最新SD-WANソリューションの実情と技術検証

日商エレクトロニクス　中島弘一
ボスコ・テクノロジーズ　太田篤　中山裕貴　林經正

NISSHO ELECTRONICS

BOSCO Technologies

アジェンダ

- SD-WANとは？
- SD-WANの特徴
- SD-WANの特徴を評価
  - ゼロタッチプロビジョニング
  - アプリケーション志向で容易なトラヒックエンジニアリング

SD-WANとは何か？

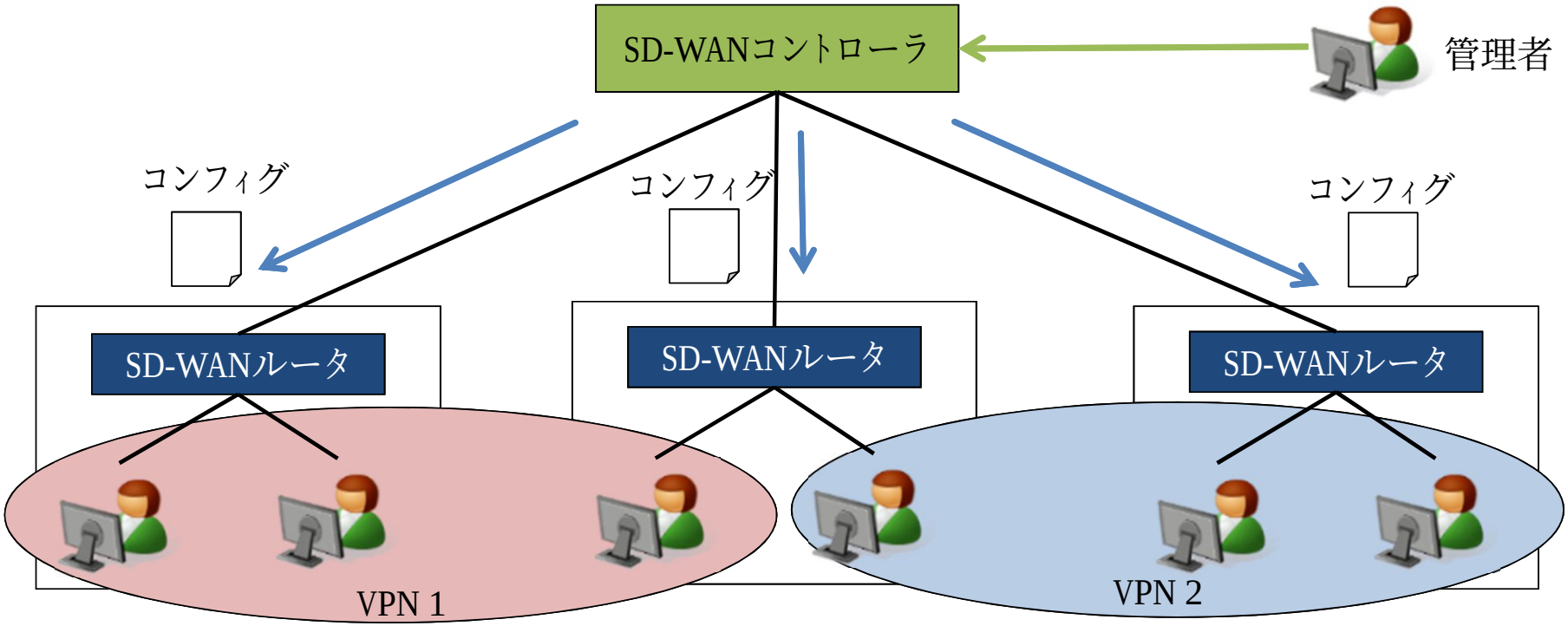
【実現するもの】
- オーバーレーイで完結できる柔軟で低コストなVPNを提供
  - お客様の申込から10分～3日程度でVPNを提供できる
  - VPN以外に種々のネットワークサービスも利用できる
- アンダーレイの面倒で時間がかかる処理を分離してVPNを提供
  - 個々の機器設定が必要なVPNプロビジョニング（ネットワーク設計）
  - 通信事業会社におけるリソース買付と設置（設備設計）

【諦めるもの】
- 精度の高いプロテクション
  - 50ms～300ms程度　→　数秒～10秒
- 精度の高い遅延伝送
  - 数ms～40ms程度　→　数十ms～40ms以上

【これまでのSDNとの決定的な違い】
- VPNやNFVを提供するネットワークサービスという意味では、差分は無い
- VPNエッジ端末（SD-WANルータ）を購入すれば、何時でも誰でもVPNを利用できる

SD-WANの基本特徴

- SD-WANルータを購入すれば、何時でも誰でもVPNを利用できる

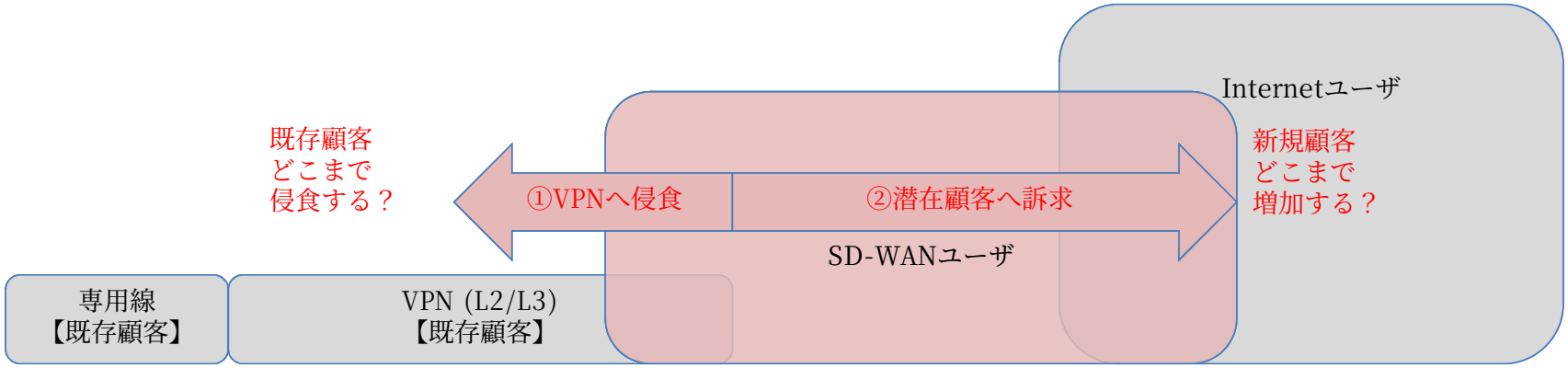


SD-WANが目指すサービスの特徴

1. ゼロタッチプロビジョニングが実現できる
   – SD-WANルータ購入からVPNサービス利用まで：～2日
2. アプリケーション志向で容易なトラヒックエンジニアリング
   – 条件を満たすための動的パス選択、帯域制御
   – 遅延インパクトの低減やアプリケーションレスポンスの最適化など
3. 短時間でネットワークを構成できる
4. どこでも同じセキュリティポリシーで運用可能
   – 柔軟なFailover機能を利用できる

SD-WANが持つイノベーションの可能性

- アンダーレイはなんでもよく、
  SD-WANルータを入手すればVPNを構築
  →通信事業会社のビジネスから、端末販売ビジネスに大きく変更
- SD-WANイノベーションの脅威
  ① 現VPNサービスを侵食
  ② これまでVPNを利用していない膨大な数の潜在顧客へ訴求



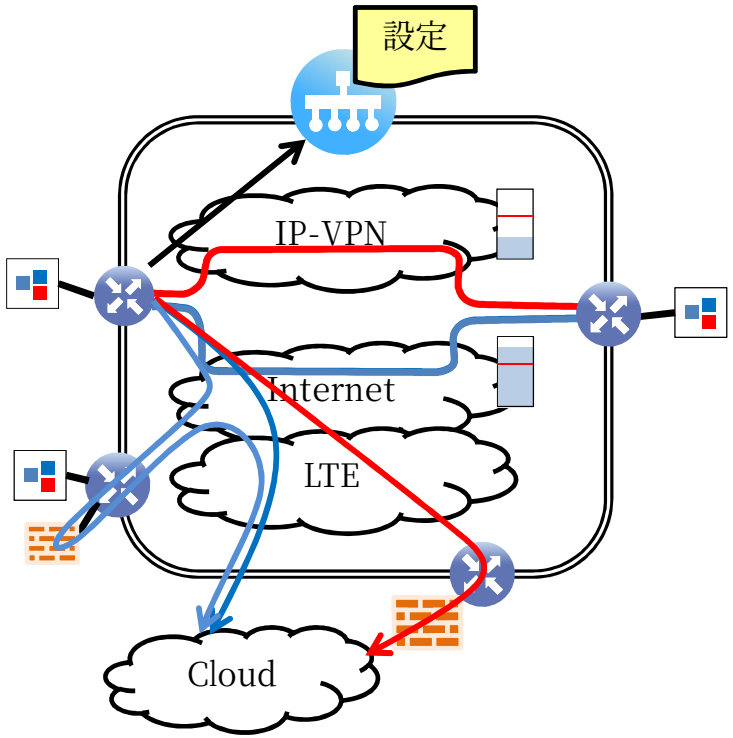
評価対象の検討

- 幾つものSD-WANベンダーが出現
  - Cisco Systems: IWAN
  - Nuage Networks
  - Velocloud
  - Viptela
  - その他
- 下記の評価が期待できるViptelaのSD-WANを評価
  - 遅延、パケットロスに対するプロテクション
  - SD-WANコントローラによるVPN制御
  - VPN接続におけるゼロタッチプロビジョニングを加速化
    - ソフトウェア版SD-WANルータの可能性

