応募区分：提言型論文

エンタープライズ WAN の高度化を実現する

ネットワーク技術の検討

平河内　竜樹（ひらこうち　りゅうき）
ネットワンシステムズ株式会社
ビジネス推進本部 第１応用技術部

■ 要約

企業 IT のクラウド利活用に伴い，エンタープライズネットワークにおける WAN は，サービス基盤として一層重要なものとなっている．WAN の帯域はランニングコストに直結する貴重なリソースであり，有効利用のためにキャッシュや圧縮・QoS などの技術が活用されている．併せて，サービスレベルを維持する上で WAN の可用性はより留意すべき事項となる．

本稿では，可用性の向上と複雑さの軽減を両立させるため，IP ベースとなるプロテクション技術の活用を提言する．併せて本技術の有用性について評価検証を実施し，MPLS を全く利用しない VPN 環境においても障害からの復旧時間が予測可能であり且つ非常に短いサービス停止時間で行われることを確認した．これによりエンタープライズ WAN の拠点間接続においても，拡張された技術の利活用によって，高度化の実現が期待される．

目次

1. 背景

1.1. エンタープライズ WAN における要求

クラウドの利活用に伴って企業 IT におけるデータや処理系の外部移行が進み，エンタープライズ WAN では利用帯域が増加すると共にサービス基盤としての重要性が拡大している．

WAN の帯域はランニングコストに直結する貴重なリソースであり，有効に活用するため様々な技術が利用されている．例として，利用帯域を削減可能なデータ圧縮やコンテンツキャッシュといった WAN 最適化に分類される手法や，主に通信のバースト性からユーザやアプリケーションを保護するために継続的に利用されている伝統的な QoS 等がある．また，WAN への依存度が増加している現在では企業 IT のサービスレベルを高い水準に維持する上で，WAN の可用性はより注視すべき要素となる．

日本のエンタープライズ WAN では，管理上の理由などからインターネットアクセスにおいても代表拠点やデータセンターなどのセンターサイト（以下，センターと呼ぶ）を経由して行われることが多く，拠点間接続を経由して行われる通信の比重が高い．そのような運用を行っている企業においても利用帯域の増加が続けば，この通信パスを堅持することはコストの面から困難になるケースが生じる．そのため，承認されたクラウドサービスに限定するなどして，センターを経由して通信を行っていた拠点（以下，ブランチと呼ぶ）から直接インターネットアクセスを行う検討も行われると考えられる．しかしながらその際も適用は段階的に行われることが予想され，またそのような形態が必要とされていないケースや許容が難しいケースも多く存在することを考慮すると，拠点間接続の安定稼働は依然として重要な要素となる．

なお拠点間通信においては，WAN 環境に起因して低下した，アプリケーションレスポンスの改善なども留意すべき事項であり，この点はアプリケーションレイヤの視点から最適化を図るアプローチが中心となる．本稿ではネットワークレイヤの視点から，エンタープライズ WAN における可用性に関して，掘り下げて述べるものとする．

1.2. 可用性の要求と関連技術

1.2.1. 規模と可用性の両立

エンタープライズ WAN においては，拠点間通信の可用性を確保するため WAN サービスおよび WAN のアクセス回線に接続される機器（以下，エッジ機器と呼ぶ．多くの環境でルータ製品が利用される）を複数用意して冗長トポロジを形成し，ルーティングプロトコルを適用する方法がよく用いられる．また IPsec VPN では多くの冗長化手法が存在するが，適用可能なトポロジの柔軟性やマルチパスによる負荷分散の実現・LAN 環境の延伸といった観点から，VPN 環境においてもルーティングプロトコルはよく利用される．図１はその適用例であり，冗長トポロジから実際に利用されるパスの選出および障害発生時におけるパスの再選出をルーティングプロトコルが担い，可用性の確保を実現する．

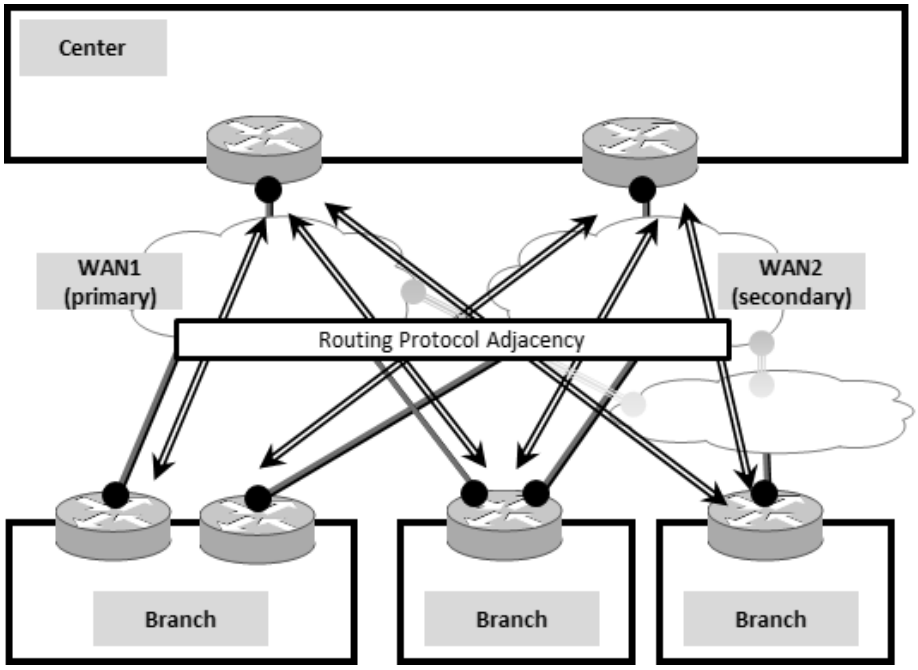


図１. ルーティングプロトコルを利用する拠点間接続の例

また，エンタープライズ WAN の構成は多重障害を想定して WAN サービスを３つ以上契約しているケース・複数の WAN サービスを経由して階層化され多くの経路が存在しているケース・一組のエッジ機器で多数のブランチを収容しているケースなど環境によって様々であり，BGP を利用しサービスプロバイダの様な構成を取る大規模ネットワークも存在する．

なお経路制御によって可用性を確保している場合，ネットワークの障害から通信の復旧に至るまでに発生するサービス停止時間（以下，断時間と呼ぶ）は，ネイバー数や経路数といった規模の要素にも依存する．エンタープライズ WAN で発生する経路数に対し，データ転送時に参照されるエッジ機器の転送テーブル（以下，FIB :Forwarding Information Base と呼ぶ）が容量不足となることはほとんど無いが，ネットワーク構成は環境によって異なるため，予測は必ずしも容易ではない．

一例として，多数のブランチを収容する構成では，センター側は接続される各ブランチの経路を保持する必要があり，ブランチの数が多くなるほどセンターのエッジ機器で発生するルーティングの負荷は増大していく．またブランチ側も，常に集約された経路で通信できるとは限らない．例えば，経路集約が行われないケースや，ホストルートなどサブネットより細かい単位で制御を行うケースなどが挙げられる．

