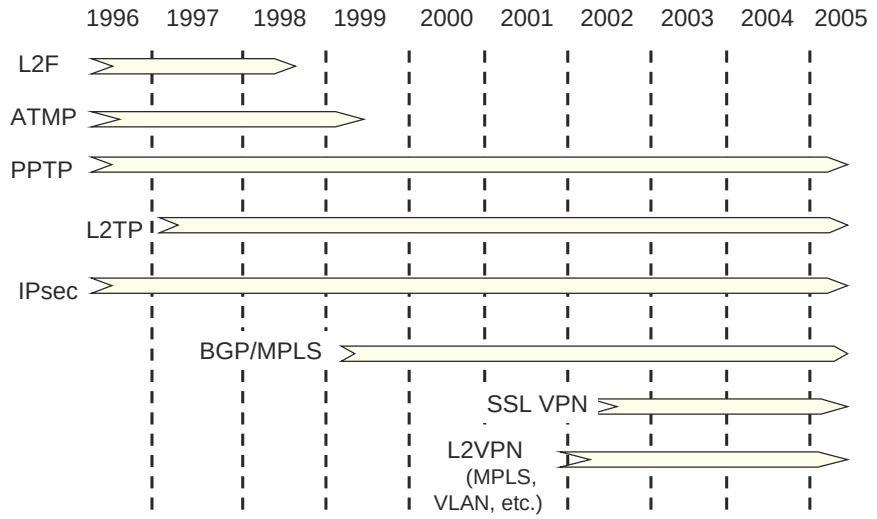
T22 : VPN 再考

～ IP-VPN vs SoftEther 他 ～

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

VPN年表



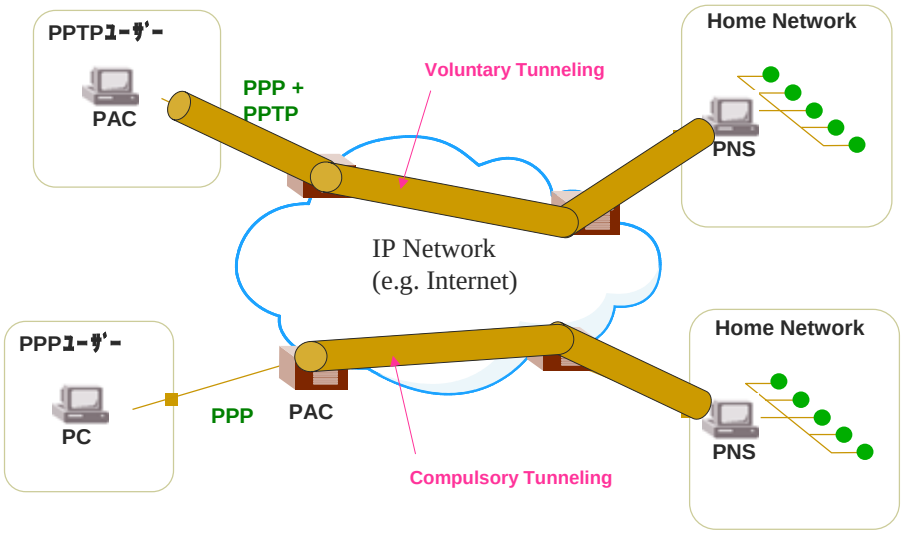
各種VPNに共通する概念

- トンネル方式
  - トンネル
  - セッション
  - Encapsulation
- シグナリング方式
- 何を運ぶか
  - IP, PPP, Ethernet, etc.
- 何で運ぶか
  - IP, TCP, UDP, MPLS, etc.