ViptelaのSD-WAN

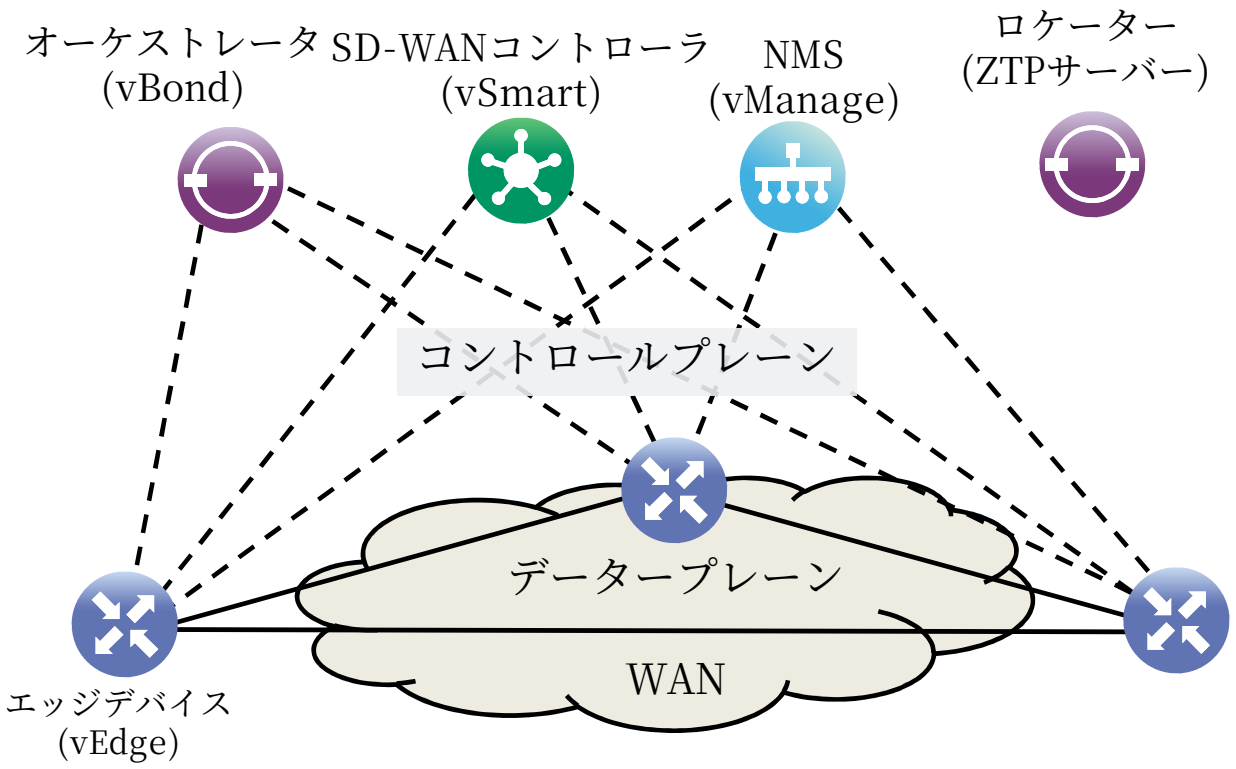
- 運用の容易化
  - 設定の集中管理／通信の可視化
- ブランチでのオペレーションの簡易化
  - ゼロタッチプロビジョニング
- 構成の柔軟性の確保
  - マルチセグメント/マルチパス
  - DPI(Deep Packet Inspection)
- アプリケーションに対する通信品質のコントロール
  - WAN回線の品質に基づく経路選択
- スケーリングの確保
  - 管理の集中化による情報の簡素化
  - ハードウェア処理による負荷の低減

ViptelaのSD-WANで実現する機能



- ゼロタッチプロビジョニング
  - Internetに接続すると、設定を自動的に読み込む
- マルチセグメント
  - 複数の独立したVPNを多拠点で構築
- 回線品質によるパスの最適化
  - 回線品質による最適なパスの選択
- アプリケーション毎のパスのコントロール
  - 通信するパスの変更
  - NFVのポリシーエンジン

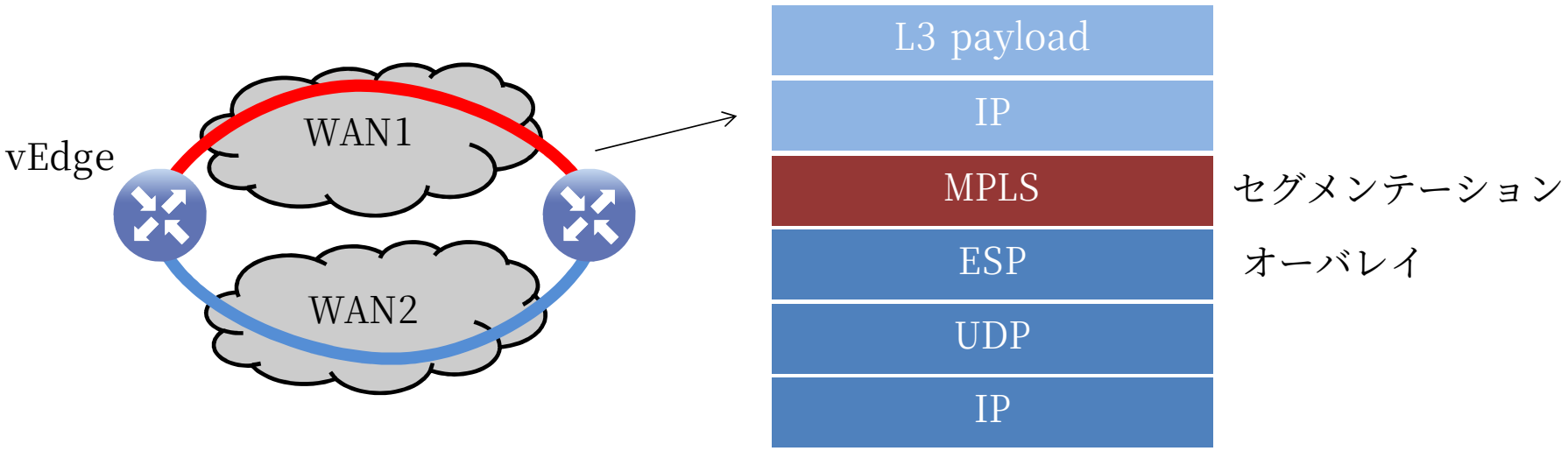
全体の構成



- オーバレイ型のSDNと似た構成
- vBond
  - オーケストレーションシステム。
    vEdgeの初期認証を行う。
- vManage
  - ネットワークマネージメントシステム。
    管理、監視を行い、GUIとAPIを提供する。
- vSmart
  - SD-WANコントローラー。
    データープレーンの通信を管理する。
- vEdge
  - エッジデバイス。データープレーンを
    構成し、実通信を行う。

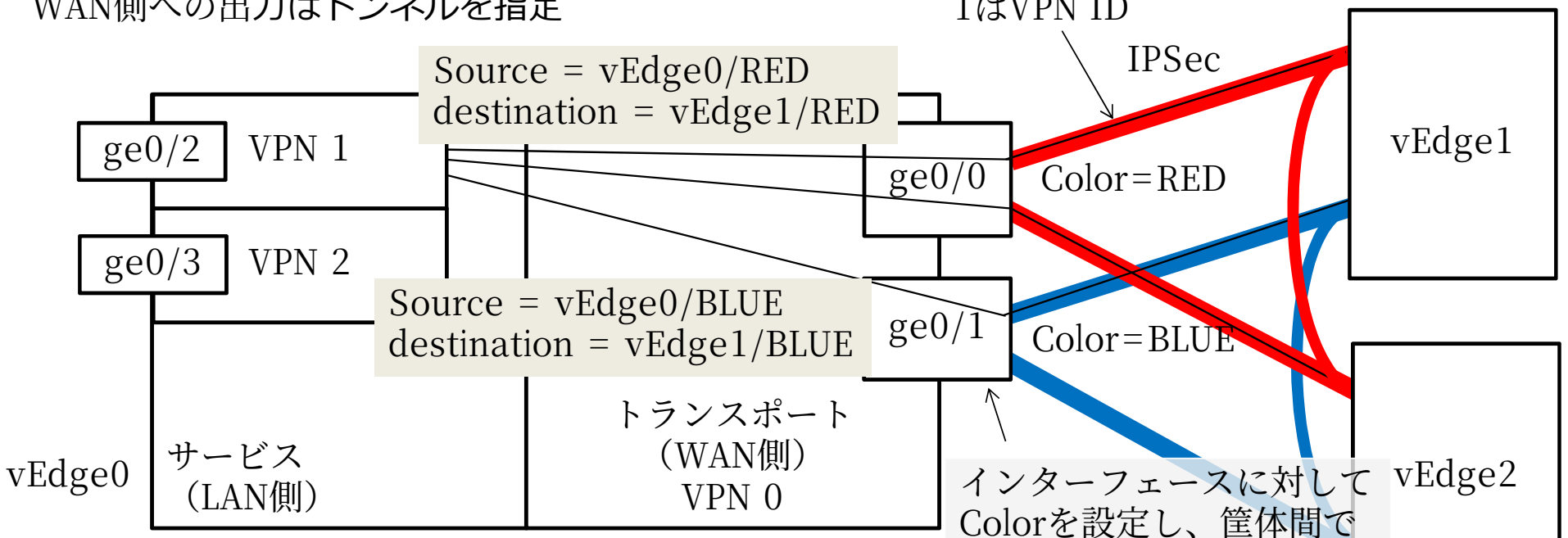
データープレーン

- vEdge間でフルメッシュに構成
- 接続情報はコントローラ(vSmart)から取得
- IPSec/GREでオーバレイ
- MPLSのLabelでセグメント毎の通信を分離