実際の WAN 設計においては早い段階から相応の精度で断時間を推定する必要があることも多く，視点によっては「環境に依存する」こと自体が悩ましい課題と言える．

1.2.2. プロテクション技術

他方，サービスプロバイダのネットワークで使われる技術に目を向けると，大規模環境にも関わらず高い可用性が実現されている．この分野で MPLS FRR (Fast Reroute) はコアネットワークを保護する技術としてよく知られており，十分な実績を持つ技術である．昨今ではデータセンター間の接続

などでも利用されている．本稿ではMPLS FRRの様に，事前に用意されたバックアップパスを利用することによって高速な障害復旧を行う技術全般を指し，プロテクションと呼ぶこととする．

また，IPおよびMPLS VPNのエッジを保護可能な技術としてBGP PIC (Prefix-Independent Convergence) Edgeが存在する．この技術の中核を成す要素は階層化FIB (Forwarding Information Base) であり，共通のバックアップパスがリストされている各経路はその情報をポインタで参照することによって，更新処理に対するテーブルサイズの依存性を排除するというものである．ネットワーク機器においてFIBの更新処理は高い負荷が発生する箇所であり，この技術は断時間の短縮において非常に大きな効果がある．図２の資料では，階層化FIBを利用している技術がリストされている．

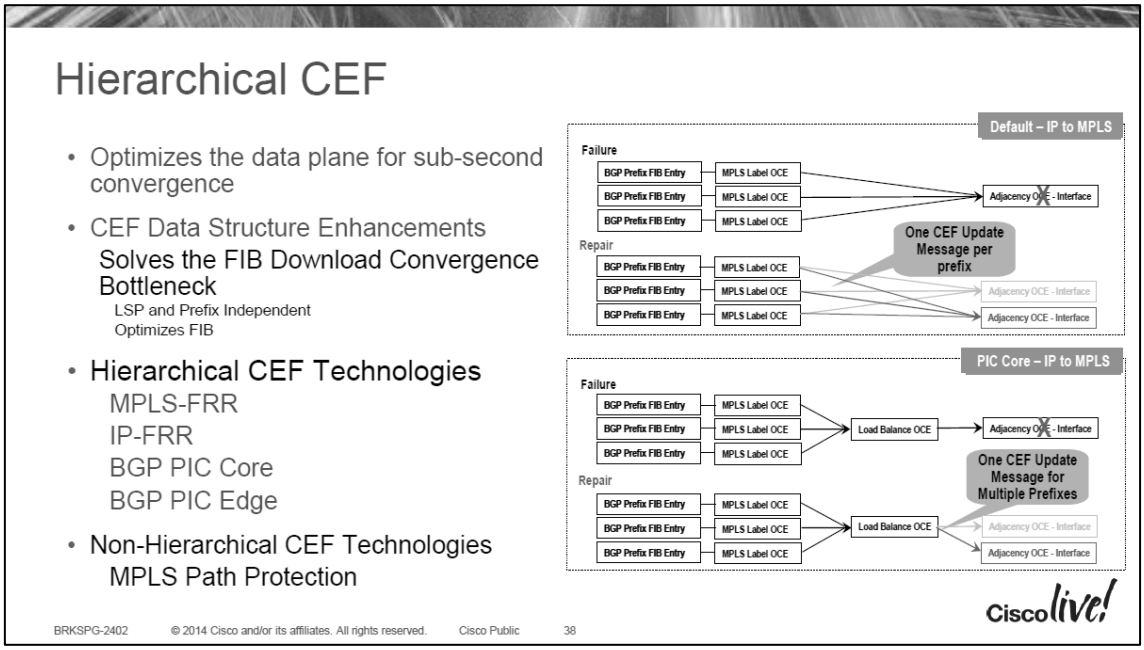


図２.　階層化FIBを利用する技術（引用元は参考文献を参照のこと）

また，MPLSを用いずにMPLS FRRと同様の高可用性獲得を目的とした技術として，IP FRRが存在する．IP FRRを実現する手法の一つとしてOSPF LFA (Loop Free Alternate) が存在し，主にIPベースのコアネットワークを保護する用途が想定されている．OSPF LFAは経路計算上ループフリーが担保されたセカンドベストのパスを階層化FIB として格納する形態となっている．プロトコルに拡張を加えない点はシンプルであるが，バックアップパスの保持率はトポロジに依存する[1]ため，適用を検討する上ではこの点が一つの課題になると考えられる．EIGRPでフィージブルサクセサの利用を検討した場合にトポロジの影響を受ける点と，関係性は同様である．

なおCiscoルータには『EIGRP Loop-Free Alternate Fast Reroute』(以下，EIGRP LFAと呼ぶ) という機能が存在し，従来からのフィージブルサクセサがバックアップパスとして利用される．当該機能はFIBとの関係性が拡張されたものと位置づけられる．

[1] 関連技術であるRemote LFAなどはEncapsulationを伴い適用トポロジの拡大が実現されている

2. 提言

これまでの背景を踏まえ，本章では可用性の観点からエンタープライズ WAN の高度化に寄与するための提言と検討を行う．

2.1. 拠点間接続におけるプロテクション技術の活用

本節の概要はエンタープライズ WAN の拠点間接続対し, BGP PIC Edge や OSPF/EIGRP LFA の活用を検討するものである．

ネットワークに起因した断時間の影響を検討する際はエンドツーエンドで考慮する必要はあるものの, WAN に起因した断時間に対し,「将来にわたって規模の影響を受けづらく予測が容易になること」および「短縮できる可能性であること」には一定の価値を見出すことができると考えられる．

着目する技術への期待効果は上記の通りであり，本稿では，エンタープライズ WAN の環境に対し適用可能であるか・導入負荷を軽減する手段はないか等を主な焦点とする．

2.1.1. BGP PIC Edge の適用

Cisco ルータにおける BGP PIC Edge は，VPNv4 および IPv4 VRF に限らず IPv4 のアドレスファミリをサポートしており，マルチプロトコル BGP や VRF の利用を前提としていない．このため，センター・ブランチの片方もしくは双方のエッジ機器で利用することによって，エンタープライズ WAN の拠点間接続に適用することが可能となる．また，閉域網上でトンネルを介さない構成・インターネットや地域 IP 網を経由した VPN 構成のどちらに対しても利用することができる．

また，次項で取り上げる LFA の様なリンクコストに基づいたセカンドベストの採用判断を行わないため，トポロジの自由度および設計のシンプルさという観点でも適用が容易な技術と言える．

懸念の一つは対応機器の価格帯であるが, Cisco ルータではエントリモデルとなる Cisco800 シリーズ（OS は IOS 15M/T）や ISR4000 シリーズ（OS は IOS-XE 3S）にてサポートされており，同社のルータ製品ではエントリクラスのモデルから利用可能となる．

2.1.2. IP FRR の適用

BGP の利用が困難である場合を想定し, OSPF/EIGRP LFA の利用を検討する. 前章で上げた通り，OSPF/EIGRP LFA はトポロジの依存性があり，冗長化によってたびたび形成されるスクエアなどのトポロジには適さない．併せて，WAN 環境で物理配線を自由に制御することは困難である．そこで GRE 等の IP トンネルを LFA の保持が可能となる様に確立し，その上で IGP ネイバーを確立するという方法が問題への対処として考えられる．

