

メトロエッジルータ FITElnet®-G20の開発

Development of a Metro Edge Router “FITElnet®-G20”

福永 智之*

Tomoyuki Fukunaga

概要 ブロードバンドインターネットの普及により、アクセスネットワークにおいては今後 FTTHの普及が拡大すると見込まれている。また通信事業者のネットワークでは音声を含め IPをベースとするデータ通信ネットワークへ移行するために、メトロエッジルータには更なる高性能化、高機能化、そして高信頼性が要求されている。今回、我々はこういった高性能、高機能、高信頼といった要求に応えるべく、通信事業者ニーズの高い QoSやマルチキャスト、MPLSをベースとした VPNと いった高機能を、フルワイヤ中継化で性能劣化することなく実現する FITElnet®-G20を開発した。

1. はじめに

ブロードバンドによるアクセス回線の高速化や、通信事業者が提供する VPNサービスを利用したイントラネット構築の普及、地域情報網の整備などにより、IPネットワークのトラフィックは年々増大を続けている。一方、通信事業者やプロバイダでは、VoIP (Voice over IP) やコンテンツリアルタイム配信、そして MPLS機能を用いた IP-VPNや L2-VPNと いった多機能なサービスも展開されている。

こうした中でユーザアクセス網とコア網とを接続するメトロエッジルータには、ストレスなくデータを中継する高性能、及び様々なサービスに対応できる高機能に加え、それらサービスにおいて高信頼性が要求されている。

今回、LANの領域を超えてバックボーン、メトロポリタンエリアネットワーク (MAN)、ワイドエリアネットワーク (WAN) など多くの市場で普及しつつあるイーサネットをターゲットに、2001年末に発売を開始した FITElnet-G12の技術を

継承しつつ、スケーラビリティ、機能、性能を大幅に向上させることにより、バックボーンコアルータでしか実現できなかった性能並びに高度な機能を実現した FITElnet-G20 (写真1)を開発したので報告する。

2. 機能

FITElnet-G20は、通信事業者が経済的かつ効率的にネットワークサービスを運用するため、また高度なアプリケーションを使用したエンタープライズ環境においても、高品質な IP通信を実現するために、次のような機能をもつ。

2.1 大容量経路情報

FITElnet-G20は、インターネットのフルルート及び通信事業者の IP-VPN網に対応するにあたって十分な経路情報 (VRF) やラベル情報のハンドリングが可能である。表1に、FITElnet-G20のもつ経路情報等のスペックを示す。FITElnet-G20は、これら大量のデータベース検索を行いながらフルワイヤ中継を可能としている。



写真1 FITElnet-G20
Appearance of FITElnet-G20

表1 装置スペック
Specifications of FITElnet-G20

VLAN数	100/FE, 1,000/GE (合計2,026)
IPv4論理IF	2,000
L2 MAC学習テーブル	300,000
IPv4 経路情報	300,000
IPv6 経路情報	200,000
ARPエントリ	50,000
IP-VPN最大VRF	2,000
MPLSラベルパス	20,000
MPLSピア	128
アクセスリストエントリ	1,000/FE, 10,000/GE(合計20,000)

* 研究開発本部 ファイテルネットワーク研究所

2.2 VLAN多重

FITELnet-G20は、Gigaイーサネット、Fastイーサネット上で2000の802.1qタグVLAN及び26のポートVLANをサポートする。VLAN毎にIPv4、IPv6それぞれ動作する/しないを設定可能とする。またIPv4においてはVLAN Aggregation機能、IPv6においては個別サブネットを設定することにより、アドレスマップをVLAN単位で分離することを可能とする¹⁾。アドレス分離環境においては、ARPフィルタ機能を併用することにより、各分離されたセグメントのセキュリティを確保する。これによってIPネットワークシステムにおける、セキュアかつスケーラブルなユーザ収容方式を実現可能とする(図1)。