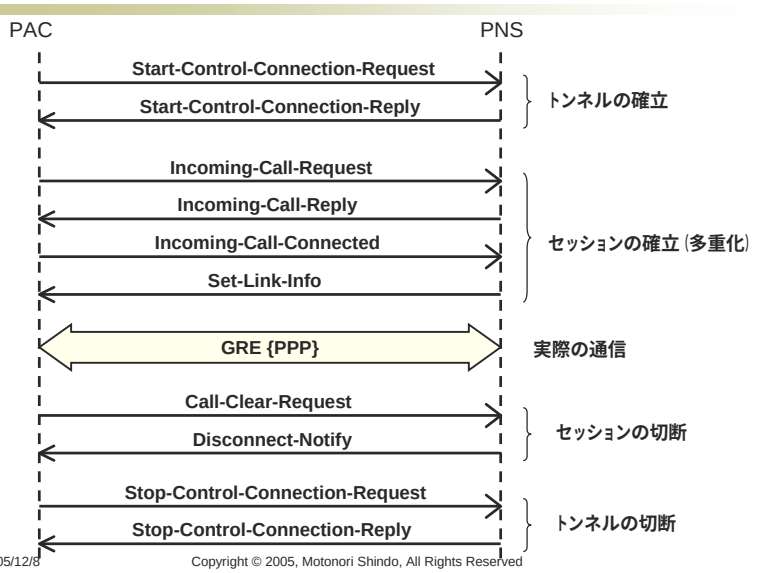
PPTP

- Point to Point Tunneling Protocol
- RFC 2637 (Informational)
  - Microsoft
  - 3Com
  - Ascend (Lucent)
- 幅広いサポートプラットフォーム
  - Windows 系
  - MacOS X
  - ブロードバンドルーター
  - …

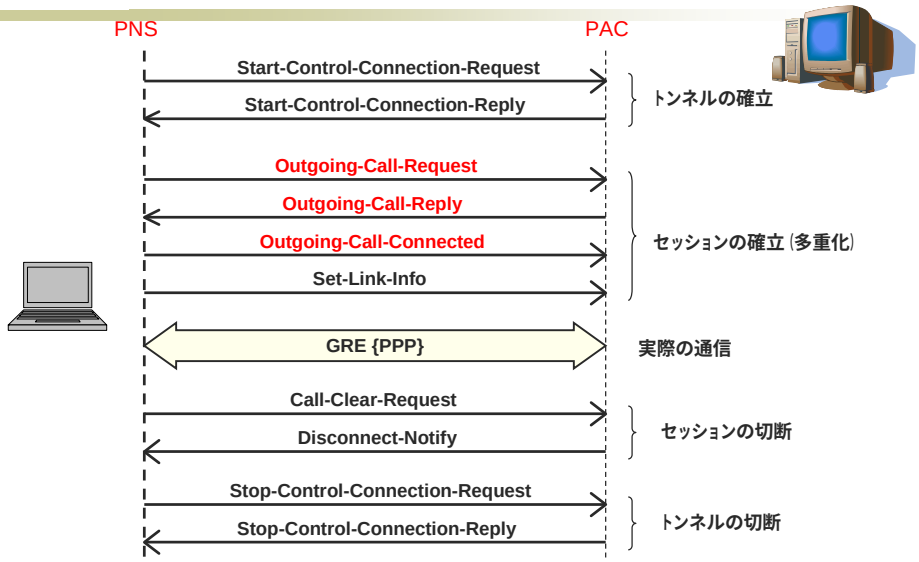
PPTPによるVPN



PPTPの動き

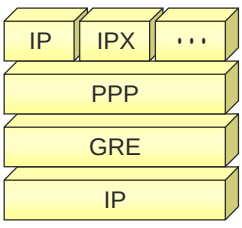


MicrosoftのPPTPの動き



Quick Review (PPTP)

- シグナリング
  - TCP
  - ダイアルアップの延長
- 何を運ぶか
  - PPP
- 何で運ぶか
  - GRE



PPTPの利点・欠点

- 利点
  - 幅広いサポート
    - Windows
    - Mac OS X
    - UNIX
    - ブロードバンド・ルーター
  - 暗号化（ただし、プロトコルの規定外）
  - 既存のPPPのためのインフラ（e.g. RADIUS)を利用できる
    - 認証
    - 課金
- 欠点
  - NATとの相性が悪い
  - トンネルに対する認証がない（→ DoS攻撃）
  - 暗号化に若干の脆弱性（プロトコルの脆弱性ではなく、実装の脆弱性）

なぜPPTPはNATしづらいか？

- PPPをGRE (Generic Routing Encapsulation; Protocol = 47)でつつむ
  - TCPでもUDPでもない
  - “ポート番号”がない
- でも、がんばるとNATできる！
  - パススルー（1対1）
  - 1対多

PPTPで使われているGREヘッダ

C	R	K	S	s	Recur	A	Flags	Ver	Protocol Type
Key (HW) Payload Length									Key (LW) Call ID
Sequence Number (Optional)									
Acknowledgement Number (Optional)									