例えば，バックアップとなるトンネルを作成し，Loopback インタフェースなどを活用して各エッジ機器にトンネルエンドポイント用のアドレスを用意する．次いで，期待する伝送路を経由する様に各中継機上でトンネルエンドポイントに対する経路を Static Route 等で指定する．例としては，図 3 に示す様に，MPLS/RSVP を用いた時の様な Edge-to-Edge の Explicit Path も実現可能となる．

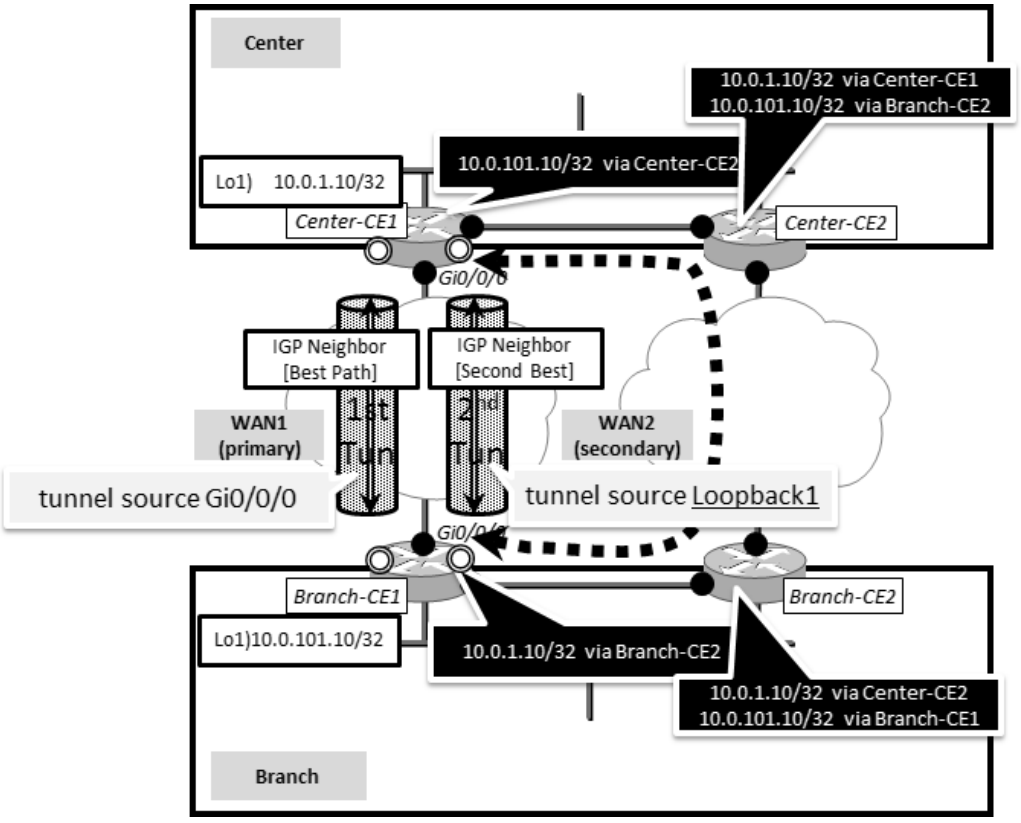


図３. トンネルエンドポイント固有のアドレスと固定経路による明示的な伝送路の選出

しかしながら，IP トンネルを併用した場合も，課題は残される．まず，Edge-to-Edge でトンネルを確立した場合，LFA の選出は容易になるが，「トンネル数の増加」「伝送路を指定する経路のメンテナンス性」などが問題となる．

一つのアプローチとして，直接接続されていないエッジ機器間に限定してトンネルを確立し，LFA に適したメッシュトポロジを形成する方法が挙げられる．

例えば図４にある様なトポロジに対しては「センターでは渡りのリンクを作成するなどして，エッジ機器が一台のブランチに対してトライアングルトポロジを提供する」「エッジ機器が二台で冗長化された，限られた数のブランチとの接続に対しては，メッシュトポロジに足りない分だけのトンネルを追加し，その伝送路は共通してセカンダリ側のエッジ機器を経由するという指針に基づいて指定する」といった方針によって，WAN 関連の障害に対して LFA による保護が可能となる．必要最低限のトンネル追加と共通のポリシーに基づいた伝送路指定を行う形となる．

