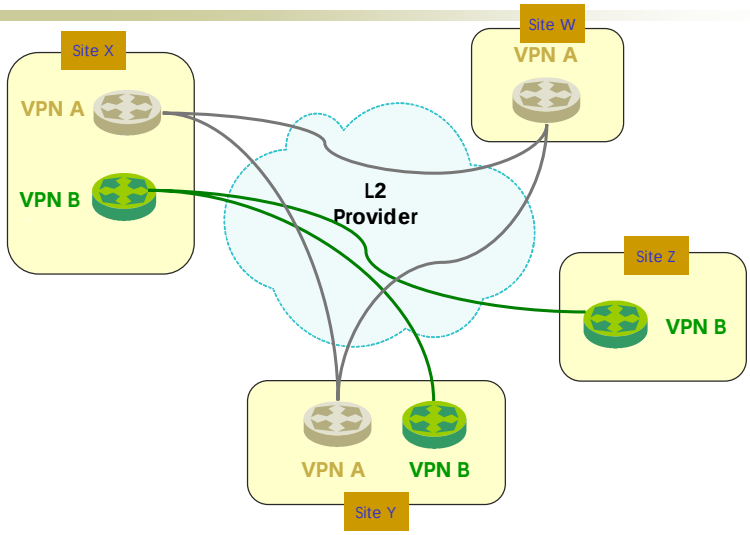
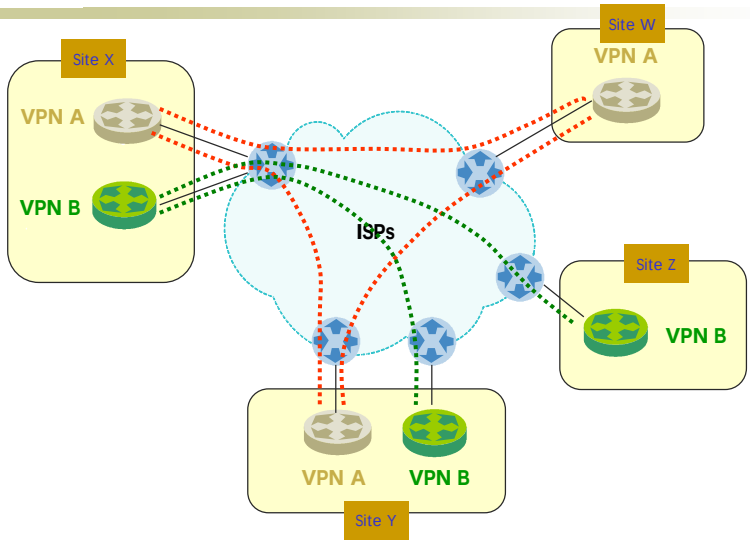
T22 : IP-VPNとPacketiX(SoftEther)