C: Checksum Field があることを示す。PPTP の場合には必ず0。
R: Routing Field があることを示す。PPTP の場合には必ず0。
K: Key Field があることを示す。PPTP の場合には必ず1。
S: Sequence Number Field があることを示す。データパケットの場合には1、Acknowledgment のみの場合は0。
s: Strict source route Field があることを示す。PPTP の場合には必ず0。
Recur: encapsulation が何段多重に行われているかを示す。PPTP の場合には必ず0。
A: Acknowledgment Number Field があることを示す。
Flags: フラグ。PPTP の場合には必ず0。
Ver: バージョン番号。PPTP の場合には必ず1。
Protocol Type: プロトコル番号。PPTP の場合には必ず 0x880B。
Key (HW) Payload Length: Key Field の上位16bit。PPTP はこれをPayload の長さを格納するのに使う。
Key (LW) Call ID: Key Field の下位16bit。PPTP はここを Call IDを格納するのに使う。
Sequence Number: シーケンス番号
Acknowledgment Number: 肯定応答番号

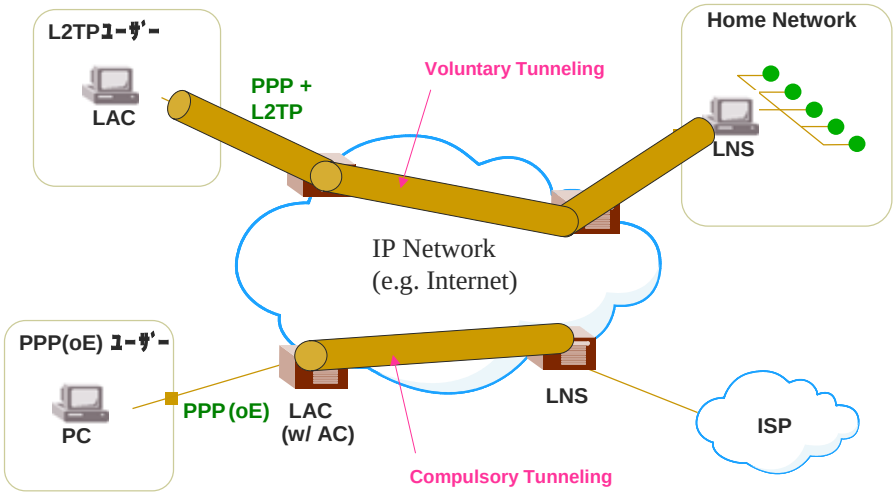
L2TP

- Layer 2 Tunneling Protocol
- RFC 2661 (Standard Track)
  - Cisco
  - Ascend (Lucent)
  - Microsoft
  - Redback
- L2F + PPTP
  - **メッセージフォーマット、LCP関連機能** ← L2F
  - **発呼の概念、フローコントロール** ← PPTP
- Windows 2000 **以降の** Windows **に搭載**

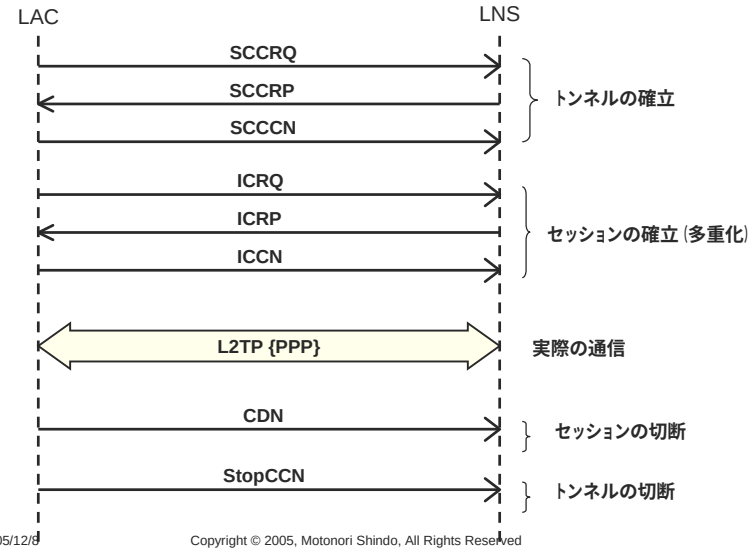
L2TPの特徴

- PPPベース
  - 豊富なPPPのインフラストラクチャを活かせる
- 下位レイヤー独立
  - UDP (最も一般的)
  - Frame Relay
  - ATM
  - IP
- 拡張性の高いメッセージフォーマット(AVP)
- トンネル認証のサポート
- 一部のAVPの暗号化をサポート
  - データ自体の暗号化はされない