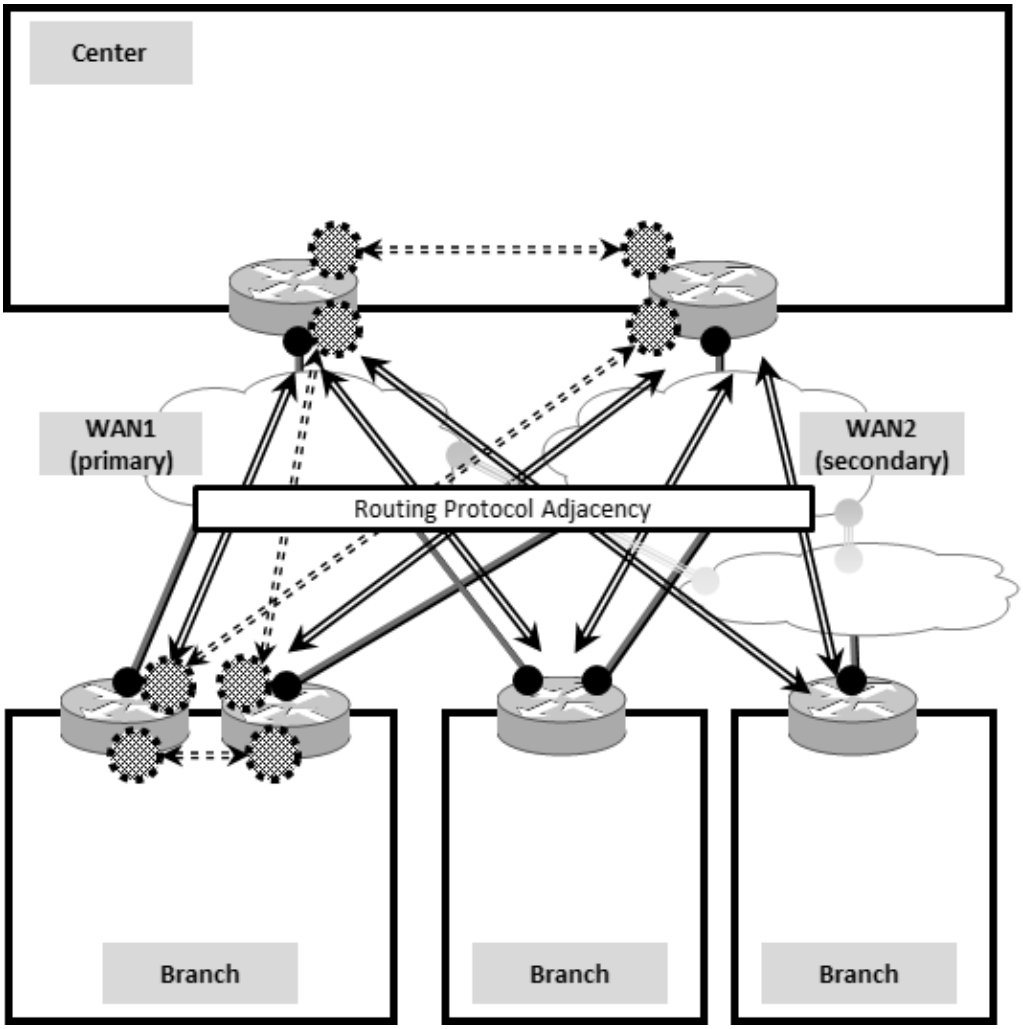


図４. 想定構成と LFA 利用のために追加で作成するリンクもしくはトンネル（点線部）

留意点および課題として，柔軟なパス選出は実現困難ということが挙げられる．メッシュ型のトポロジを形成することによって LFA の適用は容易になるが，バックアップパスの検討を行った際に，意図した組み合わせが提供可能であるとは限らない．EIGRP であれば任意のメトリック操作も活用できるが，用途によっては複雑さを増大させる原因になることが考えられる．LFA の利用が検討されるケースとしては，例えば WAN 上の障害に対しては特に可用性を高めたいので，非対称を気にせず少しでも高速に迂回できる手法を利用する・コスト上は既にバックアップパスが保持可能であるため見直しを機に利用するといったことが考えられる．

また，利用上の留意点として，OSPF/EIGRP LFA は IOS 15M/T では現状サポートされていないこと，IOS-XE 3S では OSPF/EIGRP 共に LFA を利用可能であるが OSFP LFA は Tunnel インタフェースでの利用をサポートしていないことが挙げられる．

補足として，IOS-XE 3S で稼働する CSR1000V を利用した仮想化環境にて，図４を再現するトポロジで OSPF LFA を適用した．各サイトで LAN 相当の経路を含めて広報したところ，全ルータにおいてカバー率 100%の出力が得られた（表 1）．

表１． 図４の論理トポロジに合わせてOSPF LFAを適用した場合の出力

```
Center-01a#show ip ospf fast-reroute prefix-summary | i Protected|All|Process
           OSPF Router with ID (10.0.1.1) (Process ID 1)
Interface        Protected    Primary paths     Protected paths Percent protected
                            All  High   Low   All  High   Low    All High  Low
Process total:               19     5    14    19     5    14   100% 100% 100%
Center-01a#
```

```
Center-01b#show ip ospf fast-reroute prefix-summary | i Process
           OSPF Router with ID (10.0.1.2) (Process ID 1)
Process total:               19     5    14    19     5    14   100% 100% 100%
Center-01b#
```

```
Branch-01a#show ip ospf fast-reroute prefix-summary | i Process
           OSPF Router with ID (10.0.101.1) (Process ID 1)
Process total:               23     7    16    23     7    16   100% 100% 100%
Branch-01a#
```

```
Branch-01b#show ip ospf fast-reroute prefix-summary | i Process
           OSPF Router with ID (10.0.101.2) (Process ID 1)
Process total:               23     7    16    23     7    16   100% 100% 100%
Branch-01b#
```

```
Branch-02#show ip ospf fast-reroute prefix-summary | i Process
           OSPF Router with ID (10.0.102.1) (Process ID 1)
Process total:               24     8    16    24     8    16   100% 100% 100%
Branch-02#
```

```
Branch-03#show ip ospf fast-reroute prefix-summary | i Process
           OSPF Router with ID (10.0.103.1) (Process ID 1)
Process total:               24     8    16    24     8    16   100% 100% 100%
Branch-03#
```

3. 検証

3.1. 試験環境

前章で述べた「BGP PIC」および「EIGRP LFA」をIP トンネルであるGREに適用する環境を用意し，期待する動作に対する実現可能性および断時間の検証を行う．

物理構成を図 5 に示す．利用したネットワーク機器はいずれも Cisco ルータであり OS は共通して IOS-XE 3.16.0S を利用した．試験対象となるエッジ機器は全て ISR4000 シリーズであり，各々中継ルータである ASR1006 に接続される構成となる．中継ルータでは WAN の加入者収容ルータおよび地域 IP 網 / インターネットを模す形で VRF が作成されており，障害の発生は VRF 間を接続する仮想インタフェース[2]に対し shutdown を実行することによって再現する．

経路については，テスターとセンターのエッジ機器との間で EBGP ピアを確立し，/32 のルートを配布する．センターのエッジ機器は BGP PIC の構成ではそのまま BGP で・EIGRP LFA の構成では EIGRP への再配布を行い，ブランチのエッジ機器へ広報する．

経路数は[A]10 経路・[B]10,000 経路・[C]40,000 経路の 3 通りを用い，ブランチ側に接続されたテスターから各経路の宛先に対して 2pps ずつとなる[A]20pps・[B]20,000pps・[C]80,000pps のレートで通信を片方向で印加する．この状態で前述の障害を発生させ，全ての通信が復旧するまでに破棄されたパケット数を採取する．フロー単位の平均サービス停止時間を示すため，損失パケット数を PPS にて除算し，数字を整理した．

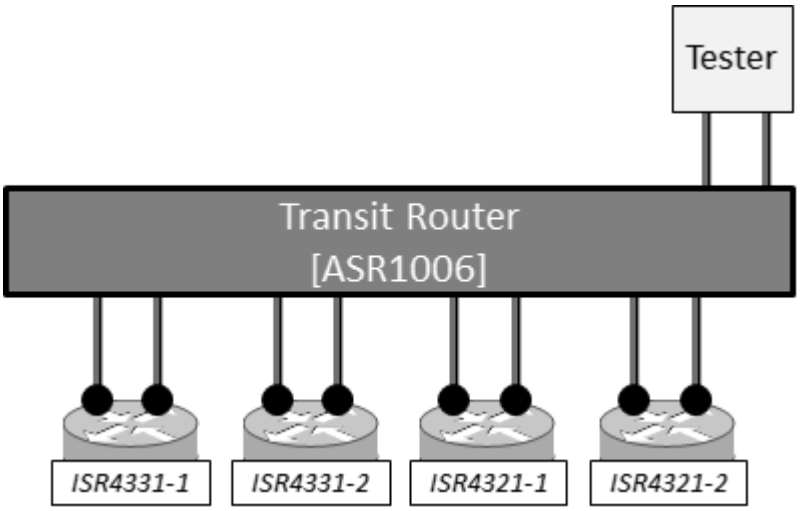


図 5.　本節で実施する検証の物理構成図

なお本節の試験環境では，中継網上で発生させる間接リンク障害の検出を可能な限り高速に行うため，いずれも送出間隔が 50msec・カウント数が 3 回となる様に，エッジ機器の GRE 上で BFD を有効にしている．BFD の適用は断時間の短縮においては有効な反面，収容可能なネイバー数への影響がある上に，損失に対して過敏になると回線品質によっては意図しない回線の選択や安定性の低下を招く可能性もある．

BFD を GRE 環境含めて利用可能であることは Cisco ルータの利点であり，エンタープライズ WAN に適用する際は断時間の要求に応じて適切な障害検出手法およびパラメータの検討を行うべきである．

[2] 本構成では IOS-XE の機能である VASI(VRF-Aware Service Infrastructure)を利用している

3.2. BGP PIC over IP Tunnel

本項における試験の論理構成と機器構成を図６に示す.