進藤　資訓
ファイブ・フロント(株)
Chief Technology Officer
mshindo@fivefront.com

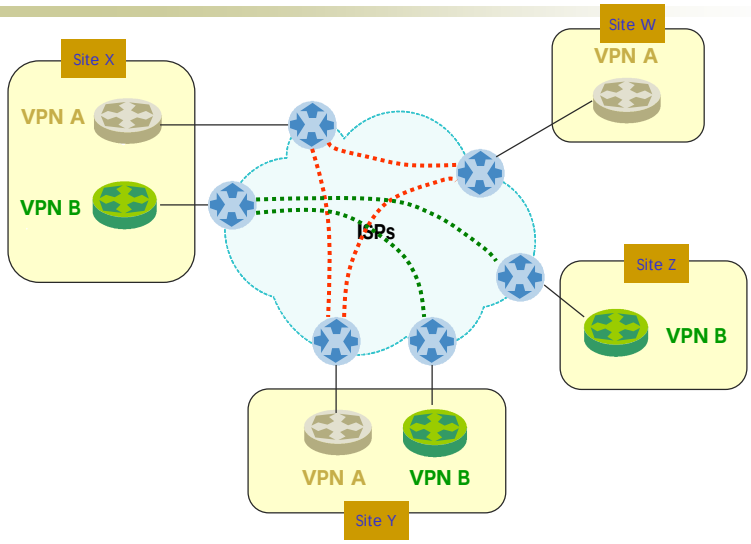
VPNの変遷（1）　～(!V)PN時代～



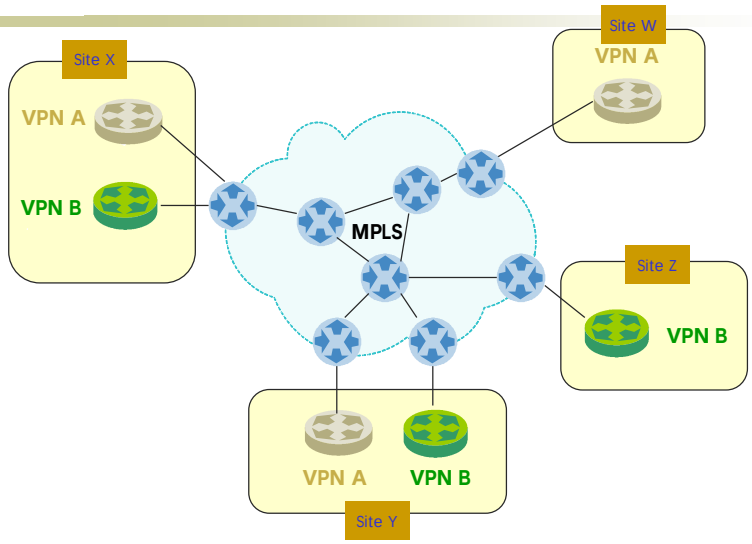
VPNの変遷 (2) ～ CE-based VPN ～



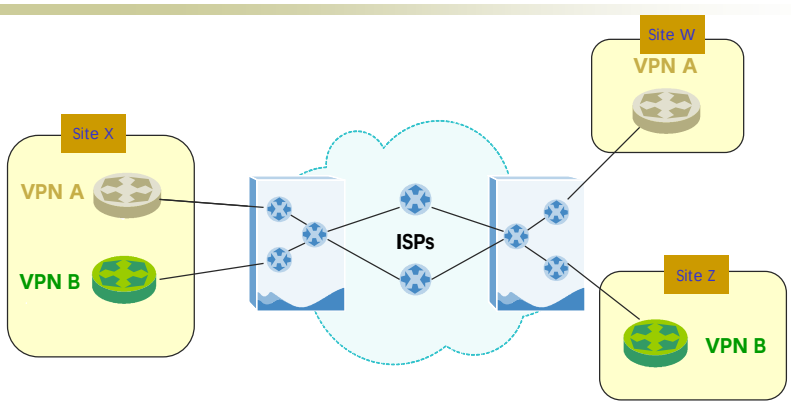
VPNの変遷 (3) ～ Managed Router ～



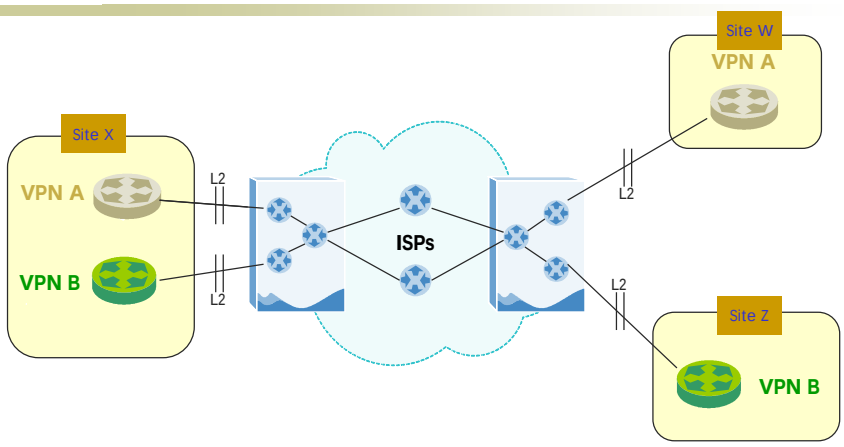
VPNの変遷 (4a) ～ Network-based VPN ～



VPNの変遷 (4b) ～ Network-based VPN ～



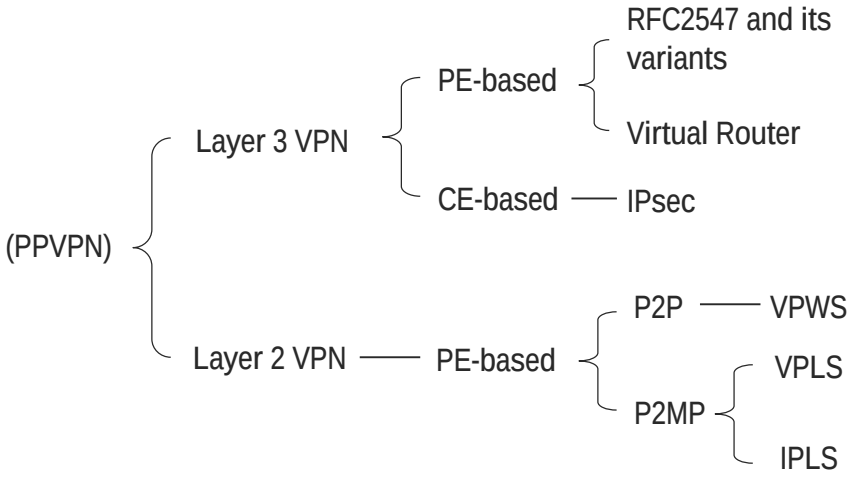
VPNの変遷 (4c) ～ Network-based VPN ～



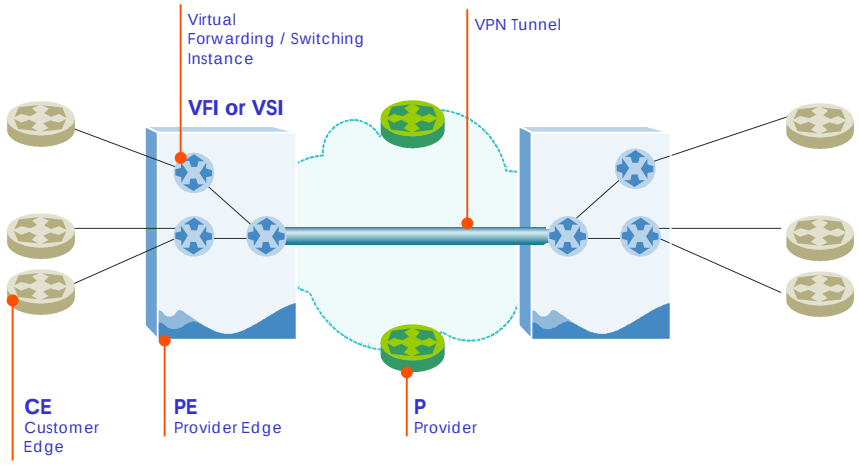
IETF の活動の歴史

- Network-based VPN (NBVPN)
  - August 3, 2000 – 48th IETF @ Pittsburgh - NBVPN BOF
- Provider Provisioned VPN (PPVPN)
  - December 14, 2000 – 49th IETF @ San Diego - PPVPN BOF
- Pseudo Wire Edge to Edge Emulation (PWE3)
  - March 18-25, 2001 – 50th IETF @ Minneapolis – PWE3 BOF
- L3VPN, L2VPN
  - Nov 12, 2003 – 58th IETF @ Minneapolis