L2TPによるVPN



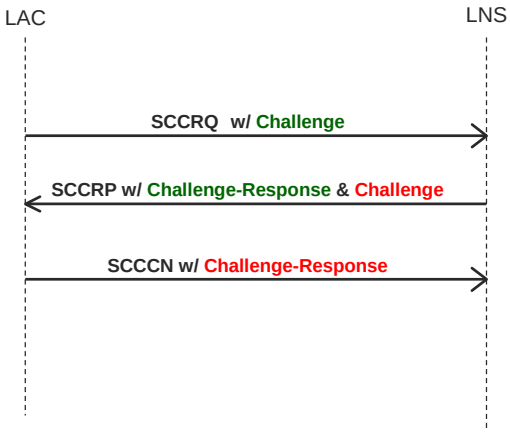
L2TPの動き



トンネル認証

- LAC / LNS がパスワードを共有しているのが前提（Shared Secret）
- チャレンジ・レスポンス型認証
  - 認証したい側が相手に対してチャレンジを送る
  - チャレンジとShared Secretのハッシュを相手に送り返す
- 相互認証可能

トンネル認証の動き

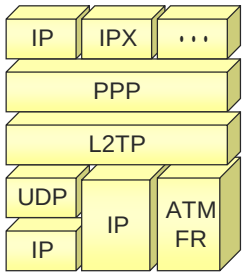


L2TPの適用箇所

- Voluntary TunnelとしてはPPTPのほうがより多く使われている
- Compulsory TunnelとしてはL2TPのほうが多く使われている（はず）

Quick Review (L2TP)

- シグナリング
  - 何の上にでも乗る
    - 信頼性はL2TP自身で確保
  - ダイアルアップの延長
- 何を運ぶか
  - PPP
- 何で運ぶか
  - UDP, etc.



L2TPの利点・欠点

- 利点
  - 優れた相互運用性
  - 拡張性
  - NAT friendly
  - PPPの既存のインフラを流用可能
  - 下位レイヤ独立
- 欠点
  - ユーザーが使うにはちょっと面倒
    - IPsecにたよる場合
  - 下位レイヤ独立

L2TPの今後

- L2TPv3
  - RFC 3931
    - PPPからの脱却
      - IPネットワーク用の汎用Pseudo Wireのシグナリング・プロトコルとして生まれ変わった
    - （プロトコルとしての）スケーラビリティーの向上
      - Session ID, Tunnel ID の32ビット化
    - トンネル認証をすべてのコントロールメッセージに対して適用
  - draft-ietf-l2tpext-l2tp-ppp-02.txt

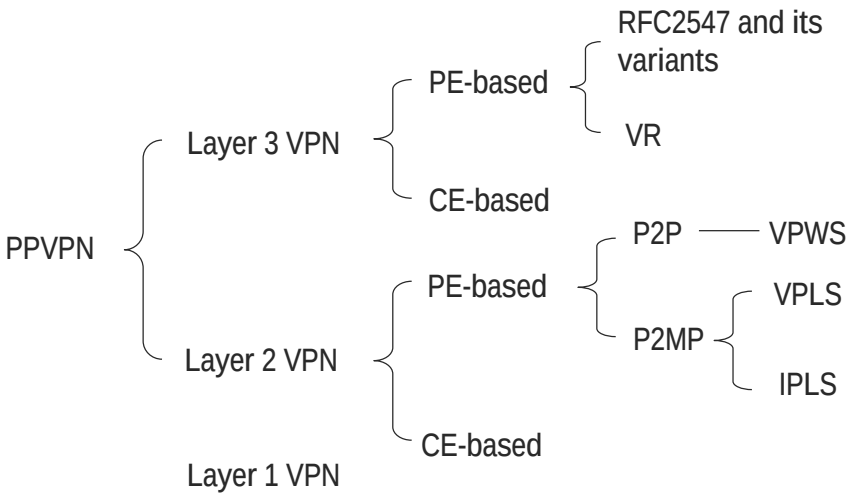
IP-VPN

- 非常に曖昧
  - IPを使ったVPN？？
  - IPだけのためのVPN？？
  - インターネットを使ったVPN？？
- 一般的には
  - 通信事業者の持つ
  - IPネットワーク
    - プライベートネットワークのことが多かったりする
  - で構築されているVPNのこと
- IP-VPN　BGP/MPLS VPN (a.k.a RFC2547) ??