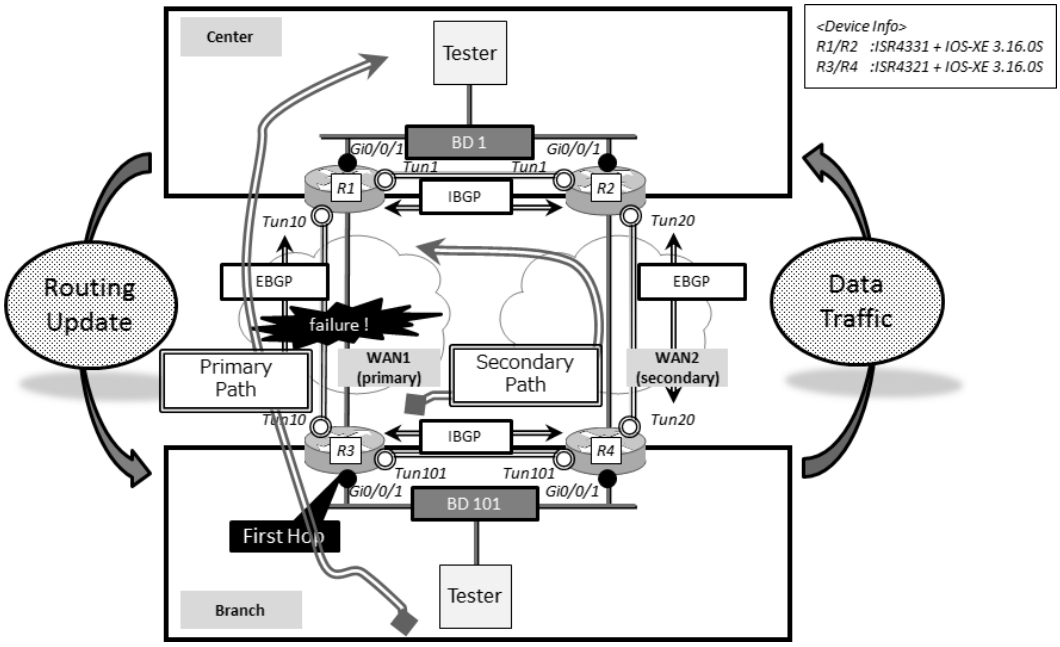
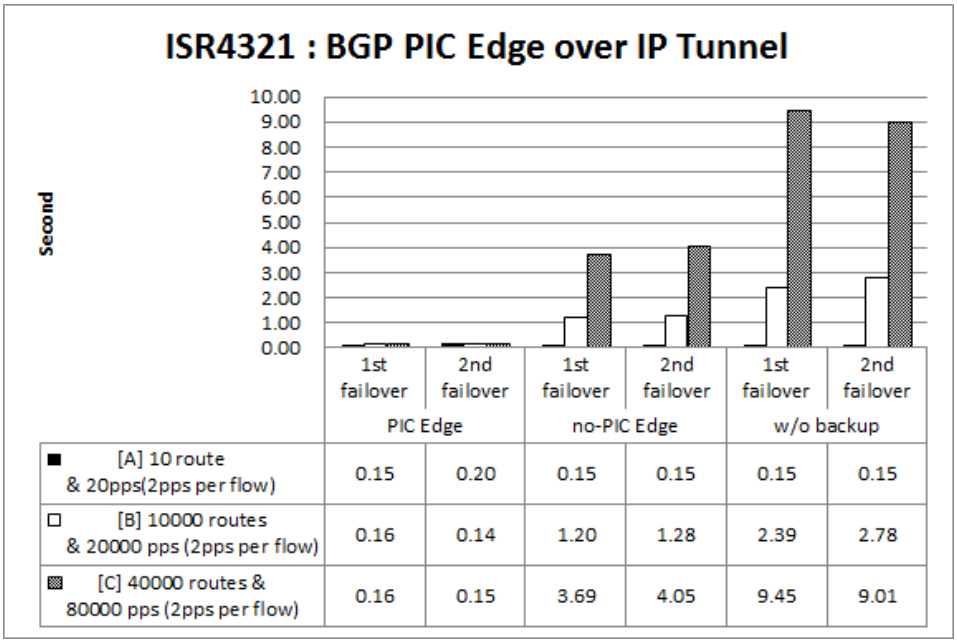


図６. BGP PIC Edge を用いた試験構成

BGP PIC Edge を有効にしたパターン[1]の他，比較対象として BGP RIB としてバックアップパスを持つが BGP PIC Edge を有効にしていないパターン[2]およびバックアップパスを持たないパターン[3]を同様の物理・論理構成上で設定変更によって用意した．測定結果を表２に示す.



	PIC Edge		no-PIC Edge		w/o backup	
	1st failover	2nd failover	1st failover	2nd failover	1st failover	2nd failover
■ [A] 10 route & 20pps(2pps per flow)	0.15	0.20	0.15	0.15	0.15	0.15
□ [B] 10000 routes & 20000 pps (2pps per flow)	0.16	0.14	1.20	1.28	2.39	2.78
▨ [C] 40000 routes & 80000 pps (2pps per flow)	0.16	0.15	3.69	4.05	9.45	9.01

表２. BGP PIC Edge を有効にした場合の効果測定結果

表２における全６列の内訳は左から[1]・[2]・[3]で，各２回ずつ実施している．表の値はこれらのパターンに対してそれぞれ経路数および印加レートを変えて試験を行った際の結果となる．

表中の値より，BGP PIC の特徴が IP トンネル環境でも再現されていることが伺える結果となった．

なお，中継ルータのインタフェースで no shutdown を実行した際の切り戻りにおいては，表中[C]の条件下で各パターンの間で，一瞬パケットが破棄される現象の発生有無が生じた．PIC 有りの場合では発生は２回中０回であり，PIC 無しでは１回・バックアップパス無しでは２回とも発生した．

参照上の注意点として，PIC を利用していないパターンでは FIB の更新処理を終えたアドレスを宛先として持つ通信から順次復旧していく．このため，全フローが復旧に至るまでの時間，つまり全ての通信が障害の影響を受けずに転送可能になるまでの時間は表の値より長い結果となる．テスターの出力を観測していた結果，表中[C]の条件下で通信の破棄が開始されてから全ての通信フローを受信する様になるまでに要した時間は，PIC 無しで１回目７秒程度・２回目８秒程度・バックアップパス無しで１回目 13 秒程度・２回目 12 秒程度となっていた．

3.3. EIGRP LFA over IP Tunnel

前項の試験で利用した通信に対し，プライマリ／セカンダリのパスが共通且つ LFA が保持される様に構成を変更した．その論理構成を図７に示す．なお，R1・R4 間および R2・R3 間のトンネルはセカンダリの WAN を経由する様に Static Route を設定している．