Provider Provisioned VPN の分類



トポロジーと用語 (L2 and L3)



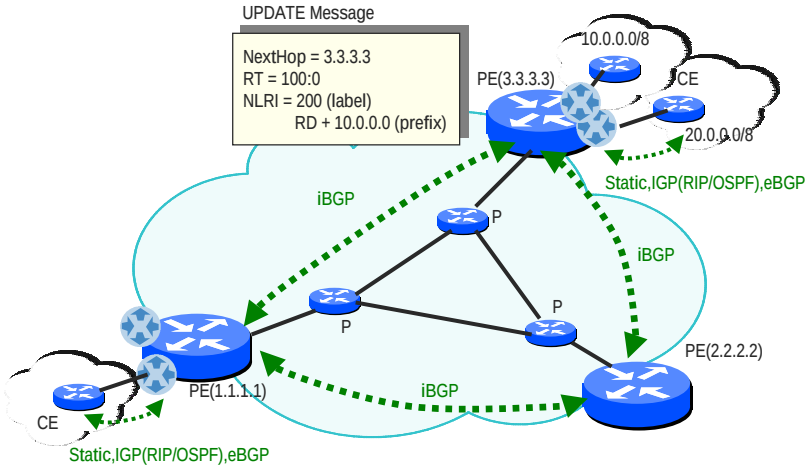
各種VPNに共通する概念

- トンネル方式
  - トンネル
  - (多重化された) セッション
  - Encapsulation
- シグナリング方式
- 何を運ぶか
  - IP (L3) or Frame (L2)
- 何で運ぶか
  - IP, TCP, UDP, MPLS, etc.

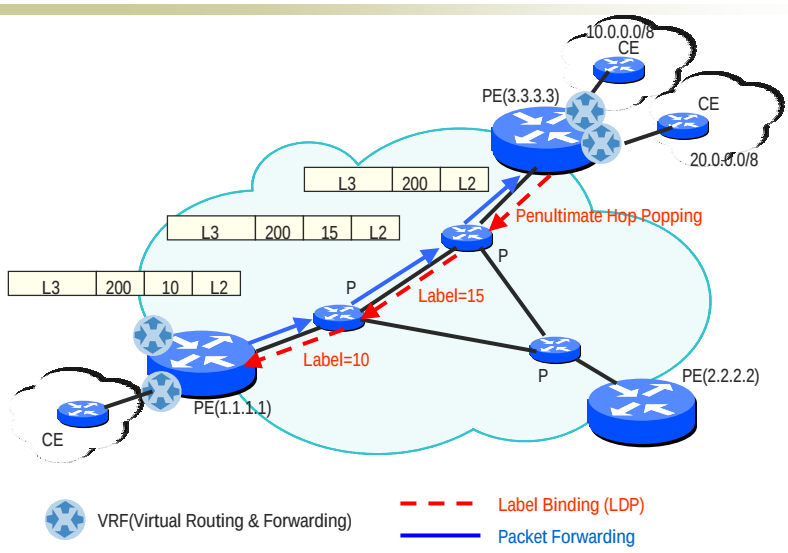
BGP/MPLS VPN

- 通称「2547」
  - 日本で“IP-VPN”というと、通常これを指すことが多い
  - RFC 4364 としてアップデート (Proposed Standard)
- 一言で言うと、
  - BGPを “巧み” に使った VPN 方式
    - マルチプロトコルBGP
    - Extended Community によるトポロジー
  - MPLS はおまけ！？
  - どうしても解決できないところは力技 ☺
    - VRF

BGP/MPLS VPN の動き (1)

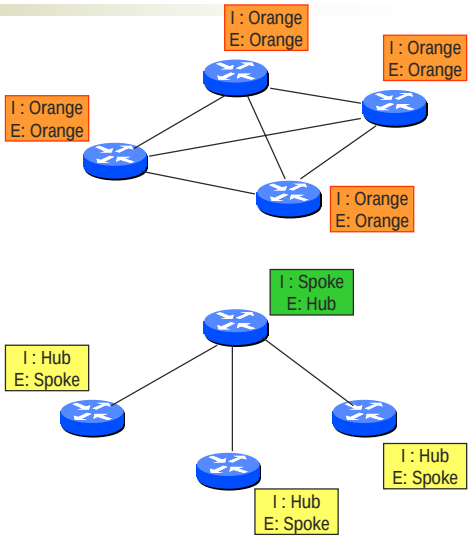


BGP/MPLS VPN の動き (2)



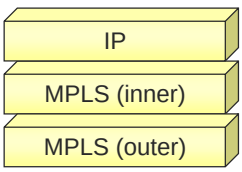
Topology Control in BGP/MPLS VPN

- Route Target（RT）
- Full Mesh
  - **すべての** PE **で**
    - Import : “Orange”
    - Export : “Orange”
- Hub & Spoke
  - Hub **となる** PE **で**
    - Import : “Spoke”
    - Export : “Hub”
  - Spoke **となる** PE **で**
    - Import : “Hub”
    - Export : “Spoke”



Quick Review (BGP/MPLS VPN)

- **シグナリング**
  - BGP
- **何を運ぶか**
  - IP
- **何で運ぶか**
  - MPLS



BGP/MPLS VPNの利点・欠点（顧客にとって）

- 利点
  - 非常に透過的（おまかせモデル）
    - NAT / Firewall などの心配をしないで済む
    - セキュリティーはプロバイダを信頼
  - 安い？？
- 欠点
  - ルーティングの自由度に欠ける
  - IP Only
  - リモートアクセス向きでない