vEdge間の接続

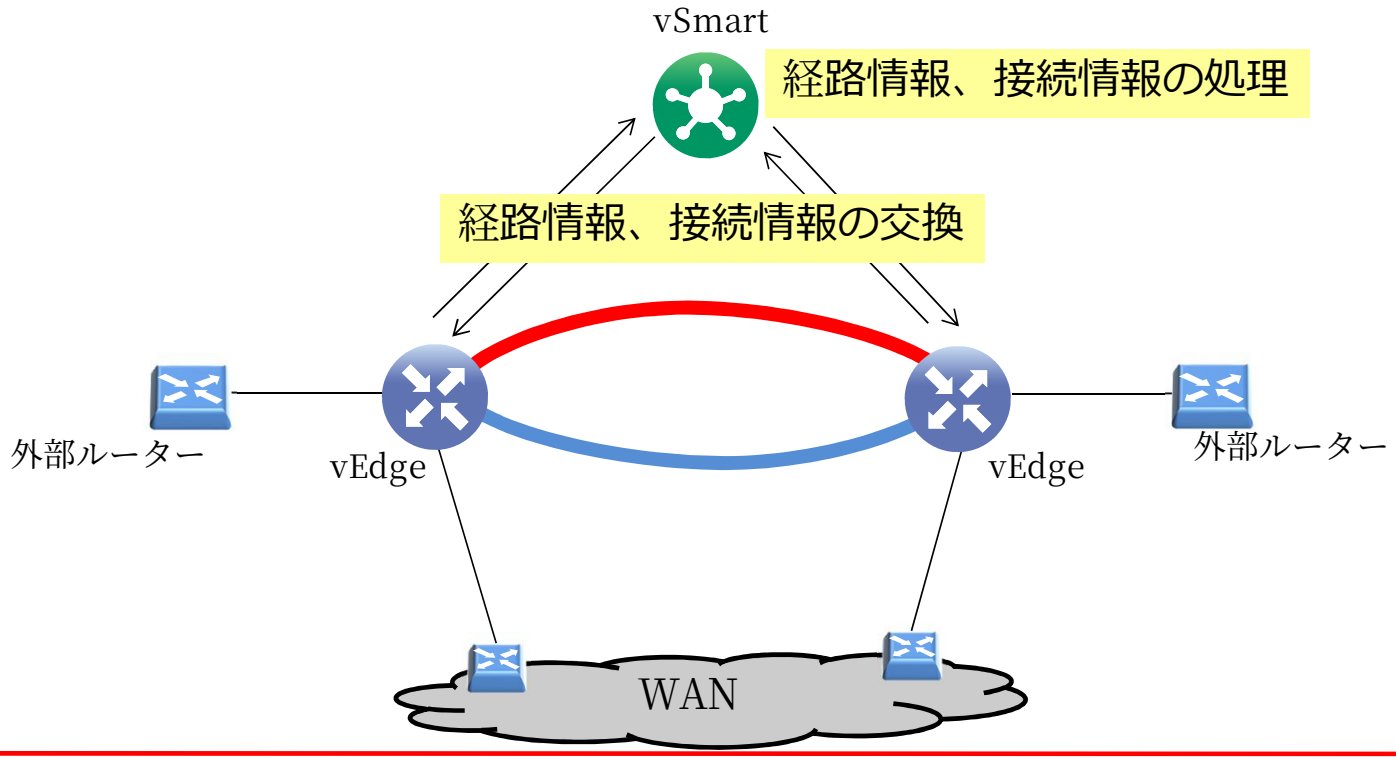
VPN毎に経路情報を独立して扱う
WAN側への出力はトンネルを指定



トンネルの生成
自インターフェースへの通信の割り当ては
トランスポート側で行う

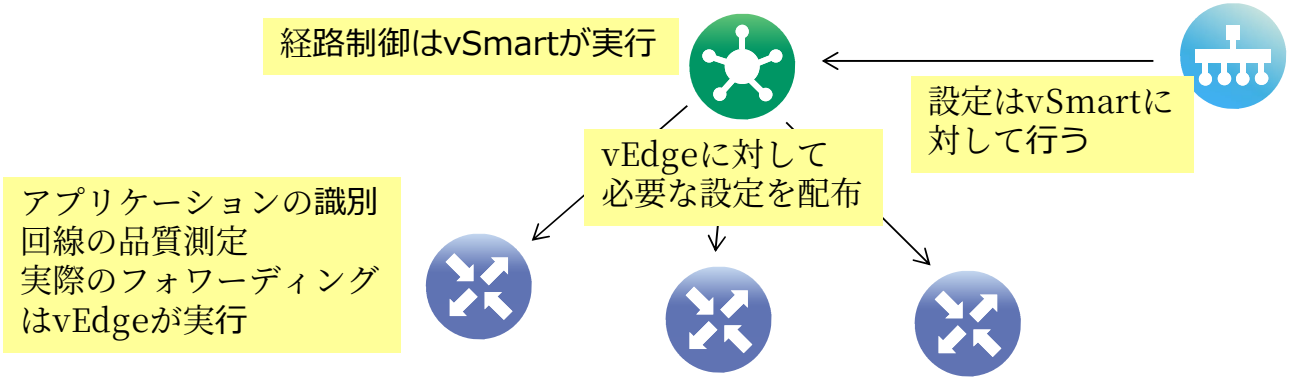
vEdge間の経路制御

- WAN経由の経路制御はvSmartが集中して制御
- vEdge内の経路はvEdgeが制御



ポリシーの設定

- アプリケーション単位の処理等特殊な処理を行うための設定
  - matchとアクションを列記する形式
- vSmartに対して行う
- vEdgeに設定が必要かは、vSmartが判断し、vSmartが行う
  - 経路制御に関わる設定はvSmartで完結する場合が有る
  - アプリケーションの識別、回線品質の測定はvEdgeが行う



ポリシーで出来ること

- マッチング条件
  - アドレス/アドレスプレフィックス
  - プロトコル
    - IP Protocol
    - TCP/UDP port
  - DSCP
  - DPI … 約3000プロトコル
  - VPN
  - Site
- アクション
  - 送信先トンネルの変更
  - 送信先vEdgeの変更
  - NATの実行
  - サーバーへの転送(NFV)
  - 回線品質制御の実行
  - 回線への重み付け
  - ドロップ
  - cflow(netflow)の設定
  - QoSマッピング

ポリシー設定例 – WAN回線品質による経路制御

アプリケーションのSLAを保つための設定。回線の品質により経路を変更する

回線の品質の測定

VPNとは別に常時測定
遅延、ロス、ジッタを
全トンネルで測定

同じ回線なので、品質も同じとみなすことが出来る。

ポリシーの処理

Protocol: rtp
SLA:
　遅延：100msec
　ロス：10%
ジッタ：2ms

vEdgeで動作

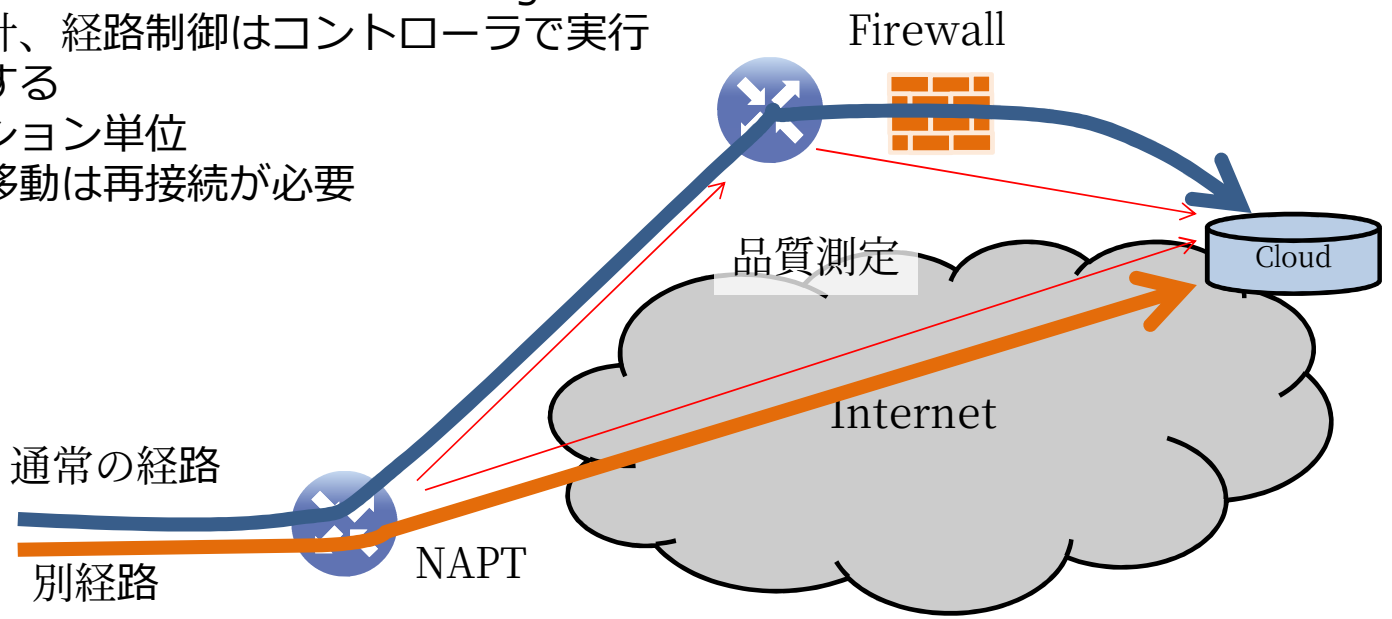
rtp以外は影響を受けない
異なったSLAの複数条件を設定可能

WAN1	WAN2	経路
loss<10% 遅延<100ms	loss<10% 遅延<100ms	WAN1 WAN2
loss>10% 遅延>100ms	loss<10% 遅延<100ms	WAN2
loss<10% 遅延<100ms	loss>10% 遅延>100ms	WAN1
Loss>10% 遅延>100ms	loss>10% 遅延>100ms	WAN1 WAN2