またFITELnet-G20では、自由なブロードキャストドメインの設定を可能としている。例えば異なる802.1q VLANタグ終端インタフェースを同一ブロードキャストドメインに収容することができる。転送においても同様で、例えばtag100のインタフェースとtag200のインタフェースを同一ブロードキャストドメインに設定した場合、双方のインタフェースの先にある端末同士のL2中継が可能である。この場合はインタフェースに合わせてタグを付け替えて転送する。

加えてFITELnet-G20では、プロトコル別にブロードキャストドメインを指定することも可能としている。これにより、ARPやIPv4、IPv6といったL3フレームはL3中継を行い、その他はブロードキャストドメイン内でL2中継を行うことが可能(図2)。

2.3 QoS / CoS機能

複数ユーザを1本のイーサネットでVLAN多重により集約する場合、ある1ユーザの大量トラフィックがイーサネットの帯域を殆ど使ってしまい、他のユーザの通信を妨害することがある。このような事態を防ぐためにもユーザ毎の帯域保証などのQoSは必須である。

FITELnet-G20は以下のような充実したQoS/Cos機能を実装する。

- 1) RICで開発したPPQ及びDiffServをサポートする。
- 2) VLAN毎の公平性機能を実装する。VLAN公平性動作時はVLANあたりの最大レート制御、VLANグループに対する

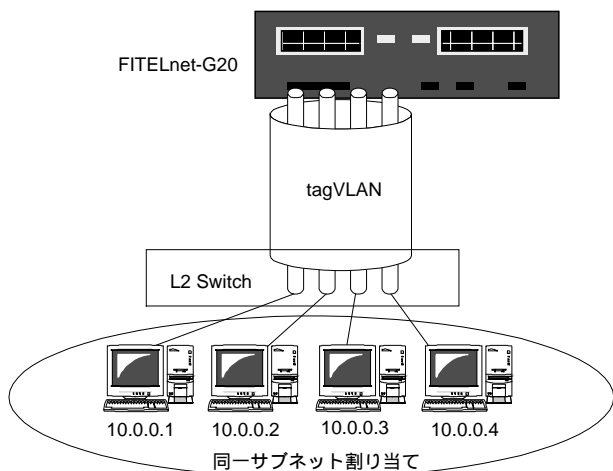


図1 VLAN Aggregationによる同一サブネットでのセグメント分割
Network segmentation on the same subnet by using VLAN Aggregation

る帯域制御を可能とする。加えてVLAN内優先度を設定することによるVoIPなどの優先トラフィックに対応する。

- 3) アクセスリストによる細かいポリシングを可能とする
- 4) VLAN毎に、入力/出力両方のインタフェースでのポリシングをサポートする。また出力インタフェースでのシェーピングをサポートする。これによりユーザ側への細かい帯域制御を可能としている。

FITELnet-G20は、上記QoS機能をワイヤレス通信環境において実現している。複雑なQoS機能を高速に実現するアーキテクチャを図3に示す。

2.4 マルチキャスト

マルチキャストを利用することにより、ユニキャストを主とした従来のCDN (Content Delivery Network) では困難であった大規模な同時配信の実現を可能としている。加えてFITELnet-G20は、サービスプロバイダのエッジ部分でRADIUSサーバと連携し、認証済ユーザ宛のデータのみ中継す