BGP/MPLS VPNの利点・欠点（SPにとって）

- 利点
  - 新たな収益源！
- 欠点
  - 顧客のルーティングに関与しなければならない
  - 結構おおがかり

Layer 2 Network-based VPN

- **キャリア・ISP は** Layer 3 **に関与するのは止めよう！**
- **ユーザのルーティングには関与しない**
- Overlay **モデル**
  - **ピアモデル信奉者、さようなら！**

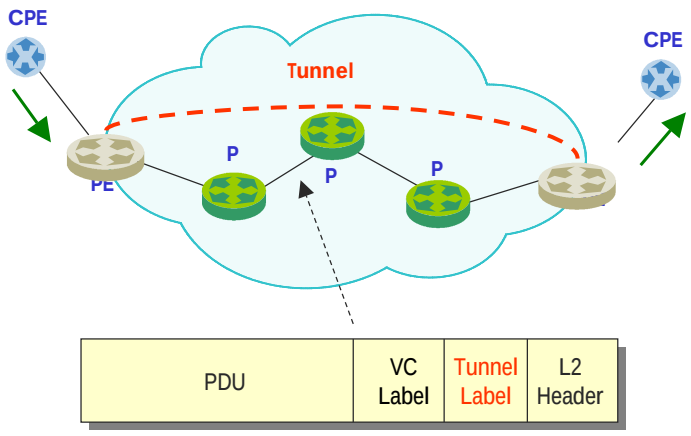
Layer 2 VPN

- Virtual Private Wire Service (VPWS)
  - Martini **方式**
  - Kompella **方式**
- Virtual Private LAN Service (VPLS)
  - Lasserre-V.Kompella **方式**
  - Kompella **方式**
- IP over LAN Service (IPLS) / ARP mediation
  - Shah **方式**

Martini (transport) 方式

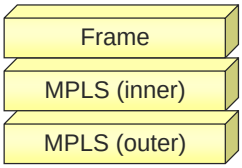
- VPWS の一方式
  - draft-martini-l2circuit-trans-mpls-20.txt
- MPLS ベース
- シグナリングは LDP
  - VC Label を配布するための方法を規定

Tunnel Label vs VC Label



Quick Review (Martini Transport)

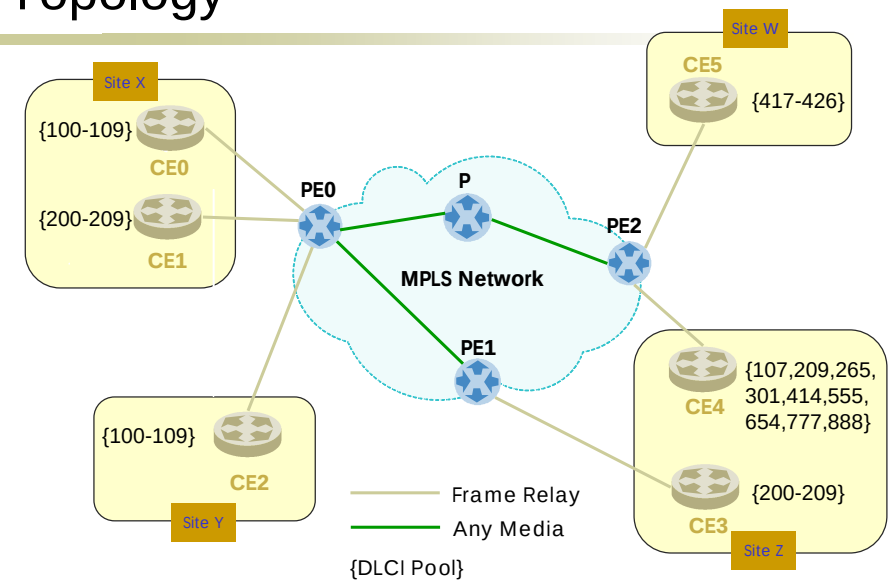
- **シグナリング**
  - LDP
- **(何を運ぶか)**
  - Any
- **(何で運ぶか)**
  - MPLS



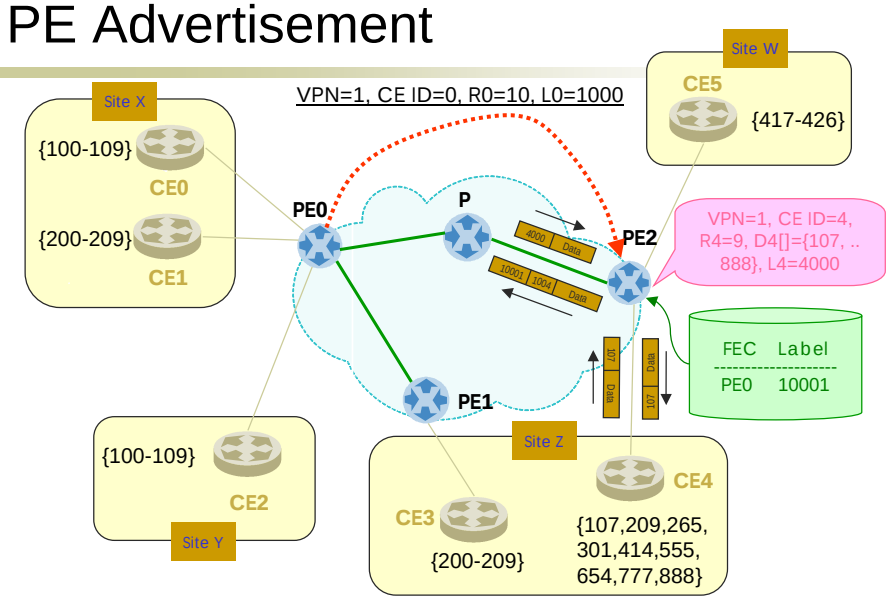
Kompella**方式**

- VPWS **の一方式**
  - draft-kompella-l2vpn-l2vpn-01.txt（**復活！**）
- MPLS **ベース**
- Signaling **は** BGP
- N^2 **問題の軽減**
  - Over Provisioning **で**Provisioning**の負荷を軽減**（**半自動** Provisioning）
  - Layer 2 ID (DLCI, VPI/VCI) **および** Label **は** cheap **である、という前提**