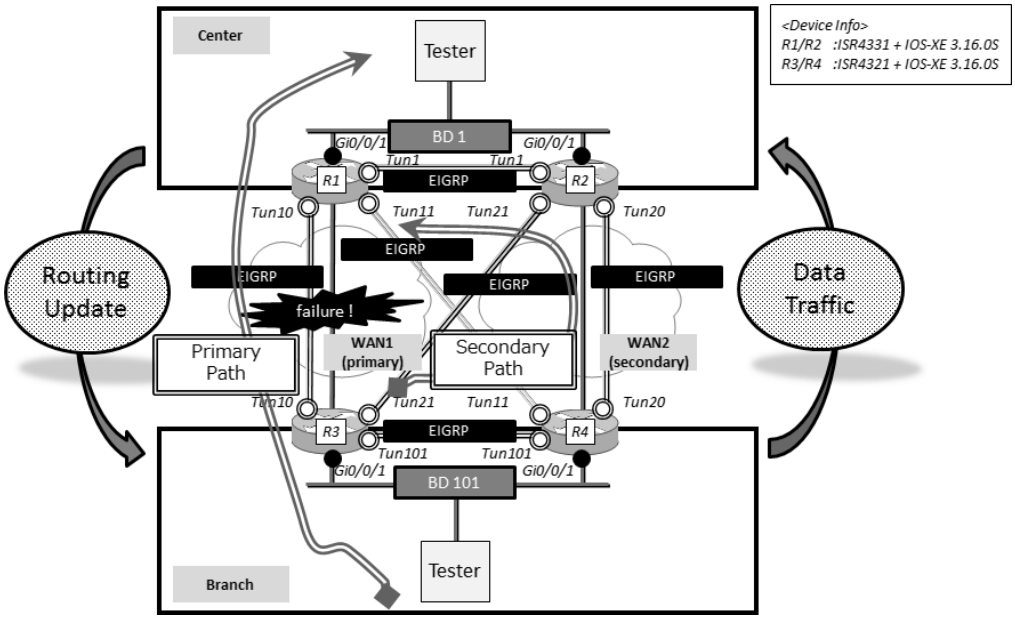
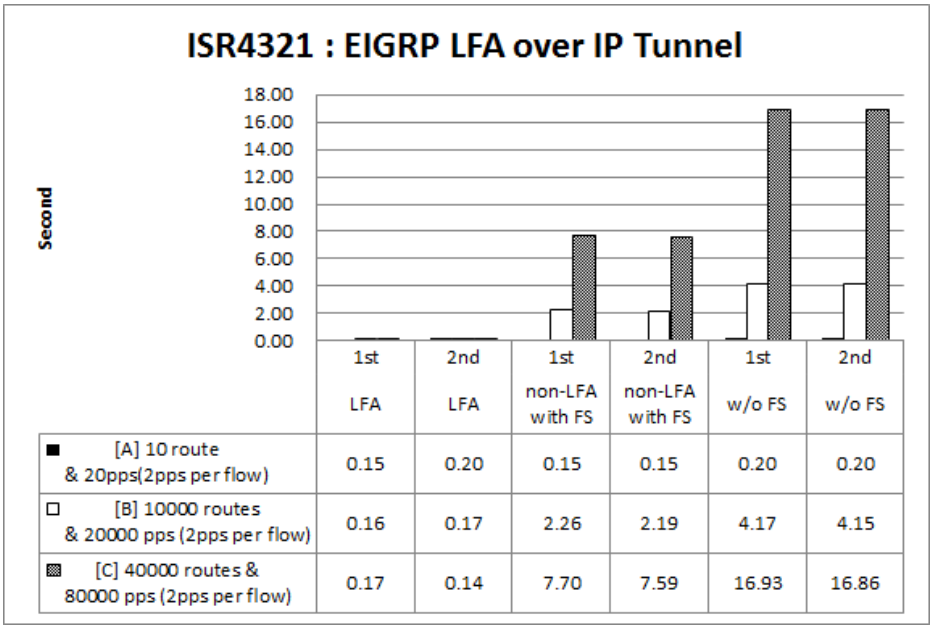


図７．　EIGRP LFA を用いた試験構成

EIGRP LFA を有効にしたパターン[1]の他，比較対象としてフィージブルサクセサを持つが LFA PIC を有効にしていないパターン[2]およびフィージブルサクセサを持たないパターン[3]を同様の物理・論理構成上で設定変更によって用意した．

この構成に対し，測定された断時間を表３に示す．

表 3.　EIGRP LFA を有効にした場合の効果測定結果



	1st LFA	2nd LFA	1st non-LFA with FS	2nd non-LFA with FS	1st w/o FS	2nd w/o FS
■ [A] 10 route & 20pps(2pps per flow)	0.15	0.20	0.15	0.15	0.20	0.20
□ [B] 10000 routes & 20000 pps (2pps per flow)	0.16	0.17	2.26	2.19	4.17	4.15
▨ [C] 40000 routes & 80000 pps (2pps per flow)	0.17	0.14	7.70	7.59	16.93	16.86

経路数の少ない条件においては断時間にほとんど差が出ないこと，保持経路数が増大すると同じフィージブルサクセサを保持している環境であっても LFA の有無によって断時間に差が生じていることが伺える結果となった.

なお，中継ルータのインタフェースで no shutdown を実行した際の切り戻りにおいては，いずれの施行においてもパケット損失は発生しなかった.

BGP と同様の注意点として，LFA を利用していないパターンでは FIB の更新処理を終えたアドレスを宛先として持つ通信から順次復旧していく. 表中[C]の条件下で通信の破棄が開始されてから全ての通信フローを受信する様になるまでに要した時間は，LFA 無しの条件で 1 回目 14 秒程度・2 回目 14 秒程度・フィージブルサクセサ無しの条件で 1 回目 34 秒程度・2 回目 35 秒程度となっていた.

3.4. IP ベースのプロテクション技術に関する試験の総括

BGP PIC・EIGRP LFA 共に，GRE を利用した VPN 環境においても正常に稼働し，期待する効果を得ることが確認できた.

4. 考察

4.1. 複数の要素に着目して確認を要するケース

異なるネイバーを経由して学習された経路に対しては，ネイバー単位で個別に障害が検出される余地を残す．このため，多数のブランチが接続される構成で断時間を確認する際は，ネイバー数の依存性についても考慮する必要がある．併せて，安定稼働のためには障害や計画停止などによって

ネットワークから一度切り離された機器が，安定的に再参加が可能であるかなどの観点でも検討が必要となる．

パスの再選出を排除する様に設計されたネットワークでは，関連処理が省略されると共に，階層化 FIB によって経路数は断時間の変動要素から除外される．このような技術を活用することによって，多数のブランチが一組のセンターに接続される環境などにおいても，断時間要求の達成が可能であるかの判断はより円滑に行われることが期待される．

一例として，前章の ISR4331 の 2 台をセンターのエッジ機器として想定し，中継の ASR1006 にて PIC Edge を有効にした BGP および GRE over IPsec での接続となるブランチ 200 台模擬する環境を構築した．詳細は割愛するが，少なくとも今回対象とした 200 ピアまでは，有意な差は見られずほとんど一定の断時間で推移している様子が伺えた．ピア数をより増加させたケース等に関する確認は今後の課題であるが，このケースではピア単位の経路数を意識せず行えることが期待され，注目すべき点であると考える．