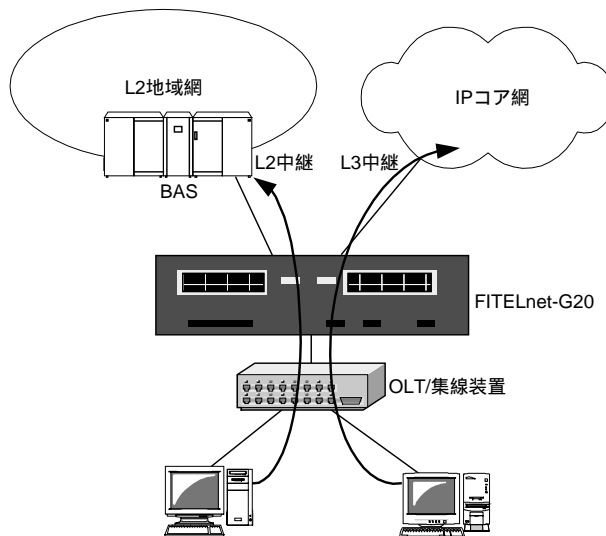


図2 プロトコル別ブリッジ機能
Protocol bridging function

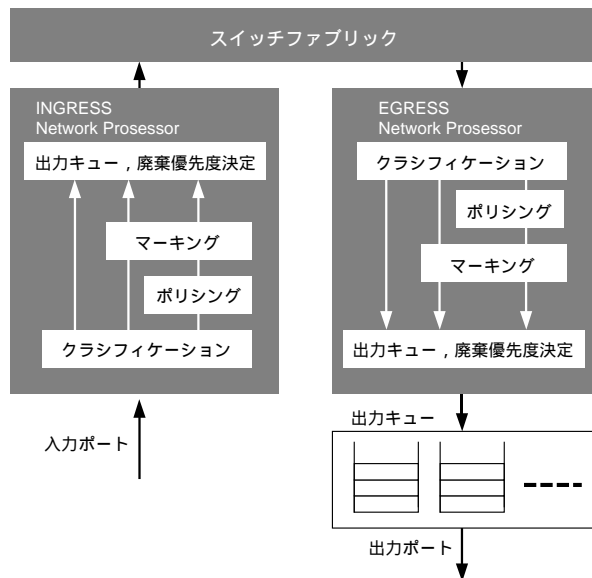


図3 フォワーディングフロー
Forwarding flow

る機能を有する。この機能により、配信サーバとユーザ環境に依存しない汎用的なユーザ認証と課金管理を実現した CDN の構築を可能にしている（図4）。また、マルチキャストに対応した QoS 機能により、様々なトラフィックが混在する状況においてもマルチキャストによる動画配信のトラフィックが保証されるため、サービスの差別化も可能となる。

2.5 MPLS

我々は FITElnet-G20 の前身である FITElnet-G12 の頃から、MPLS のさまざまなフォーラムや相互接続試験に参加しており、相互接続性に関して実績を上げてきている。FITElnet-G20 もその流れを後継し、多彩な MPLS 機能を実装している。

FITElnet-G20 のもつ MPLS 機能に関して、表2に示す。

2.5.1 VPN

通信業者が提供する VPN サービスのバックボーンプロトコルとして、MPLS が注目されている。

FITElnet-G20 は、最大 50,000 ピアとの LSP（ラベルパス）を確立した上で、RFC2547bis 方式による IP-VPN 網や、イーサネットフレームの宛先 MAC アドレスを見てラベルスイッチを行う L2-VPN 網の構築を可能としている。さらに、広域イーサネットサービスであるメトロポリタンエリアネットワーク（MAN）と L2-VPN との接続をもサポートしている。

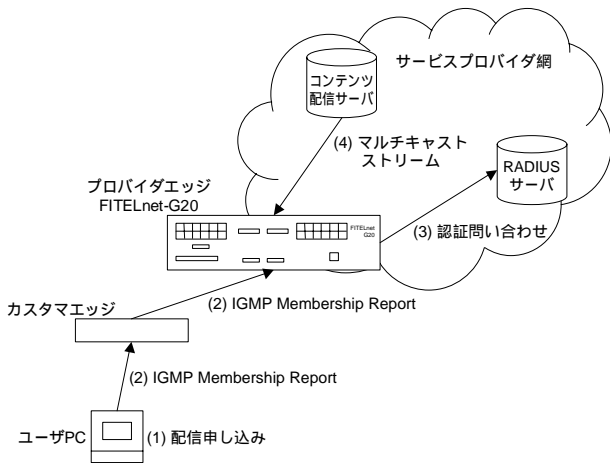


図4 コンテンツ配信システム構成例 Configuration example of content delivery system

表2 FITElnet-G20 の MPLS 機能 MPLS functions

IP-VPN	RFC2457bis	
	VRF数	2000
	Tag-VLAN連携	
シグナリング	LDP	
	LDP拡張(ポート711対応)	
	RSVP-TE	
Traffic Engineering	スタティック	
	OSPF-TE	
	IS-IS-TE	
QoS/CoS		
L2-VPN (TLS)		