ポリシー設定例 – 外部サーバーへの接続の最適化

ポリシーの処理

特定のアプリケーションの監視を行い
最適な経路を計算
アプリケーションの識別、品質の測定はvEdgeで実行
品質の測定の集計、経路制御はコントローラで実行
経路制御で対応する
切り替えはセッション単位
　　新経路への移動は再接続が必要

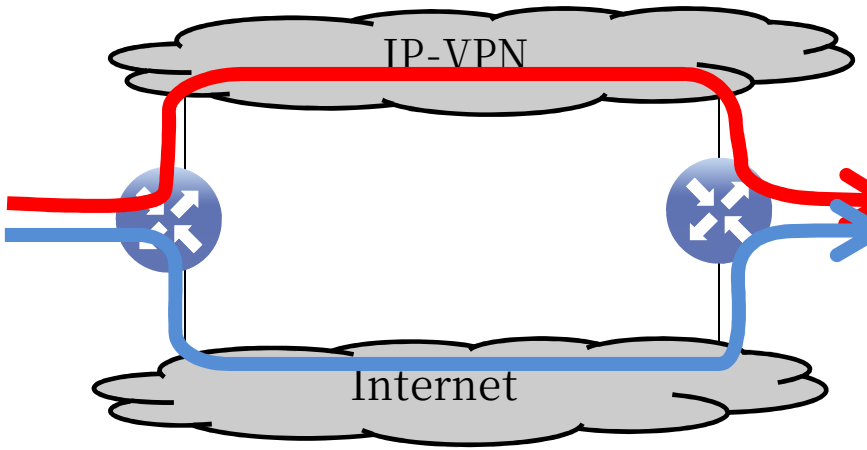


ポリシー設定例
– アプリケーション単位でのWAN経路の固定化

使用するWAN回線が複数有り、サービスレベルが違う場合等に使用するWANの固定化を行う

ポリシーの処理

Protocol: sip
Action: redの経路
Protocol: RTP
Action: redの経路
Default action:
　blueの経路



24x365サポート
復旧時間：2時間以内
帯域:1Mbps保証
Jitter:大

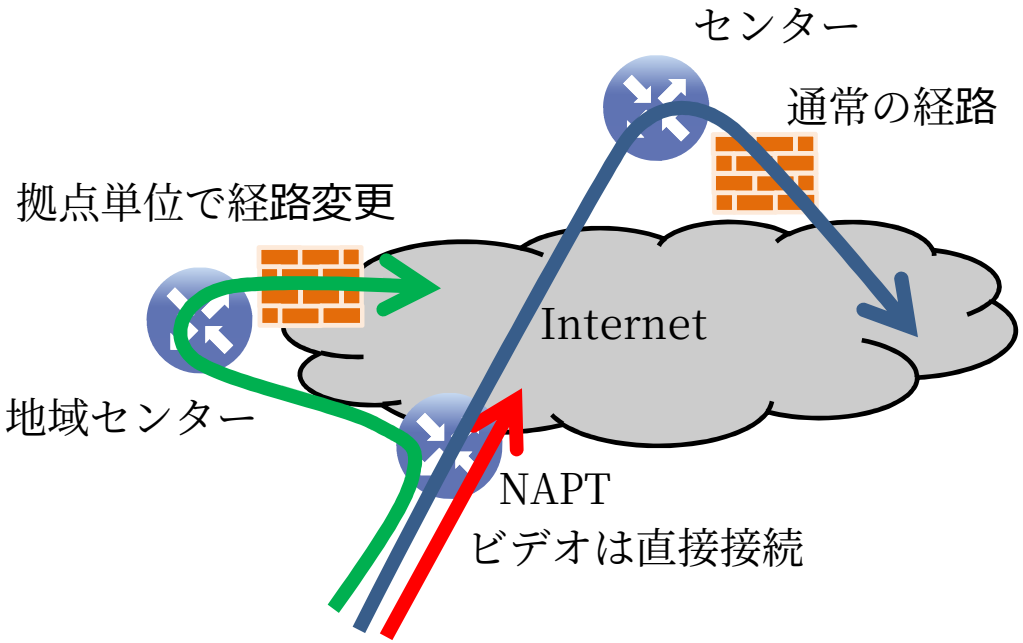
9-17時平日サポート
復旧は翌営業日
帯域:1Gbps ベストエフォート
jitter：少

ポリシー設定例 – Firewallの帯域軽減

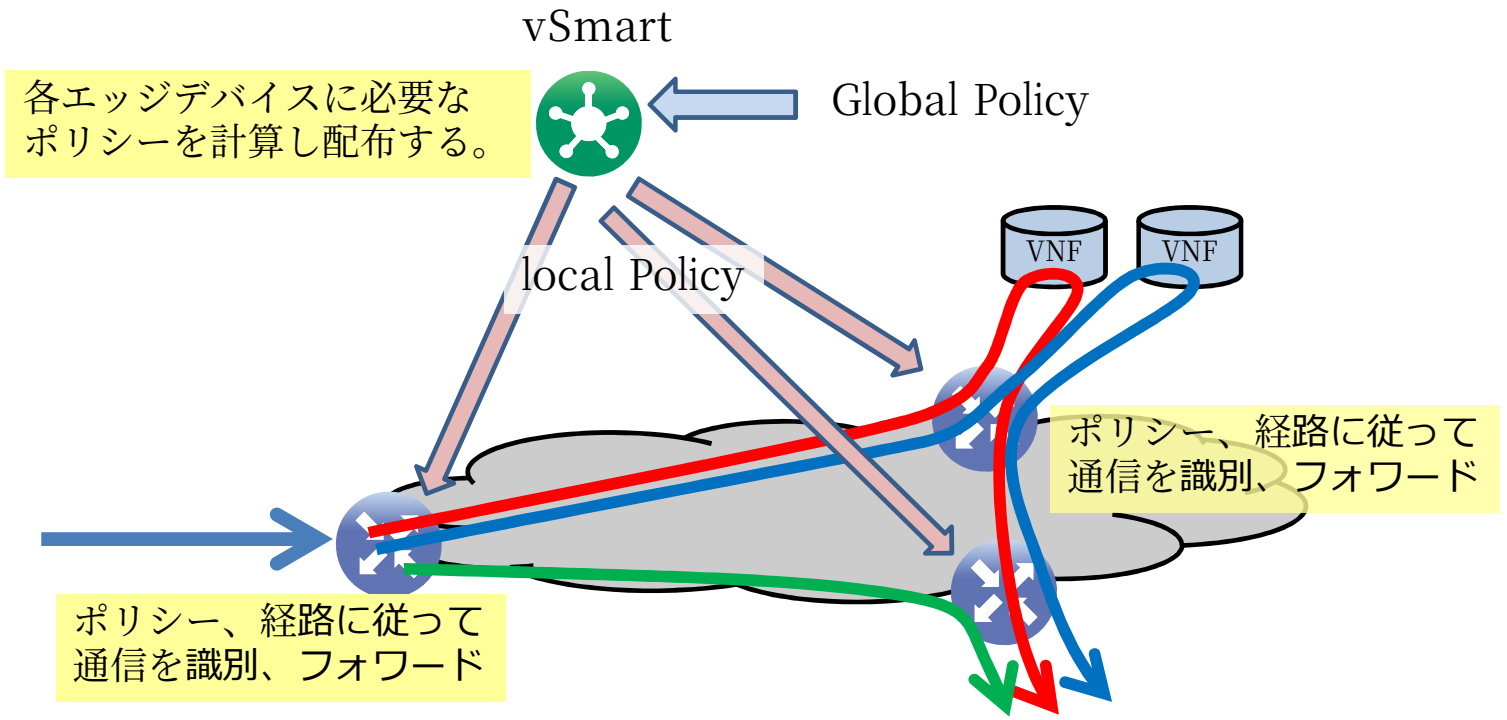
Internetへの接続を全てセンターのFirewall経由にすると、通信量が増大し
より大きいものを使用しなければならないため、通信内容によって
直接通信させたり、拠点や地域のセンターで処理を行う。

ポリシーの処理

アドレス/protocolに対して
送信先を変更する
送信先は、VPN 0(NATで直接
Internetに接続)、トンネルの指定
あるいは、破棄を選択できる。
指定しない通信は通常の経路を
使用する。