Topology

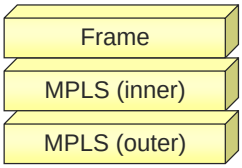


PE Advertisement



Quick Review (Kompella)

- **シグナリング**
  - BGP
- **何を運ぶか**
  - Any
- **何で運ぶか**
  - MPLS



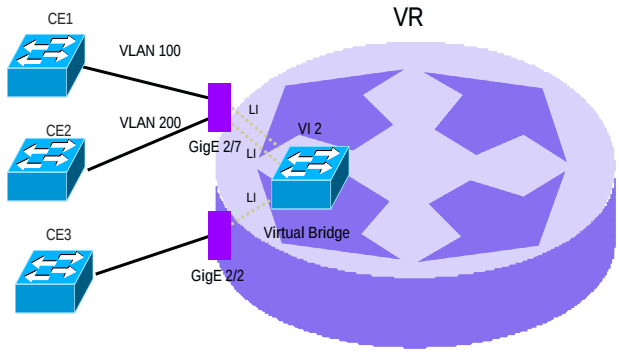
Martini vs Kompella

- Martini
  - Point to Point **のサーキットを作る**
  - **シグナリングは**LDP
- Kompella
  - **フルメッシュな** VPN **を作る**
  - **シグナリングは**BGP

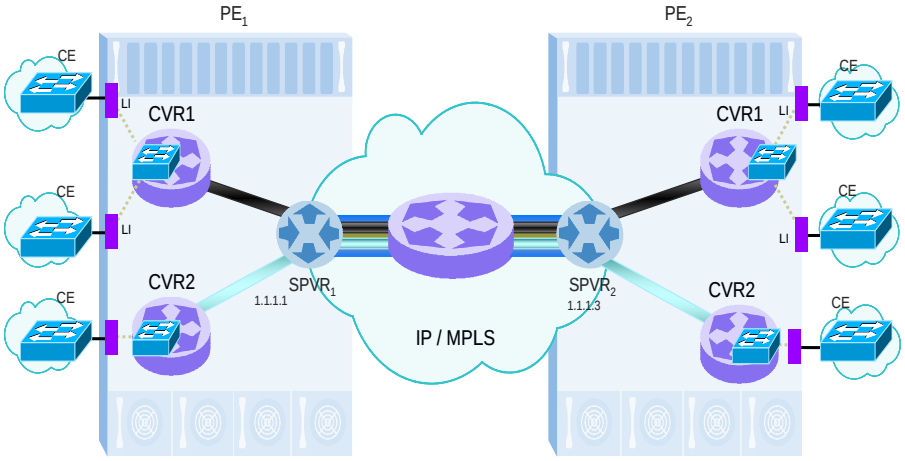
Lasserre-V.Kompella方式

- VPLS の一方式
  - draft-ietf-l2vpn-vpls-ldp-08.txt
- MPLS ベース
- Signaling は LDP
  - Martini Signaling の拡張
- Virtual Bridging (802.1D) による実現

Virtual Bridge: Local Bridging

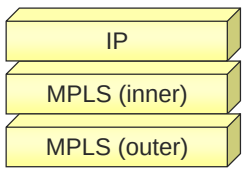


TLS - VLAN + PWE Bridging



Quick Review (Lasserre-V.Kompella)

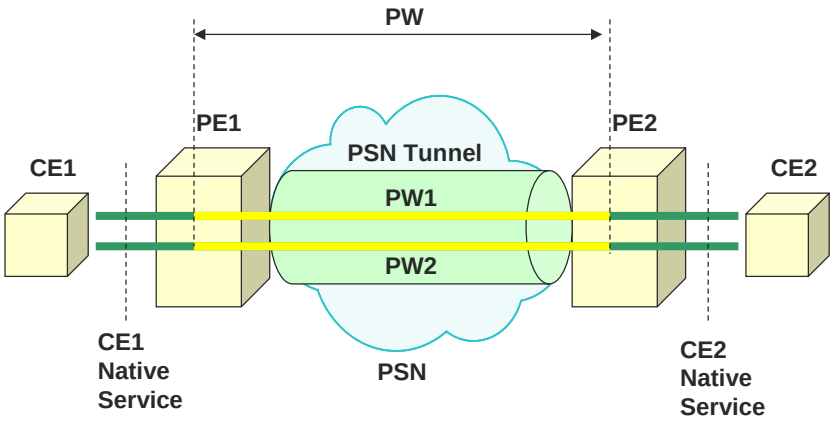
- **シグナリング**
  - LDP (Martiniの拡張)
- **何を運ぶか**
  - Any
- **何で運ぶか**
  - MPLS



別に MPLS じゃなくても・・・

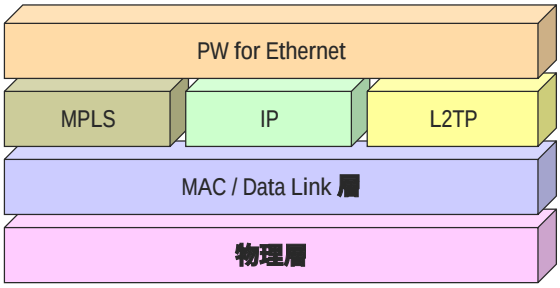
- 要は PE 間を結ぶ「線（Wire）」があればよい！
  - 汎用的（VPN用途に限らず）に
  - エンド～エンド間で
  - パケット・スイッチ・ネットワーク上に（Overlayで）
  - 仮想・擬似的な “Wire” を作ってやる技術
- Pseudo Wire Emulation Edge to Edge (PWE3)
- RFC 3916（Requirement) & 3985 (Architecture)