2.5.2 MPLS-IX

ISP間の相互接続技術であるIXにMPLSを利用するMPLS-IXが注目されている。データリングメディアを選ばないことからPOS等の広域リンクメディアも使用でき、IXを広域に分散するといったことが可能であることが注目される理由であり、distic（次世代IX研究会）を中心に研究開発や技術検証が行われている²⁾。

FITElnet-G20はMPLS-IXを構築するにあたって必要なC'sCやLDP on RSVP, LDP on LDPといった各種機能を実装しており、様々なタイプのMPLS-IXに対応可能である（図5）。

2.5.3 MPLS QoS

通常MPLSのラベルパスは、宛先IPアドレスによって決定付けられる。従って同じIPネットワーク宛のデータは同じラベルパスを通過することになる。そのため、あるIPネットワーク宛のデータが通過するパスが別トラフィックにより輻輳状態であっても、そのパスを通らざるを得ない。FITElnet-G20はこの問題を解決するために、MPLS QoS機能を実装する。MPLS QoSを用いた場合、ラベルパスは宛先IPアドレスだけではなく、送信元アドレス等、アクセスリストで指定できるフロー別に制御される。これにより柔軟なパス決定を行うことができ、結果的に網全体のトラフィック制御を行うことが可能である（図6）。

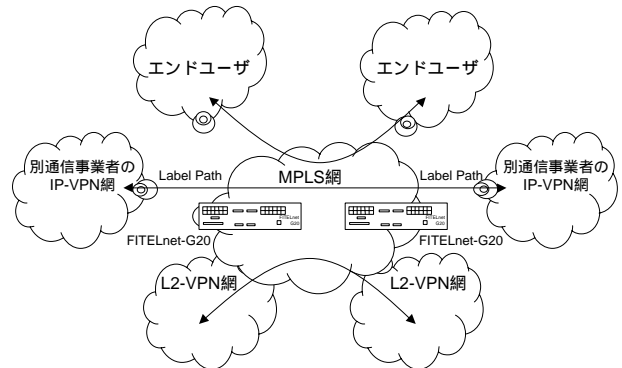


図5 VPN サービス網構成例 Configuration example of MPLS-VPN service

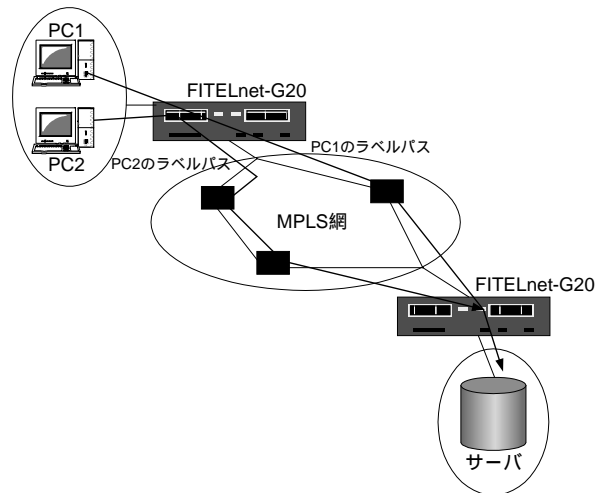


図6 MPLS QoS例 Configuration example of MPLS-QoS

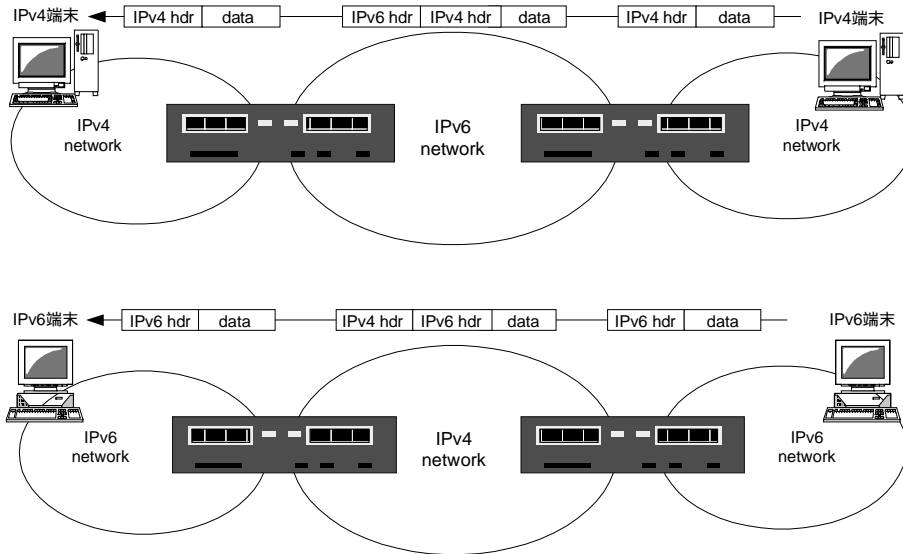


図7 v4 over v6とv6 over v4