4.2. プロテクション技術における ECMP への効用

ECMP（Equal-Cost Multi-Path）は複数のネクストホップに対するエントリが FIB 上で有効になる側面から可用性の面でも効果があり，実際に IP FRR の実現方法としても挙げられている[ii]．しかし ECMP 構成においても FIB 上でフラットにエントリが登録される場合，障害時に無効となったネクストホップを切り離す際には，全エントリに対して更新処理が発生する．この場合，規模に応じて断時間が大きく変動する余地を残すことになる．

EIGRP LFA や BGP PIC Edge の設定追加が ECMP 構成に及ぼす影響を確認するため，ECMP を利用する構成においてセカンドベストのパスを保持するケースと同様の断時間測定を行った．本試験用に前章の環境を一部変更して構築した試験構成を図８に示す．また，試験結果を表 4 に示す．

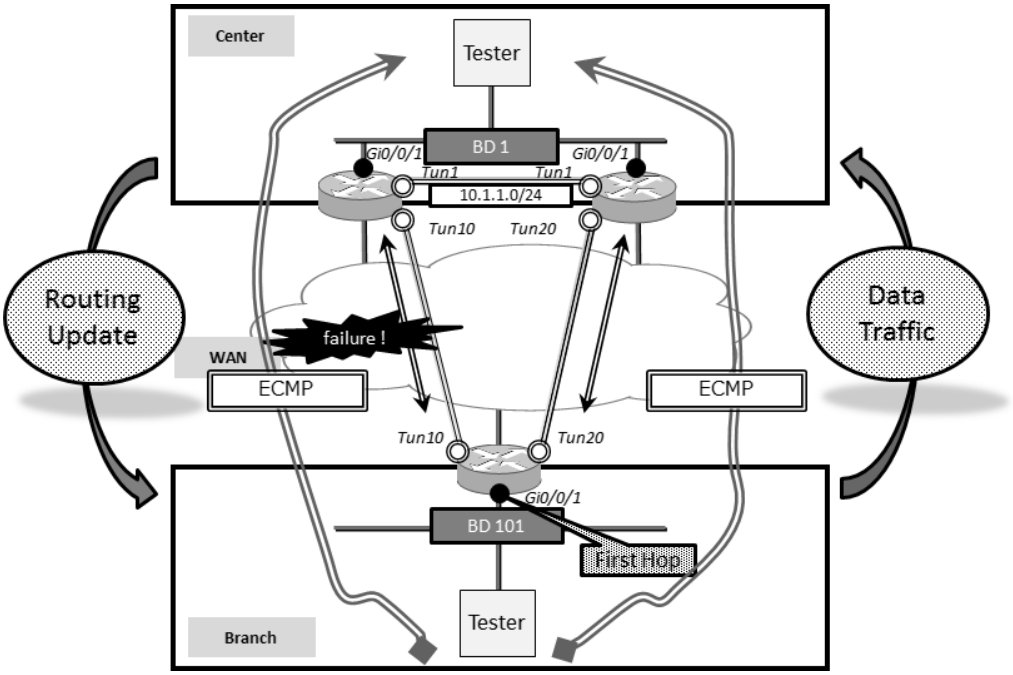
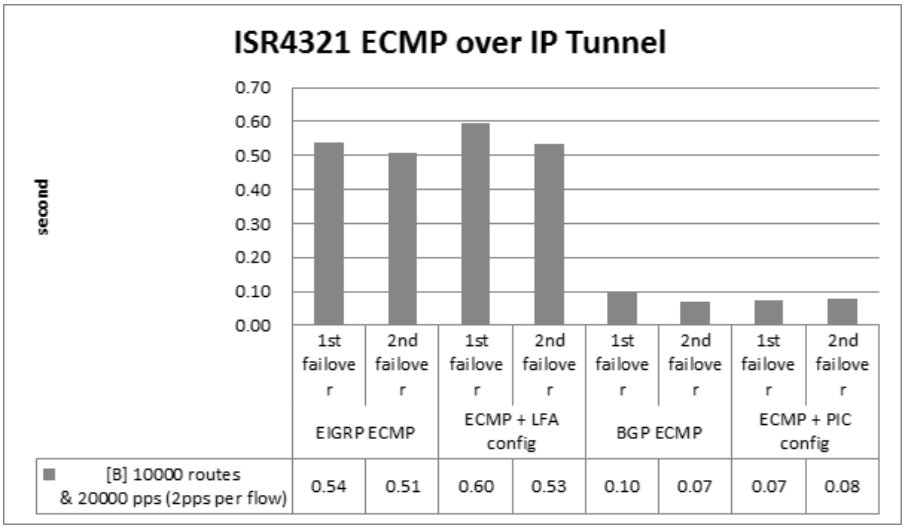


図 8.　ECMP を用いた冗長化構成

表 4.　ECMP 構成において LFA・PIC を有効にした場合の効果測定結果

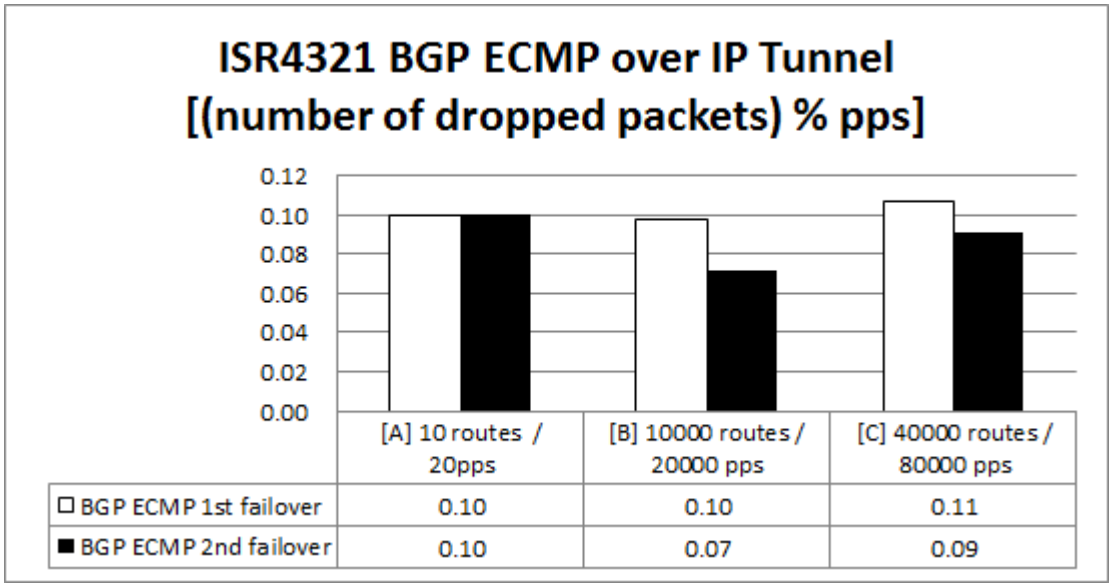


本試験の結果より ECMP 構成において LFA および PIC の設定追加は断時間に影響を及ぼさないことが確認できた.