PWE3の基本的アーキテクチャ



例) PWE3 for Ethernet

- Martini Encapsulation
  - RFC 4448 (over MPLS)
- L2TPv3
  - draft-ietf-l2tpext-pwe3-ethernet-09.txt (over L2TPv3)



その他のPW Type

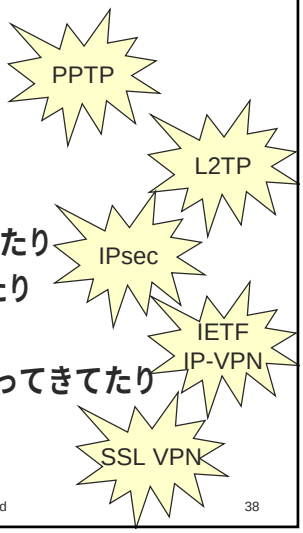
- SONET / SDH
  - draft-ietf-pwe3-sonet-13.txt
- ATM (cell & frame)
  - draft-ietf-pwe3-atm-encap-11.txt
  - RFC 4454 (over L2TPv3)
- Frame Relay
  - RFC 4619 (over MPLS)
  - RFC 4591 (over L2TPv3)
- HDLC / PPP
  - RFC 4618 (over MPLS)
  - RFC 4349 (over L2TPv3)
- IP
  - draft-ietf-l2tpext-pwe3-ip-03.txt

歴史は繰り返す！？

- キャリアの VC サービス (FR, ATM)
- CE ベースの VPN
  - PPTP
  - IPsec
- PE ベースの VPN
  - L3 IP-VPN
  - L2 IP-VPN
- CE ベースへの回帰？？
  - SSL-VPN
  - L2 な VPN

既存の VPN の問題点

- いままでのVPNは、
  - NATしづらかったり
  - DoSアタックに弱かったり
  - 認証があまりちゃんとしていなかったり
  - 暗号化もいまいちだったり
  - ちゃんと暗号化しようとすると大変だったり
  - リモートアクセスには向いていなかったり
  - 非常に大げさだったり
  - シンプルだったはずが、そうでもなくなってきてたり
  - ・・・



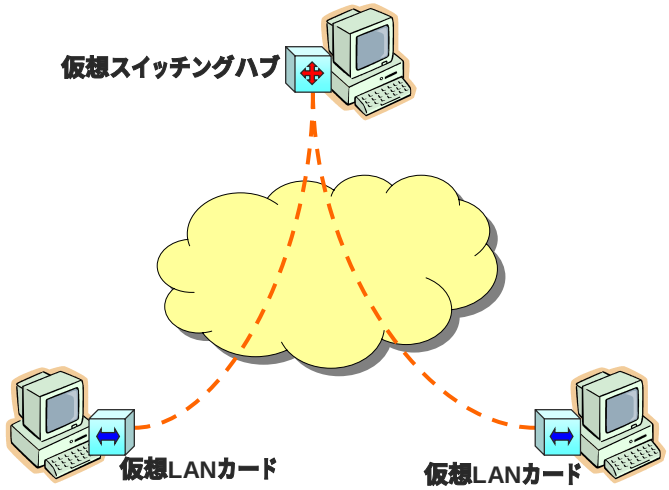
PacketiX VPN とは

- 旧称「SoftEther」
- 仮想的に (Ethernet) スイッチングハブと (Ethernet) 仮想 LAN カードを模擬
- それらを結ぶことにより Overlay ネットワーク (VPN) を形成することができる
- http://www.softether.com

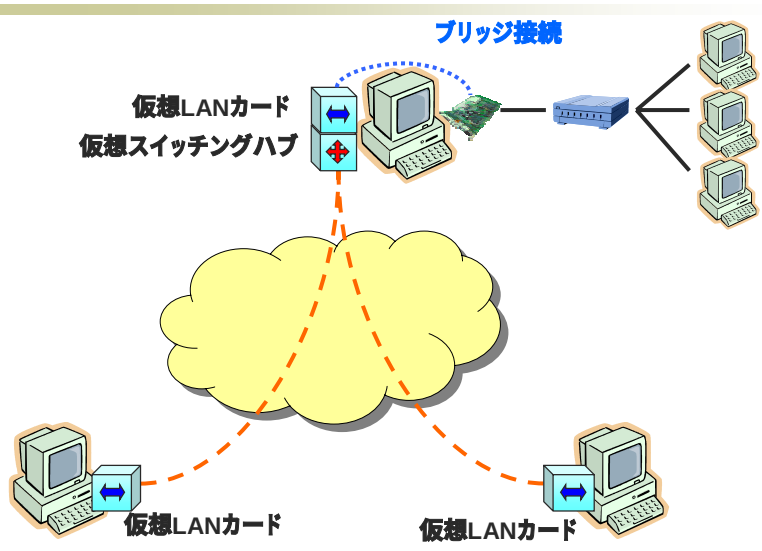
なぜ PacketiX が注目されるのか？

- (はからずも) 非常に"うまい"デビューを果たした！？
- 当初はお手軽さがウケた
  - 現在はかなり feature rich
- 純国産だけに応援したい
- …

