブロードバンドインターネット環境にさえ設置すれば、みあこネット3の基地局として稼働し、またそれだけでは無くVPNサーバ(PPTPサーバ)としても利用できる無線基地局を実装した。(図2)

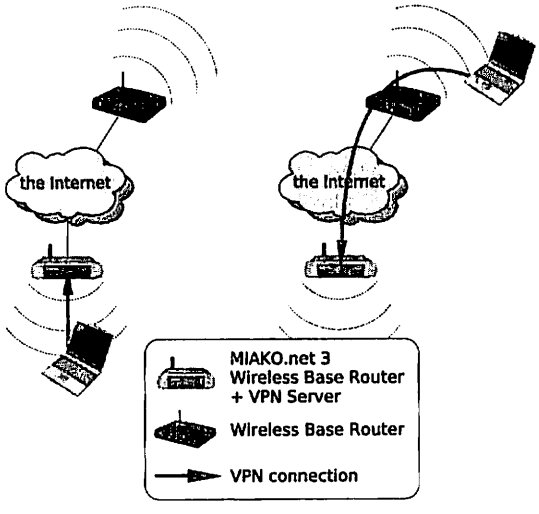

図2 VPNサーバ機能付きルータ

ハードウェアはIXP425 533MHzを基にしており、OSはNetBSD-1.6.2を利用している。インタフェースは、100BaseTX二つと、802.1a/b/g対応の無線インタフェース一つである。

3.1 SSIDの設定

HomeRGのSSIDは"MIAKO"に設定されている。その為、ある基地局がみあこネットに対応しているかどうかを容易に判別できる。なお、無線区間におけるみあこネット2と3とのフィルタなどの設定の差異は無いため、みあこネット2と3のSSIDによる区別は必ずしも必要ない。

3.2 アドレス割当

みあこネットでは、IPv6普及・高度促進委員会[3]より、IPv6促進を前提として、試験的に43.245/16のアドレス空間割当を受けている。今回、その一部をみあこネット3用に使うこととした。

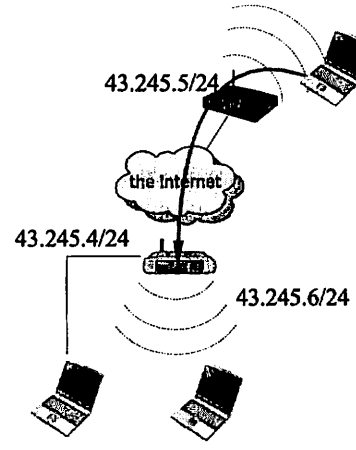

図3 アドレス割当

割当は以下の通りである。(図3)

- 43.245.4/24: LAN側インタフェース
- 43.245.5/24: PPTPサーバがPPTPクライアントに配布するアドレス
- 43.245.6/24: みあこネット用無線LANインタフェース

これらのアドレスは一般的にはグローバルアドレスとして認識されるが、みあこネット3ではプライベートアドレスのように使われ、ブロードバンドルータでNAT(NAPT)変換される。

ただし上ではLAN側インタフェースとPPTPサーバ用アドレス空間を分けているが、SOHOでの利用を考えた場合、この二つが同じサブネットであることが都合が良い場合がある。こうしておけば、外からPPTPでSOHOに接続した場合、SOHO LAN内の器機への接続が同一サブネット内で完結することになる。このため二つのサブネットを/23として纏められやうにした。なおこのように同一サブネットとする場合にはブロードバンドルータはProxy ARPを実行する。

無線LANインタフェースのアドレス空間は、LAN側インタフェースのアドレス空間とは完全に切り離される。これは、通常のSOHO用ブロードバンドルータと違い、無線LANから有線LANへの接続を直接許すことはセキュリティ上問題となるからである。

無線LANをWEPや802.1Xで保護して使いたい場合には、ルータを複数のSSIDに対応させ、SSIDに"MIAKO"以外のものを用いて、アドレスはLAN側のアドレス空間を用いるなどとする必要がある。将来的にはその様な対応も行う予定である。

3.3 フィルタの設定

HomeRG上での無線区間は設定は、各種VPNプロトコルのみを通すフィルタが設定される。(図4)このフィルタにより、提供されている無線接続を使って直接的に他サイトを攻撃することは出来なくなる。何らかのVPNサーバを経由しなければイ

ンターネットを利用できない。(注1)

```
# VPN (PPTP)
pass in quick on ath0 proto tcp from 43.245.6.0/24 to any port = 1723
pass in quick on ath0 proto 47 from 43.245.6.0/24 to any
# VPN (ESP based IPSEC)
pass in quick on ath0 proto tcp from 43.245.6.0/24 to any port = 264
pass in quick on ath0 proto udp from 43.245.6.0/24 to any port = 500
pass in quick on ath0 proto udp from 43.245.6.0/24 to any port = 2746
pass in quick on ath0 proto 50 from 43.245.6.0/24 to any
pass in quick on ath0 proto 51 from 43.245.6.0/24 to any
# VPN (SST)
pass in quick on ath0 proto udp from 43.245.6.0/24 to any port = 2233
# VPN (L2TP)
pass in quick on ath0 proto udp from 43.245.6.0/24 to any port = 1701
# SSH
pass in quick on ath0 proto tcp from 43.245.6.0/24 to any port = 22
```

図4 各種 VPN プロトコルのみを通すためのフィルタ設定

なお、PPTP 接続を NAT(NAPT) 越しに行う必要があるため、HomeRG は PPTP マルチパススルーにも対応している。

3.4 VPN サーバの組込

HomeRG に VPN サーバとして PPTP サーバを組込んだ。PPTP プロトコルは、Windows OS や MacOS などでも標準で実装されており、ユーザが VPN クライアントの設定を容易に行うことが出来る。

4. おわりに

本稿では、無線ブロードバンドルータと VPN サーバ機能とを併持ったみあこネット 3 方式対応ルータの実装に関して述べた。本稿で提案するルータにより、完全に分散化された公衆無線インターネットである、みあこネット 3 を容易に展開することが出来るようになる。

また本稿では述べなかったが、本 HomeRG には IPv6 や Location Independent Network (LIN6) [4], [5] の機能を組込むことも可能であり、今後はこれらを併せて組込んだものを展開していく予定である。

文　献

[1] T. Komura, K. Fujikawa, and Y. Okabe, "The MIAKO.NET Public Wireless Internet Service in kyoto," Proc. of WMASH 2003, September 2003.

[2] 古村 隆明, 藤川 賢治, 岡部 寿男, "VPN サーバを分散させた公衆無線インターネットみあこネット 3 の設計," IEICE IA2006, October 2006.

[3] http://www.v6pc.jp/

[4] M. Ishiyama, M. Kunishi, and F. Teraoka, "An Analysis of Mobility Handling in LIN6," International Symposium on Wireless Personal Multimedia Communication, 2001.

[5] K. Fujikawa, H. Nakano, M. Kunishi, K. Takaaki, "LIN6 Extensions for Simultaneous Utilization of Multiple Wireless Base Stations, Proc. of APSITT 2006, November 2005."

(注1)：VPN サーバのポートへの攻撃、例えば DoS 攻撃などは可能である。ただしこれらの攻撃も帯域制限などにより軽減する方法が考えられる。