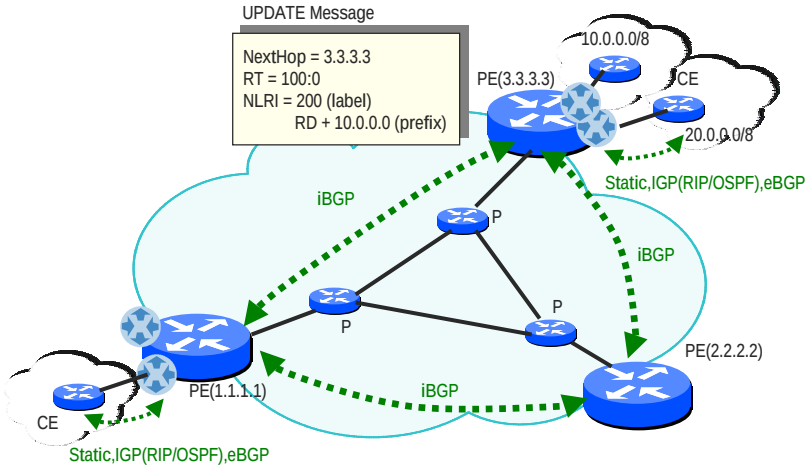
IETF の動き

- 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

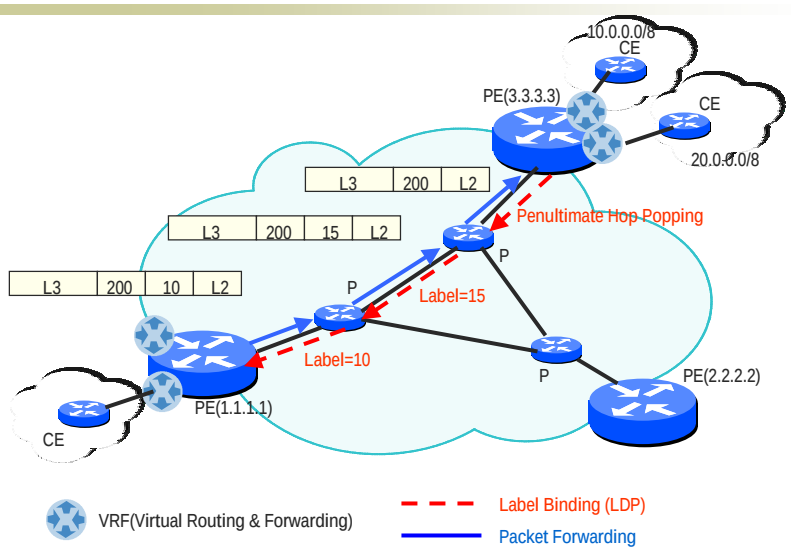
IETF PPVPN分類



BGP/MPLS VPN (RFC2457) の動き (1)

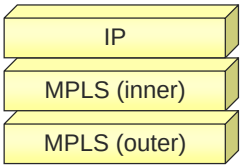


BGP/MPLS VPN (RFC2457) の動き (2)



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

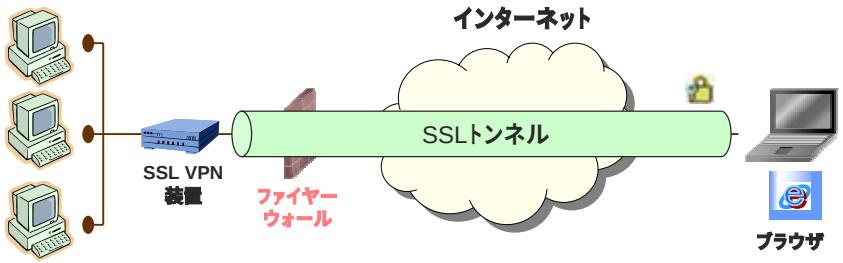
SSL VPN

- 主にIPsecへのアンチテーゼ（かな？）
- 背景
  - リモートアクセスしたい
  - もちろんきちんとしたセキュリティーは必要
  - IPsecは複雑すぎ（特にリモートアクセス時）
- ブラウザに組み込まれているSSLを使おう！