v4 over v6 and v6 over v4

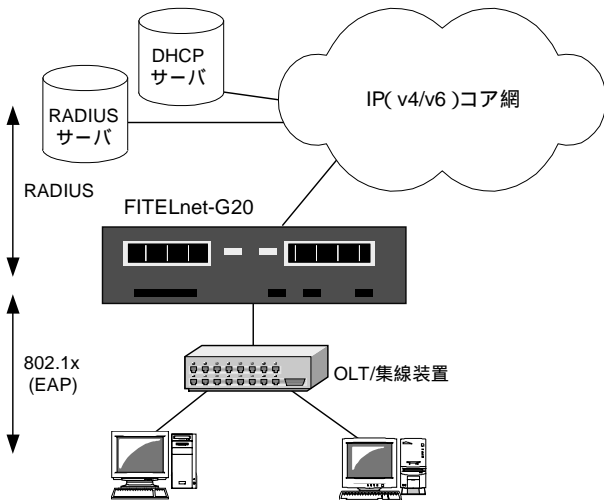


図8 アクセス認証構成例
Configuration example of authentication on network access

2.6 IPv6

IPv4/v6のデュアルスタックを実装している。したがってv4からv6への移行時のソリューションとして、v4トンネル及びv6トンネルをサポートする。v6ユーザ同士をv4網で接続する(v6 over v4)ことも、逆にv4ユーザ同士をv6網で接続する(v4 over v6)ことも可能(図7)。

2.7 アクセス認証

FITELnet-G20は、IEEE802.1xとRADIUSを使用してユーザ認証を行い、認証済ユーザにのみアドレス配布することにより、セキュアなplug & playをエッジルータにおいて実現する³⁾。

具体的にはエッジルータにおいて802.1xのポート認証の概念を拡張し、各認証をport, vlan, MAC addressに対して行う。認証可となったホスト以外は、ソースMACアドレスでのフィルタリングを行う。認証されたホストに関しては、IPv4の場合はDHCP, IPv6の場合にはRouter Advertisementによるアドレス自動設定を行う。この機構により、セキュリティの確保されたplug & play機能を提供する(図8)。

3. 性能

中継装置において、機能と性能とは相反する性質を持っている。機能が高度になれば処理が増え、その分性能が下がる。例えば経路情報保持数を増加させると、ある宛先に対する経路の検索対象も増加するために検索時間がかかり、結果的に転送能力が低下することになる。また詳細なポリシングを設定すれば、その分転送データに対する判定項目が増え、やはり性能低下に繋がる。さらにハードウェアリソースを潤沢にすることによる高速化を行うと、当然ながらコストが上がる。