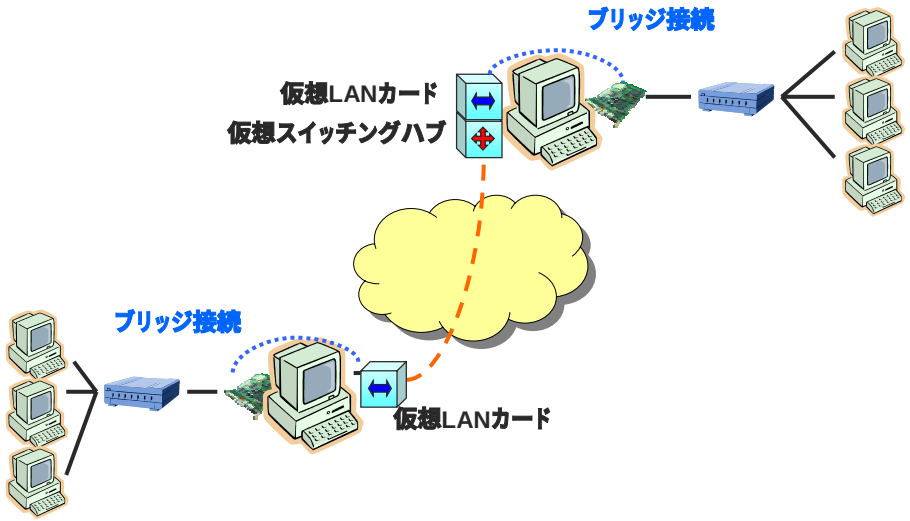
トポロジー (PC to PC)



トポロジー (PC to LAN)



トポロジー (LAN to LAN)



SoftEther から PacketiX に至るまで

- SoftEther 1.0
  - フリー版として公開
- SoftEther CA
  - SoftEther 1.0 をベースに機能を拡張
    - 電子証明書のサポート、認証デバイスのサポート、GUIベースのマネージャ、etc.
- SoftEther VPN 2.0
  - コンセプトは SoftEther 1.0 から踏襲しているが、コードは完全に書き直している
  - フリー版と製品版
- PacketiX VPN 2.0 と改名

PacketiX VPN 2.0 の強化点

- 性能の向上
- 認証サーバー（RADIUS / NTドメイン・Active Directory）との連携
- 電子証明書のサポート
- 複数の仮想Hubのサポート
- スケーラビリティーの向上
  - 4096ユーザ同時接続/サーバー
  - サーバーファーム対応
- その他多数

PacketiXをIETF的に見ると・・

- VPLS（Virtual Private LAN Service）
  - PEベースでない（i.e. CEベース）
  - Provider Provisioned ではない（Voluntary）
- Ethernet Pseudo Wire Emulation

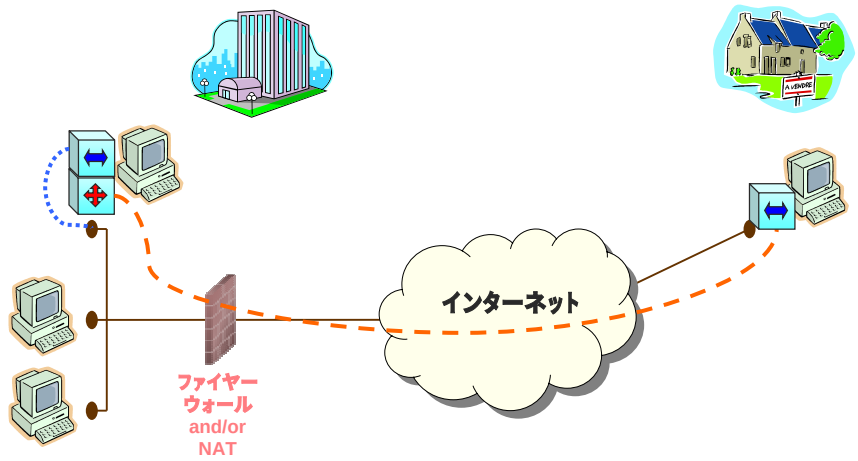
PacketiX VPN の特徴

- さまざまな接続方法に対応
  - 直接、HTTP Proxy、SSH、SOCKS
  - NAT、Firewall、Proxy などを越えられる！
- SSLによる暗号化
- 非常に簡単！
  - 繋ぎ易さゆえの弊害？

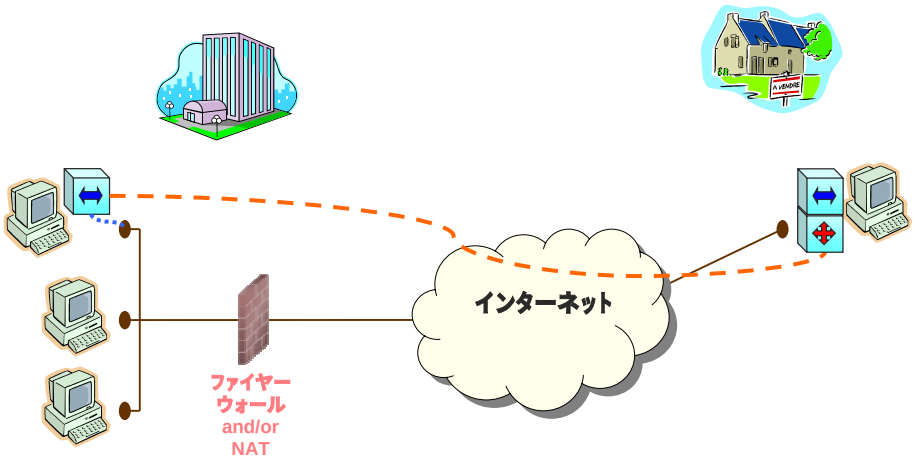
使い方いろいろ

- 社内LANへのリモートアクセス
- 社内でVLAN的な使い方
- 自宅のLANにリモートアクセス
  - ネットワーク機器のメンテナンス
  - 映像や音楽を楽しむ
- リモートアシスタンス
- ホットスポットからの利用
- オンラインゲーム
- MAPIを通す
- …