ポリシー設定例 - NFV


vSmart
各エッジデバイスに必要な
ポリシーを計算し配布する。
Global Policy
local Policy
VNF
VNF
ポリシー、経路に従って
通信を識別、フォワード
ポリシー、経路に従って
通信を識別、フォワード

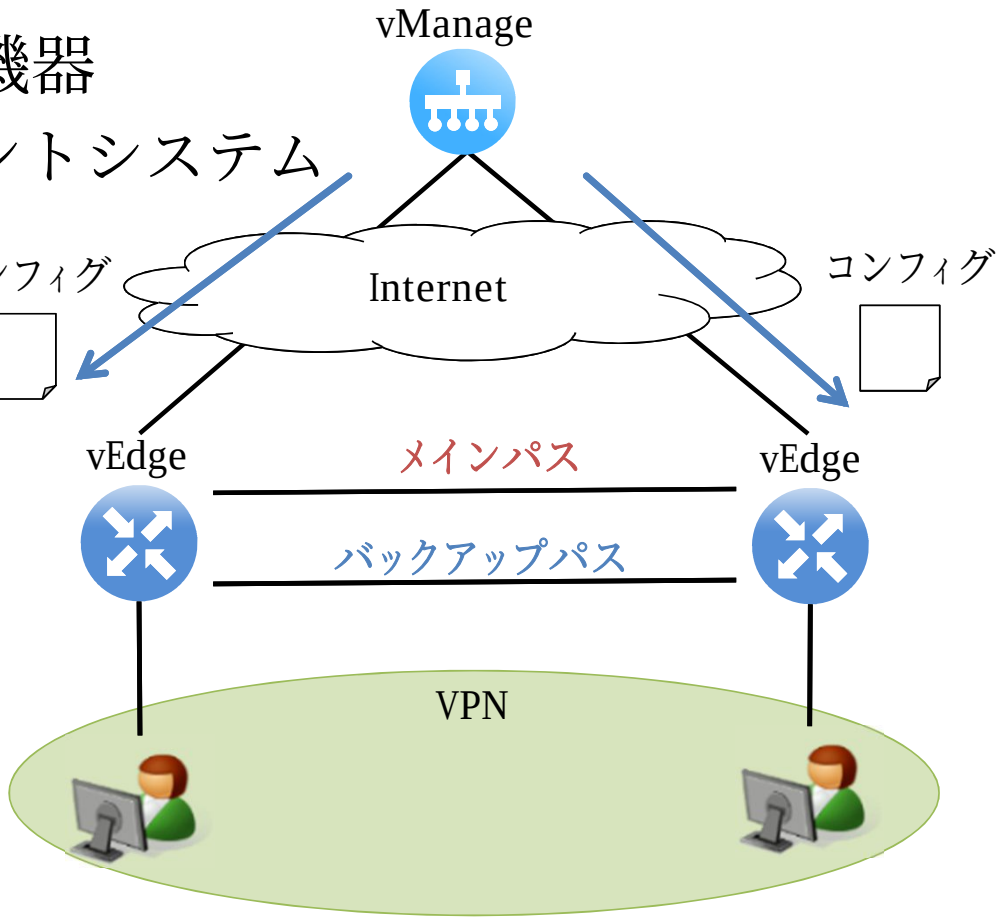
評価したSD-WANのシステム構成

- Viptela社が提供するSD-WAN機器
  - vManage: SD-WANマネジメントシステム

ゼロタッチコンフィグ
vEdgeがvManageに接続されると
自動的にコンフィグをデプロイ

  - vEdge: SD-WANルータ

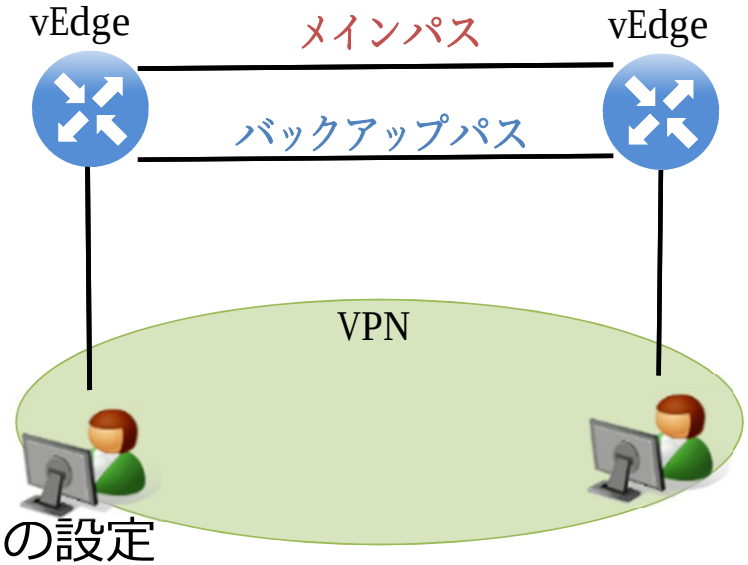
vEdge間の経路制御
障害発生時の経路切り替え
アプリケーションごとに経路選択



ゼロタッチコンフィグ

- 実際にVPN接続を確立するために必要な作業量は?
  - メーカでの作業
    - 機器購入してから届くまで –～2日
    - 初期コンフィグ投入　　- 30分
  - ユーザでの作業
    - プロビジョニング
      - ① テンプレートの作成
      - ② テンプレートを利用するデバイスの選択
      - ③ ポリシー（遅延、パケットロス管理等）の設定