FITELnet-G20は、プログラマブルな高性能ネットワークプロセッサを使用し、さらに高性能化のための技術を導入することにより、高機能・高性能・低コストを実現している。

3.1 CAM + TSEハイブリッド方式による高速検索

FITELnet-G20は30万件の経路情報を扱うため、いかにこの大量データから必要な情報を高速検索するかが高性能化の大きなポイントとなっていた。ハードウェアによる検索方式は大きく次の2方式に分れる。

- 1) CAM (検索専用メモリ) を使用
- 2) TSE (Tree Search Engine) を使用

CAM方式は非常に高速検索が可能であるが、対象データ数に比例してコストがかかる。一方TSE方式は安価なメモリを使用するために低コストで実現できるが、検索量とともに検索時間も急速に増加する傾向をもつ。FITELnet-G20では、両方の方式の長所を併せ持ったハイブリッド方式を採用した(図9)。

FITELnet-G20では、高コストのCAMを複数ネットワークプロセッサで共有させることにより、更なる高効率化を行った。共有化のためのロジックを持ち、かつ共有することにより発生するCAMの帯域ボトルネックの解消、さらに高速ネットワークプロセッサの複数スレッドからの非同期CAMアクセスの実現を目的としたカスタムロジックを開発することにより、CAMの共有化を実現した。

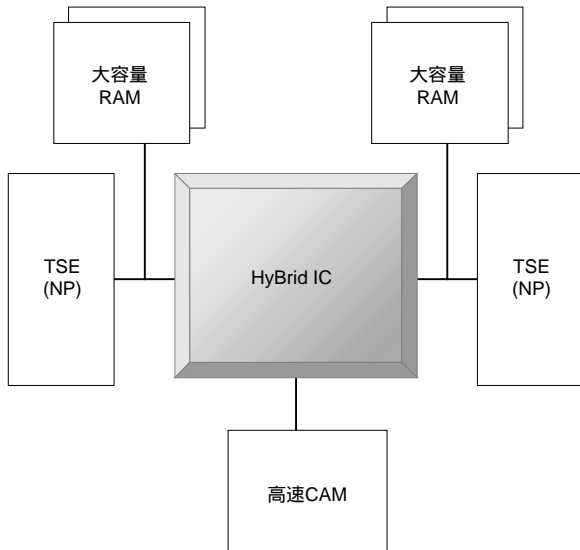


図9 CAM + TSEハイブリッド方式
Hybrid method with CAM and Tree Search Engine

3.2 QoS機能との連携

ネットワークプロセッサの検索機能のもう一つの重要な仕事にQoS機能の支援がある。経路検索と同様、QoS機能に関しても様々な検索（アクセスリスト検索）が発生する。ネットワークプロセッサはフレームを中継する毎に、そのフレームに対応するアクセスリストを検索し、ヒットすればアクセスリスト中に設定されたポリシングに従ってQoS処理を施す。

FITELnet-G20では、前記ハイブリッド検索のCAM検索の一部をアクセスリスト検索に使用し、アクセスリストの複雑な検索を高速に行うことを可能としている。この高速検索により、前述したMPLS QoSといった複雑なQoS機能を、性能劣化することなく実現している。

4. おわりに

FITELnet-G20の持つ機能と、それを実現する技術に関して報告した。プログラマブルなネットワークプロセッサと蓄積してきたネットワークソリューション技術を駆使して、顧客ニーズに応えることのできるメトロエッジルータを開発できたと考える。今後のメトロエッジルータには更なる機能と性能、及びスケーラビリティが要求されると考えられるが、柔軟に対応していきたいと考える。

参考文献

- 1) D.McPherson and B.Dykes, "VLAN Aggregation for Efficient IP Address Allocation," Feb.2001, RFC3069
- 2) 永見, 中川他: "MPLSを用いた分散IXアーキテクチャの設計"
- 3) IEEE Std 802.1x-2001 Port-Based Network Access Control