なお，ECMP のネクストホップ選択は転送パケットのフロー情報に基づいて行われることが多く，この場合宛先 IP アドレスの異なる通信間で伝送路は分散される．結果，障害発生時のパケット損失数は障害の影響を受けないパスで転送されるフロー数に応じて小さい値となる．前章の結果と比較して，本試験結果の値が減少している状態はそのためであり，断時間の短縮が実現されているわけではない.

注目すべき点として，FIB エントリ上のネクストホップおよび出力インタフェースが EIGRP の際と同一であるにも関わらず，BGP を利用した際の ECMP 構成は BGP PIC Edge を有効にした場合と同等の断時間および経路数非依存性を示していた．その結果を表 5 に示す．

表 5.　経路数に着目した BGP ECMP 構成の効果測定結果



	[A] 10 routes / 20pps	[B] 10000 routes / 20000 pps	[C] 40000 routes / 80000 pps
□ BGP ECMP 1st failover	0.10	0.10	0.11
■ BGP ECMP 2nd failover	0.10	0.07	0.09

これは BGP PIC Edge が Multipath においても効果を発揮する機能であり，ECMP 構成では専用の設定を行わず有効化されることに起因している．

また, BGP は主要な用途やデフォルトのパラメータなどから収束に時間を要するイメージがあるかもしれないが，IGP と遜色ない断時間が実現できることが改めて確認できた．本試験構成ではフラッピング耐性等の考慮は行われていないが，使い方によって十分に高速な切り替わりを提供できることが伺える．

4.3. プロテクション技術における直近で活用可能な実装と期待される実装

EIGRP LFA はバックアップパスとしてフィージブルサクセサを利用するため，既存ネットワークが EIGRP を利用しフィージブルサクセサを持つ様に設計されていれば，シームレスに導入することが可能である．EIGRP LFA は IOS-XE 3S でのサポートとなるがブランチ向けとなる ISR4000 シリーズでも GRE 環境を含めてサポートされているため，ISR4000 シリーズへのリプレースなどの際には既に活用可能な実装と言える．

なお，OSPF LFA は，現状 Tunnel インタフェースを保護の対象とすることができないという制約がある．エンタープライズ WAN では OSPF の利用を継続する環境も多く存在するため，サポートが行われれば，適用場面を拡大できる可能性が考えられる．

BGP PIC Edge は IOS 15M/T でも利用可能であり GRE 環境への適用もサポートされている．エンタープライズ WAN においても更改などを機にルーティングプロトコルを BGP に載せ替える検討

はしばしば行われており，その際には積極的に注目すべき機能であると言える．BGP PIC Edge を利用する際にはバックアップパスをどのように保持するかが検討事項となる．例えば図 9 に示す様な経路制御を行った場合，プライマリのエッジ機器は必要となるバックアップパスを保持することができない．このような環境に対応可能な機能の一つとして BGP の ADD-PATH が存在しており，IOS/IOS-XE ではこちらも既に実装されている[3]．

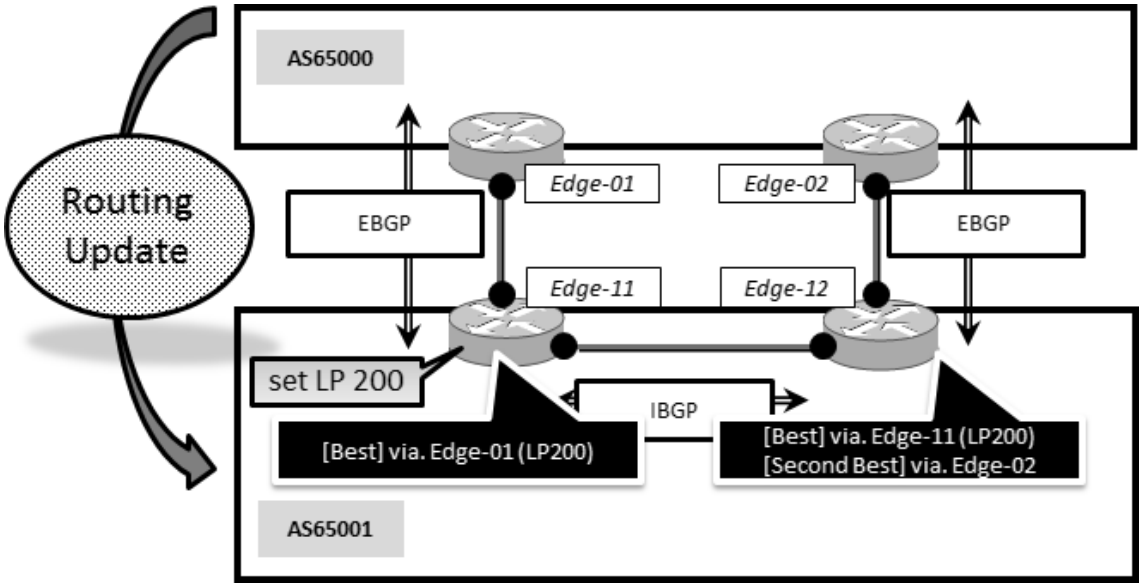


図 9.　バックアップパスの保持に別途対応が必要となる例

Cisco ルータのエンハンスメントでは，昨今の例では DPI 機能の活用や WAN 最適化の統合など，広範な分野の技術を統合することによってネットワークの付加価値を高める拡張が多く取り入れられている．同時に堅牢なインフラストラクチャを形成する分野においても積極的な拡張が進められており，この分野の技術も併せて活用することによって，より高度な水準でユーザのニーズに応えるエンタープライズ WAN を提供することができると考えられる．

5. まとめ

本稿では，拠点間接続における BGP PIC Edge・OSPF/EIGRP LFA の活用を提言した．これによって，機能追加による複雑さを低減し WAN 障害に起因するサービス停止時間を改善・予測可能なものにすることが期待される．その効果測定として Cisco Systems 社の ISR4000 シリーズを対象として検証環境を構築し，試験を行った．その結果，エンタープライズ WAN においてよく形成される冗長化トポロジに対し，期待する効果が得られることを確認できた．

[3] 今回の試験では未使用

また今回の検証を通して Cisco ルータでは高度なルーティング機能をエントリクラスのモデルから活用できることが改めて示された．様々な市場の要求に応えて実装された機能をエンタープライズ WAN に適用することができる点は注目すべき特徴であると言える．

6. 謝辞

最初に日々当社を支えて下さいますステークホルダーの方々に心より御礼を申し上げます．いつもご支援をいただいていますシスコシステムズ合同会社　パートナー営業御一同様に深く感謝の意を表します．本論文執筆の際，暖かく応援・見守っていただいた当社ビジネス推進本部第１応用技術のメンバーに改めて感謝いたします．

7. 参考文献

[i] Matthias Falkner. *Best Practices to Deploy High-Availability in Service Provider Edge and Aggregation Architectures (2014 San Francisco)*
[ii] M. Shand S. Bryant. *IP Fast Reroute Framework*. RFC5714, January 2010.