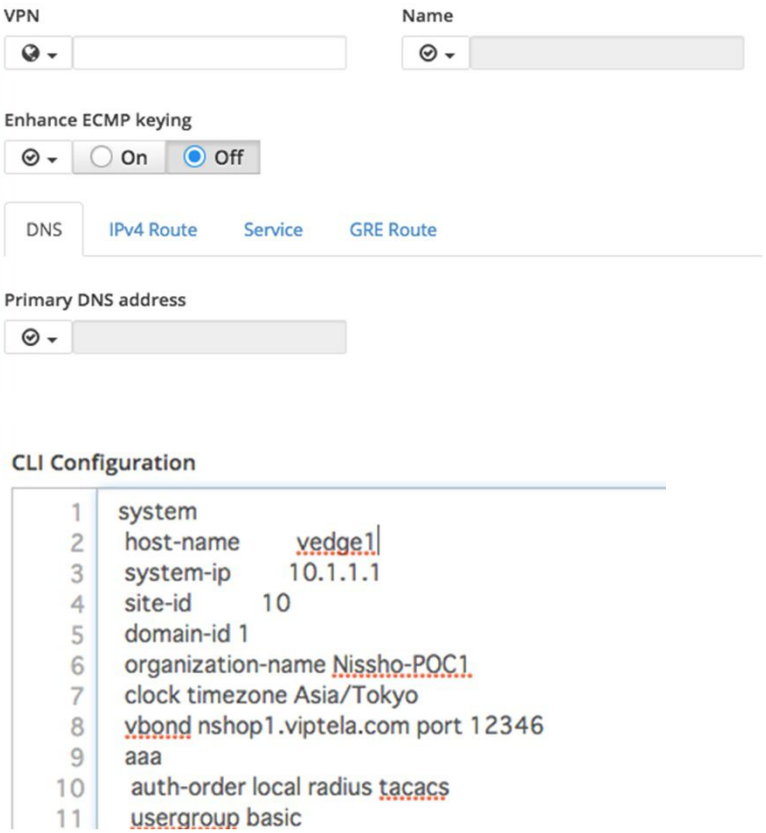
エッジネットワーク装置のコスト



ユーザでの作業に要した時間を測定

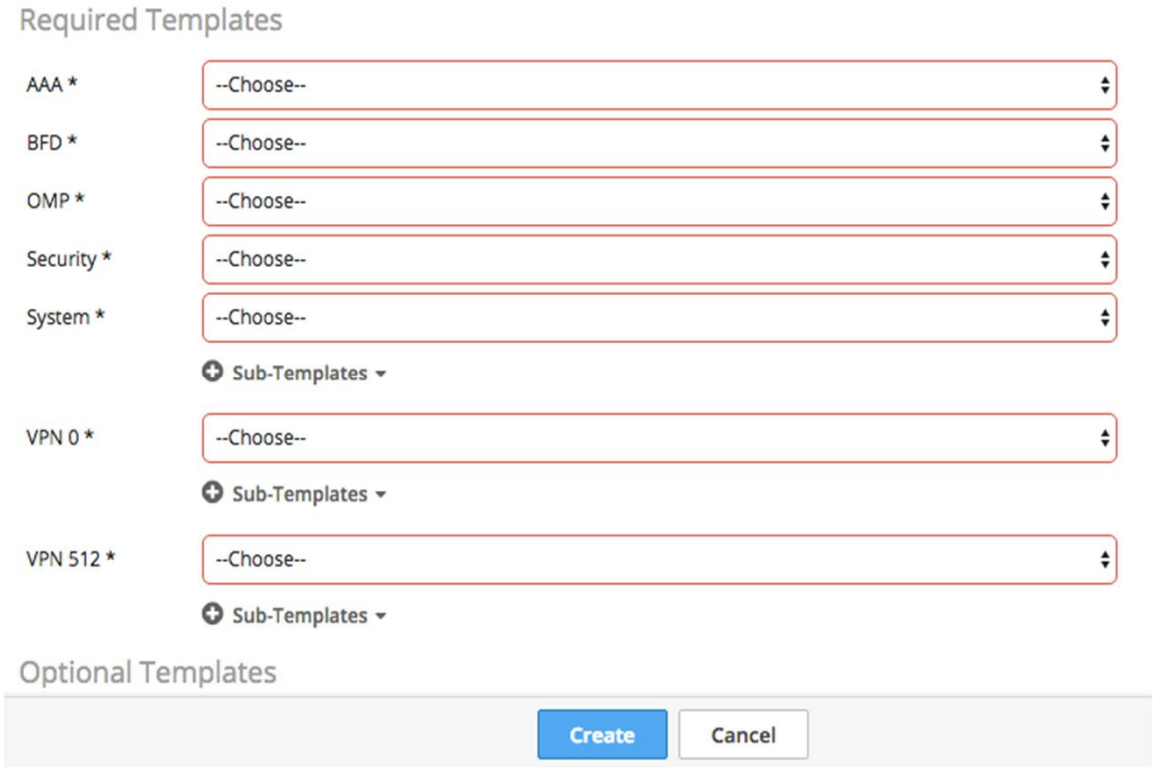
① プロビジョニング: テンプレート作成

- 2通りの方法
  - Feature テンプレート（GUI処理）
    - WebUIでの設定
    - 画面に従い穴埋めを行って設定を作成する
    - vManage上で一から設定を作成するのに向く
  - CLI テンプレート
    - 各装置のCLIと同様な内容
    - 検証等で事前に各機器上で投入した設定をvManageに登録するのに向く



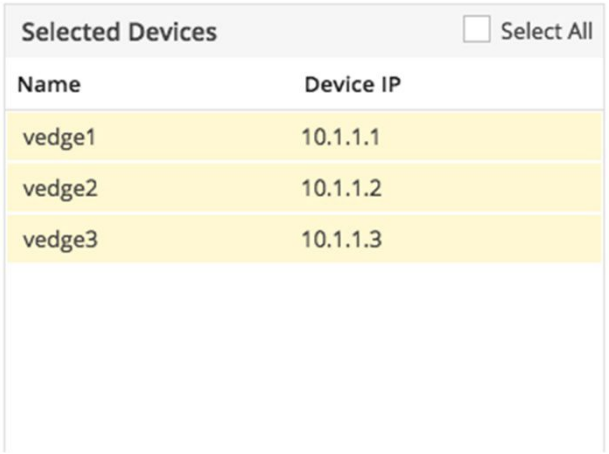
① プロビジョニング: Feature テンプレート作成

- 機能ごとにテンプレートを組み合わせる
  - vEdgeの場合
    - 設定項目: **12**
      - ユーザ認証
        障害検知プロトコル
        ルーティングアルゴリズム
        オーバレイ (IPSec, GRE)
        端末情報
        VPN
        …
    - テンプレート作成に
      かかった時間
      - **30** 分 ~ **1** 時間



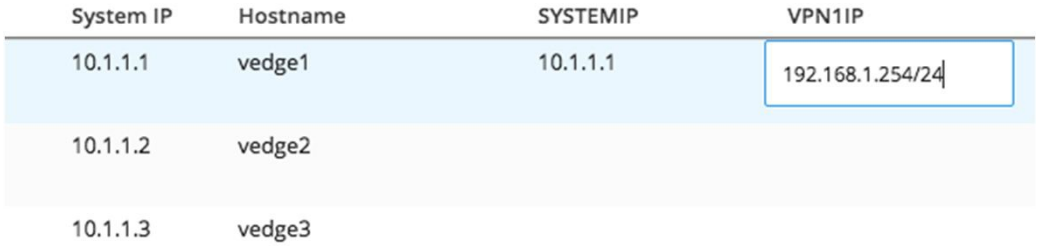
② プロビジョニング: デバイスの選択 & 変数の代入

- テンプレートを利用するデバイスを選択



- デバイスごとに固有の値を入力
  - csvファイルとして
    インポートエクスポート可

- デバイスの選択 & 変数の代入にかかった時間
  - 5 分



③プロビジョニング:ポリシー（遅延、パケットロス管理等）の設定

- CLIで記述
- 設定項目
  - 適応するアプリケーションの指定
  - 経路切り替えの閾値の指定
  - 切り替え先の経路の指定

- ポリシーの設定にかかった時間
  - 5 分

```
app-list Apps
 app icmp
 !
!
sla-class Loss_Latency
 latency 50
 loss 80
!
app-route-policy AAR
 vpn-list VPN1
  sequence 10
   match
    app-list Apps
   !
   action
    sla-class Loss_Latency preferred-colc MAIN
```

icmpパケット
遅延50ms以下かつ
パケットロス率80%以下のとき
MAIN の経路を選択

Viptelaにおけるゼロタッチコンフィグ

- ユーザ側でVPN接続にかかる時間
  - コンフィグ作成時間: 30 分 ~ 1 時間
  - vManageからvEdgeへ設定が反映される時間は 10 秒以内

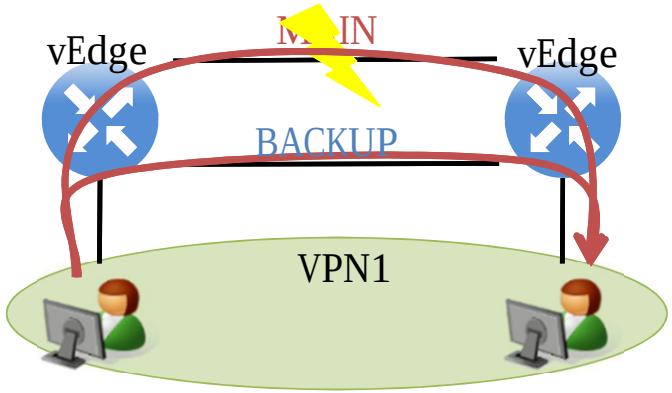
- テンプレート・ポリシーの作成にかかる時間がほとんどを占める
  - 作成するVPNの数・ポリシーの複雑さに応じて作成時間も延長