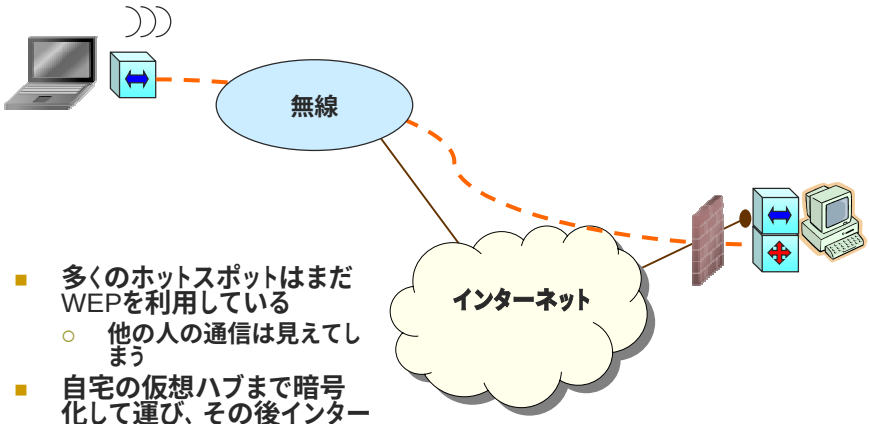
社内LANへのアクセス(1)



社内LANへのアクセス(2)



ホットスポットでの利用



- 多くのホットスポットはまだWEPを利用している
  - 他の人の通信は見えてしまう
- 自宅の仮想ハブまで暗号化して運び、その後インターネットに抜けるようにする

新しい使われ方

- ASPサービスの開始
- アプライアンスの登場
- VoIPへの適用

TCP over TCP is considered harmful?

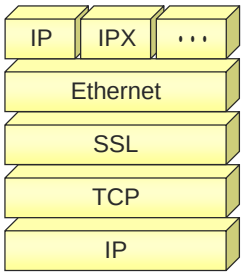
- 歴史的にはTCP over TCPはダメダメと考えられてきた
  - TCPの再送はAdaptiveである
  - 多層されたTCPの再送は独立して動く
  - もし、上位のTCPが下位のTCPよりも早く再送したら・・・
  - CIPEでの経験
    - http://sites.inka.de/sites/bigred/devel/tcp-tcp.html
- でも、工夫をするとそれほど悪くはなくなるらしい！

PacketiX を発見できるか？

- ネットワーク管理者にとっては脅威となる場合がある
- シグネチャー
  - Keep Aliveのためのping
  - 長寿命なTCPセッション
  - “SE-VPN2-PROTOCOL” (for 2.0)
  - SoftEther Alert / SoftEther Block (for 1.0)
- 専用のアプライアンス

Quick Review (PacketiX VPN)

- **シグナリング**
  - **独自 (非公開)**
- **何を運ぶか**
  - Ethernet Frame
- **何で運ぶか**
  - SSL



SoftEther/PacketiX is not alone ☺

- **他にも似たようなアイデアをもったものがある**
  - VTun
  - OpenVPN
  - …
- **フレキシビリティー**
  - TCP or UDP
  - Ethernet, PPP, IP, etc.
  - **複雑さ**

その他のVPN実装/製品/サービス

- CIPE
  - http://sites.inka.de/sites/bigred/devel/cipe.html
- TinyVPN
  - http://www.shimousa.com/tv/
- tinc
  - http://www.tinc-vpn.org/
- Emotion Link
  - http://www.freebit.com/solution/emotion.html
- HTTP Tunnel
  - http://www.http-tunnel.com
- **他にもまだたくさん**

まとめ

- VPNはさまざま
- **ただ、さまざまなように見えても、実は根っこは一緒！**
- “All Mighty” **はありえない**
- **次に回帰するとしたらどこ！？**
- **これからも、ワクワクするようなVPN技術が出てきて欲しい**

略語一覧

AC	Access Concentrator
ATM	Asynchronous Transfer Mode
AVP	Attribute Value Pair
BGP	Border Gateway Protocol
BoF	Birds of Feather
CDN	Call-Disconnect-Notify (L2TP)
CE	Customer Edge
CIPE	Crypto IP Encapsulation
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
eBGP	External Border Gateway Protocol
GRE	Generic Routing Encapsulation
iBGP	Internal Border Gateway Protocol
ICCN	Incoming-Call-Connected (L2TP)
ICRP	Incoming-Call-Reply (L2TP)
ICRQ	Incoming-Call-Request (L2TP)
IP	Internet Protocol
IPLS	IP LAN-like Service
IPsec	IP Security
ISP	Internet Service Provider
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LDP	Label Distribution Protocol
LNS	L2TP Network Server
MAPI	Messaging Application Programming Interface
MPLS	Multi Protocol Label Switching
NAT	Network Address Translation
NLRI	Network Layer Reachability Information
OSPF	Open Shortest Path First
P	Provider (Router)
P2MP	Point-to-Multipoint
P2P	Point-to-Point
PAC	PPTP Access Concentrator
PE	Provider Edge
PNS	PPTP Network Server
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PPVPN	Provider-Provisioned Virtual Private Network
RADIUS	Remote Access Dial In User Service
RD	Route Distinguisher
RDP	Remote Desktop Protocol
RIP	Routing Information Protocol
RT	Route Target
SCCCN	Start-Control-Connection-Connected (L2TP)
SCCRP	Start-Control-Connection-Reply (L2TP)
SCCRQ	Start-Control-Connection-Request (L2TP)
SSL	Secure Socket Layer
StopCCN	Stop-Control-Connection (L2TP)
TCP	Transport Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
VR	Virtual Router
VRF	Virtual Routing and Forwarding
WEP	Wired Equivalent Privacy