- テンプレート・ポリシーを利用するデバイスの選択は容易
  - 利用するデバイスが増えてもデプロイにかかる時間に影響は少ない

vEdge間の経路制御

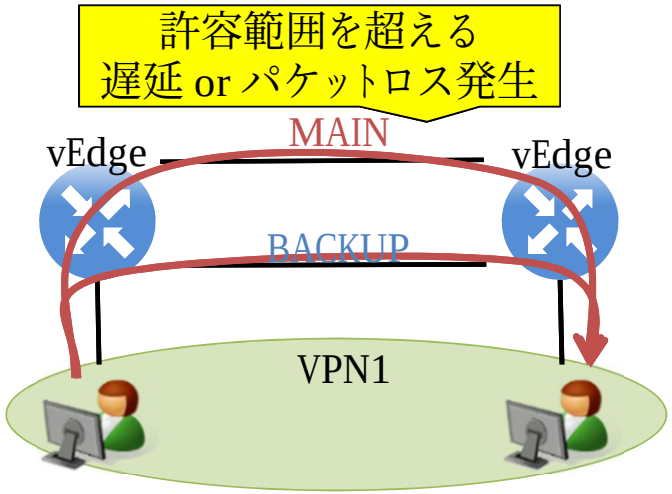
① 経路障害発生時の経路切り替え

– VPNが使用する経路を事前に複数設定しておくことで自動的に経路障害を検知・経路切り替え



② アプリケーションに応じた経路選択

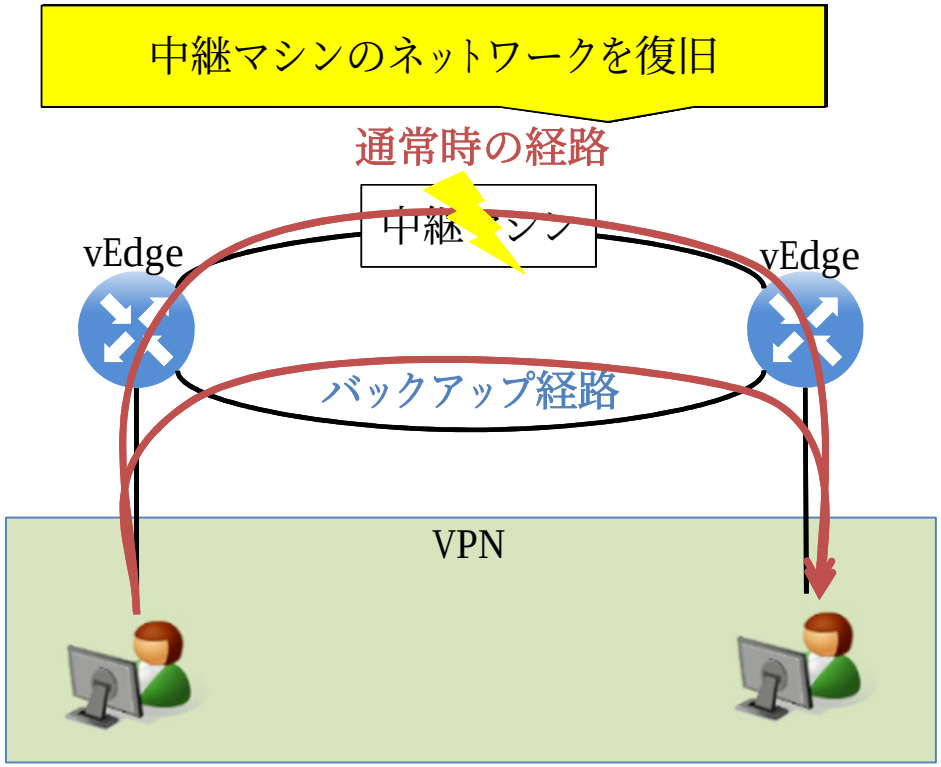
– アプリケーションごとに許容できる遅延時間パケットロス率を指定



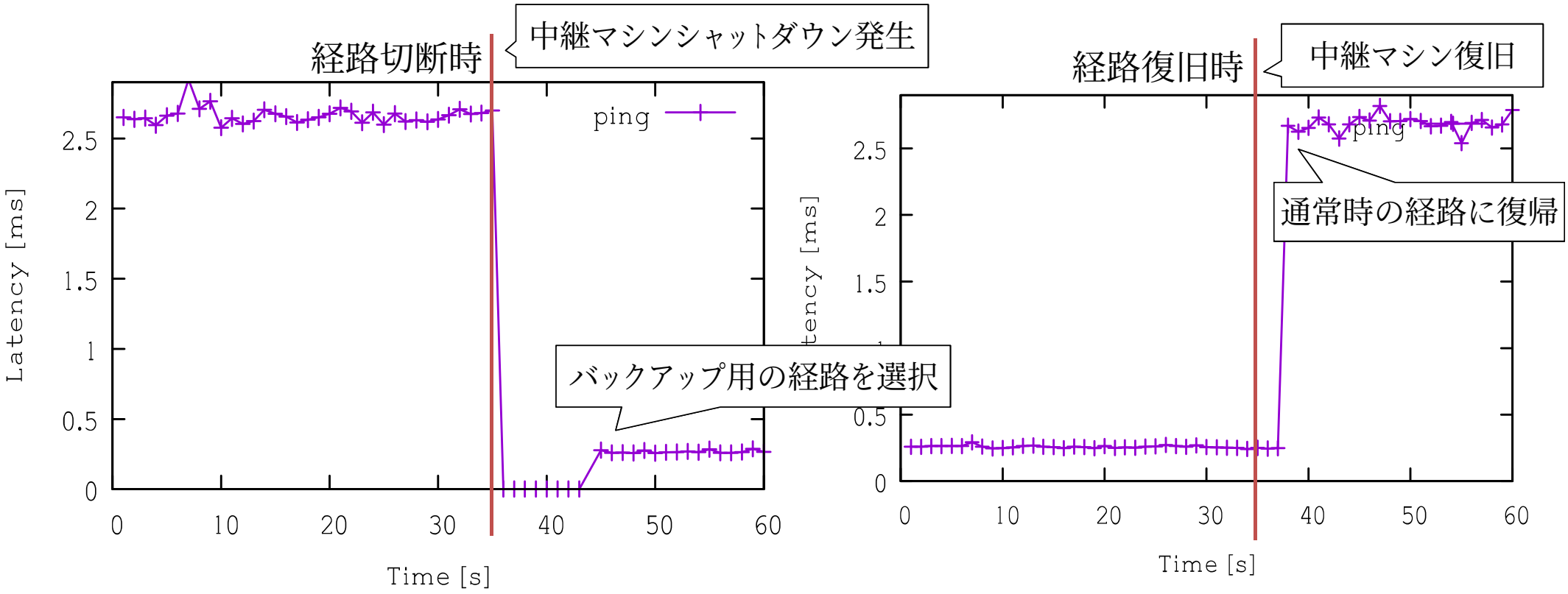
経路切り替えに要した時間を測定

① 経路障害発生時の経路切り替え

- 評価環境
  - vEdge間を2本の経路で接続
- 評価内容
  - 経路切り替え時間を測定
    - 中継マシンのネットワークを
      シャットダウンしてからバックアップへ
    - 中継マシンのネットワークを
      復旧してから通常時の経路へ



経路切断・復旧時の切り替え時間

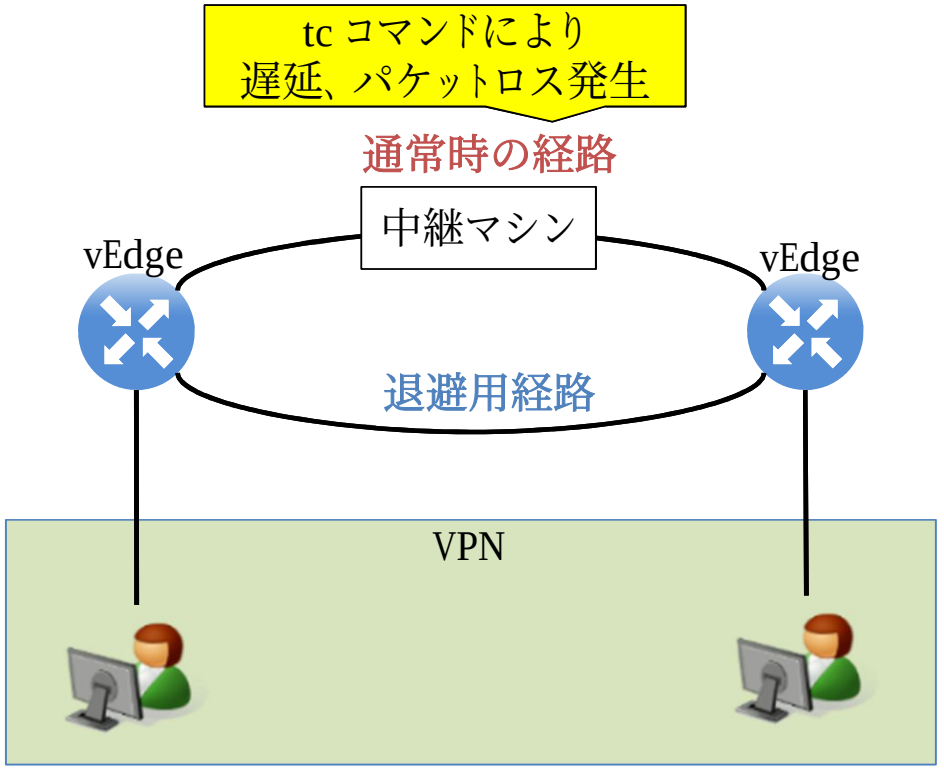


バックアップへの切り替え: 約９秒

通常時の経路への復帰: 約３秒

①アプリケーションに応じた経路選択

- 評価環境
  - vEdge間を2本の経路で接続
  - 通常時の経路で
    遅延、パケットロス率が一定値を
    超えたら退避用経路へ切り替える
- 評価内容
  - 遅延発生時の評価
  - パケットロス発生時の評価

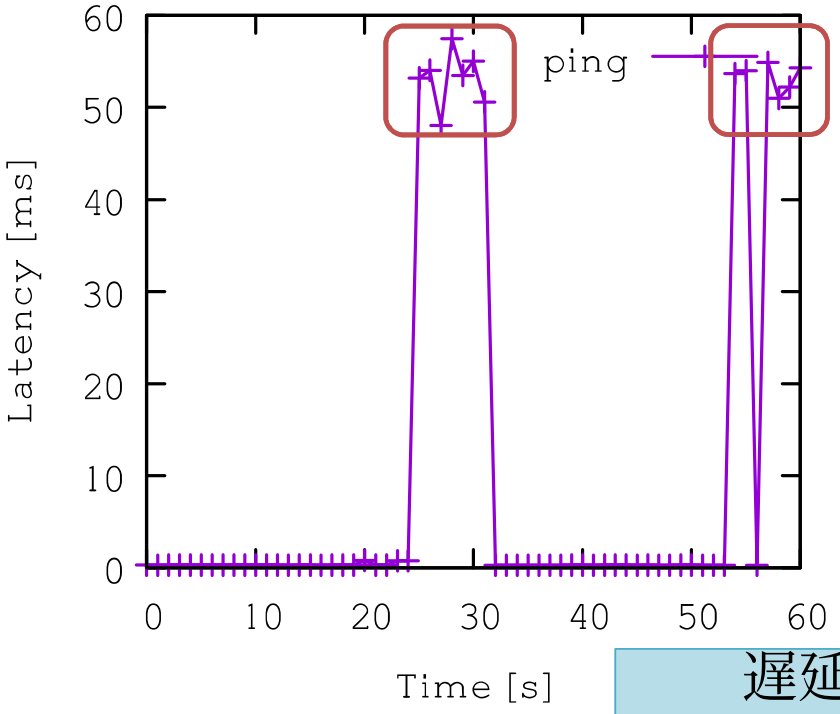


評価結果: 遅延発生時

- 遅延閾値: **50ms**

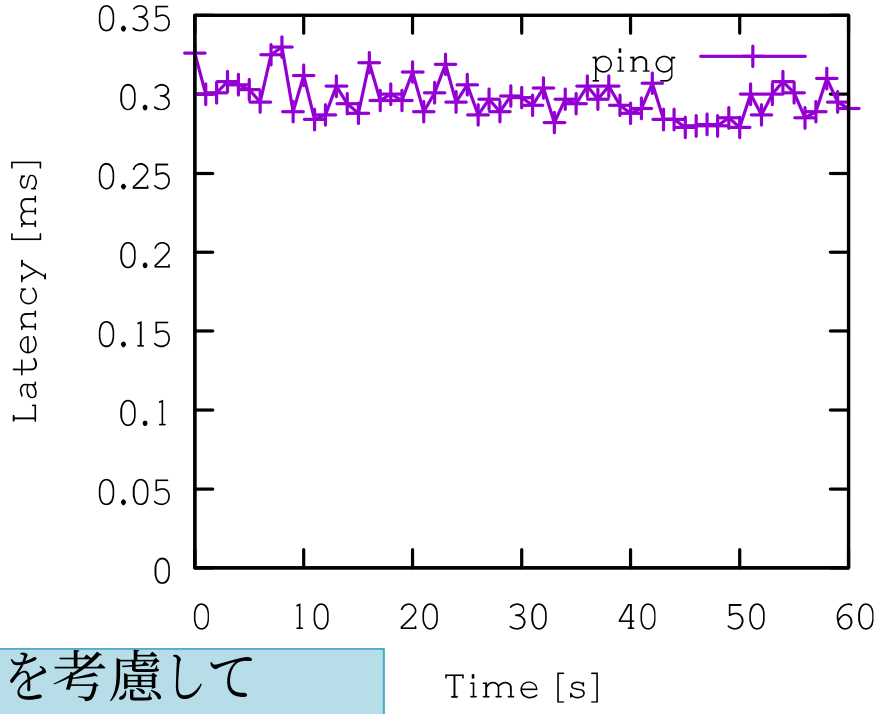
遅延が発生している経路を選択

発生遅延: 45 - 55 ms



常に退避用の経路を選択

発生遅延: 49 - 51 ms



遅延のばらつきを考慮して
閾値を設定する必要

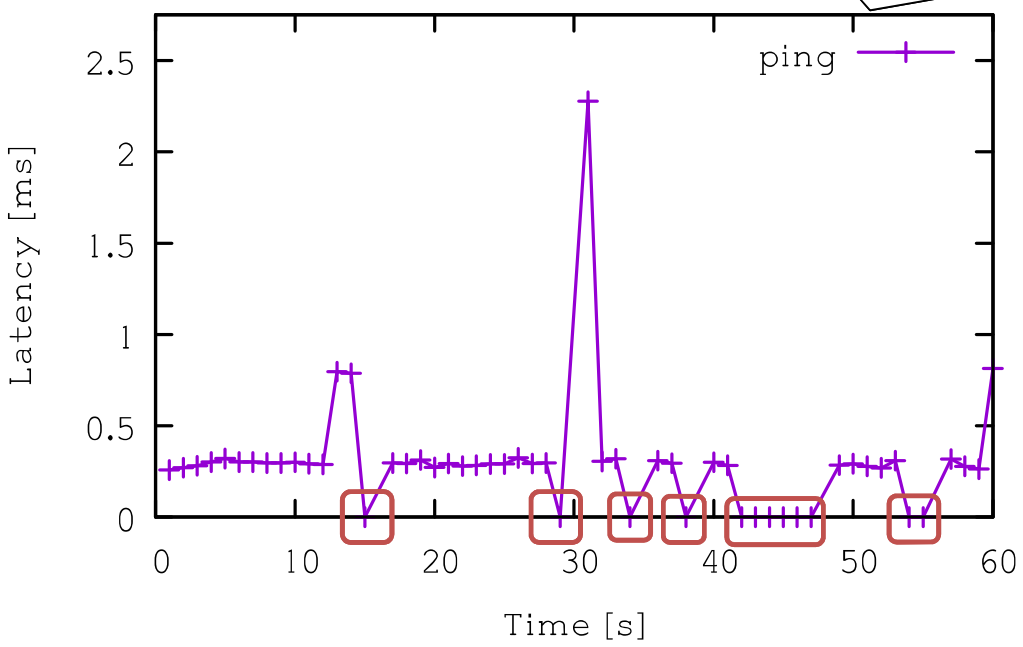
NISSHO ELECTRONICS BOSCO Technologies

評価結果: パケットロス発生時

- パケットロス率閾値: 80%

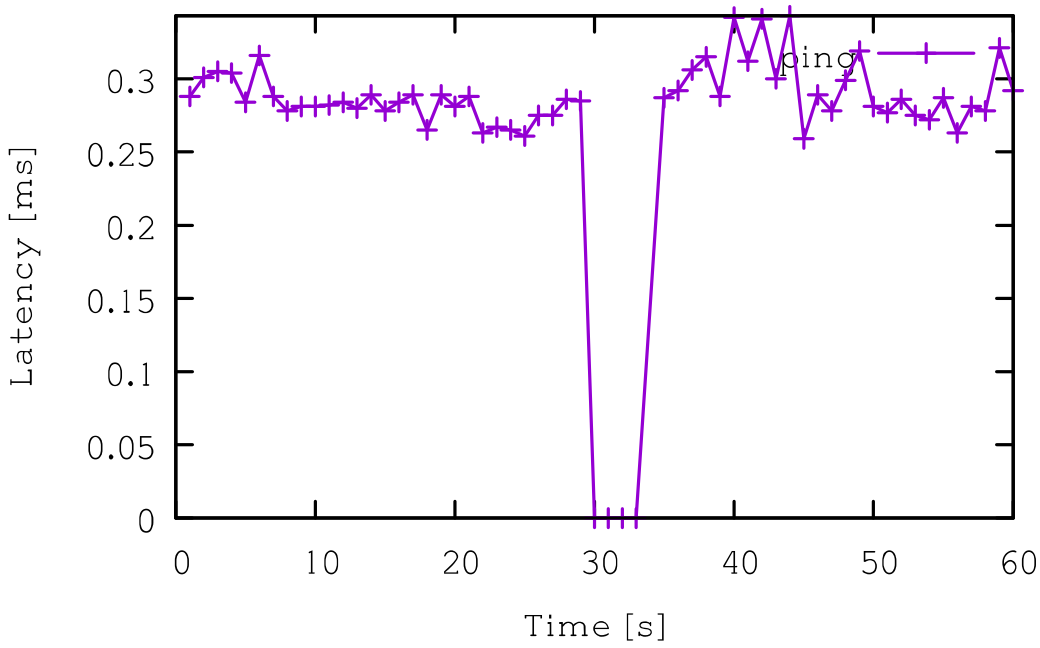
パケットロス率: 80 %

ロスが発生している経路を選択



ほとんどの場合でロスが発生していない経路を選択

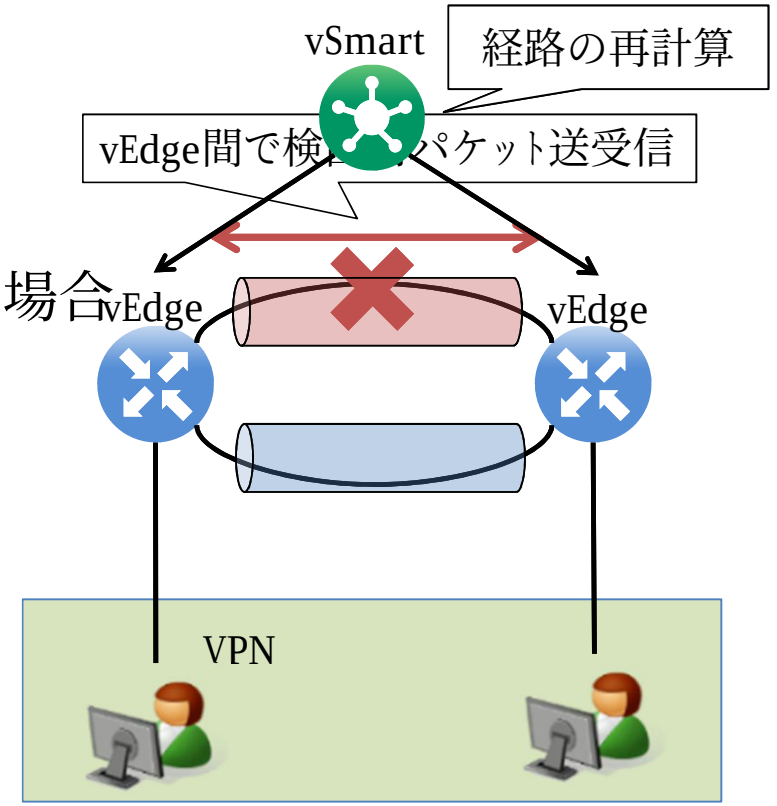
パケットロス率: 90 %



NISSHO ELECTRONICS BOSCO Technologies

経路切り替え時間の考察

- 経路切り替えにかかる時間
  - 障害検知にかかる時間
    - **障害発生時:**
      一定期間検出用パケットを受信しなかった場合
      デフォルト: **6** 秒
    - 復旧時:
      検出用パケットを一つでも受信した場合
      デフォルト: **1** 秒
    - 設定により短縮可能
  - トンネルを作成・経路の再計算
    - 約 **3** 秒



考察と今後

【本評価の考察】

- 簡易にVPNを構成できるという観点で、利用できる
  - 遅延、パケットロスを起点とした自動パス切替
  - パス切替時間は、３～９秒程度
- ゼロタッチコンフィグ
  - WebUIの提供
  - 従来は1.5ヶ月かかっていたのが 2日間ほどに短縮
  - テンプレート作成、ポリシー設定の規格化がカギ
- SD-WAN監視サービスの拡充が必要
  - 監視・通知機能
  - 外部管理システムとの連携

【今後】

- vManageのREST full API評価
  - 他のネットワークオペレーションシステムとの連携のし易さ等の評価
- ソフトウェア版SD-WANルータ”vEdge Cloud”の評価
  - 30分程度でのVPN接続の可能性評価