各種SSL VPN方式

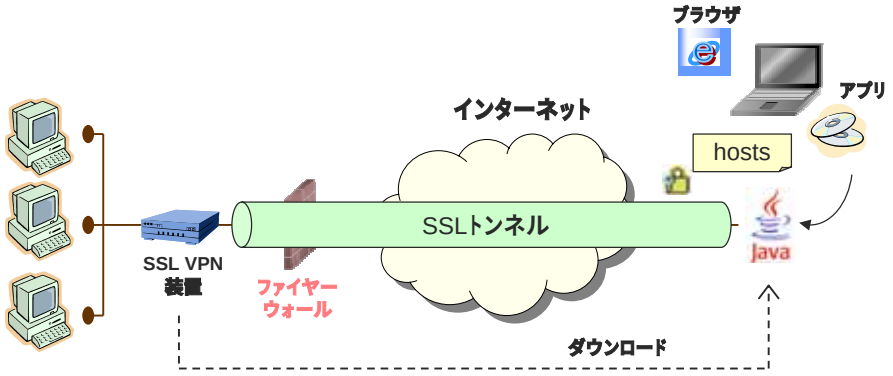
- リバース･プロキシー
- Java Applet (ポートフォワード)
- ActiveX (L2カプセル)
- その他
  - SOCKS
  - RDP

リバース･プロキシー方式



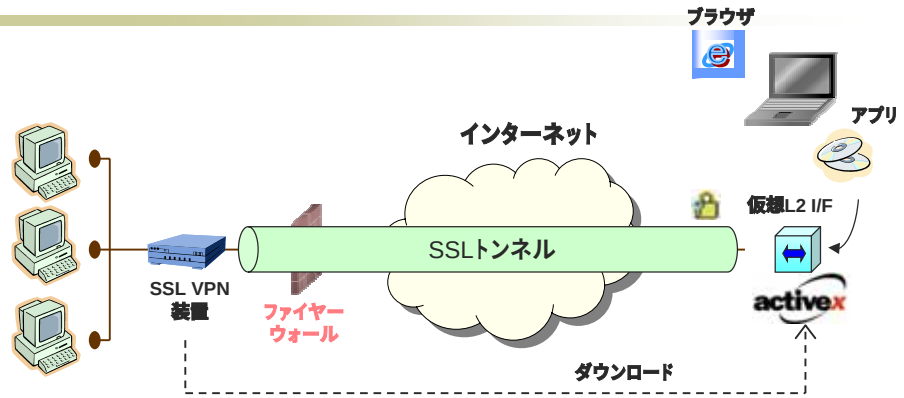
- クライアントレス
- 対応アプリケーションはWebベースのものに限られる

Java Applet方式



- Javaアップレットがダウンロードされる
- Hostsファイルを書き換え、アプリケーションのトラフィックがlocalhostに向かうようにする
- Web以外のアプリケーションも利用可能だが、固定ポートのアプリケーションに限られる

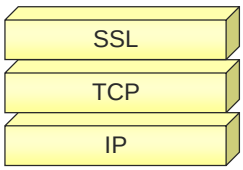
ActiveX方式



- ActiveX コントロールがダウンロードされる
- 仮想L2インターフェースが作成され、トラフィックはこのインターフェースを通じてやりとりされる
- ほぼ全てのアプリケーションを利用することが可能

Quick Review (SSL VPN)

- **シグナリング**
  - HTTP (と言っていいものかどうか・・・)
- **何を運ぶか**
  - TCP session
  - UDP session
  - Any frame
- **何で運ぶか**
  - SSL



SSL VPNの利点・欠点

- **利点**
  - 安全なリモートアクセス
  - ファイヤーウォールの越えやすさ
  - アクセスコントロール
- **欠点**
  - 利便性 vs 複雑性のジレンマ

さて、・・・

- 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
  - ・・・

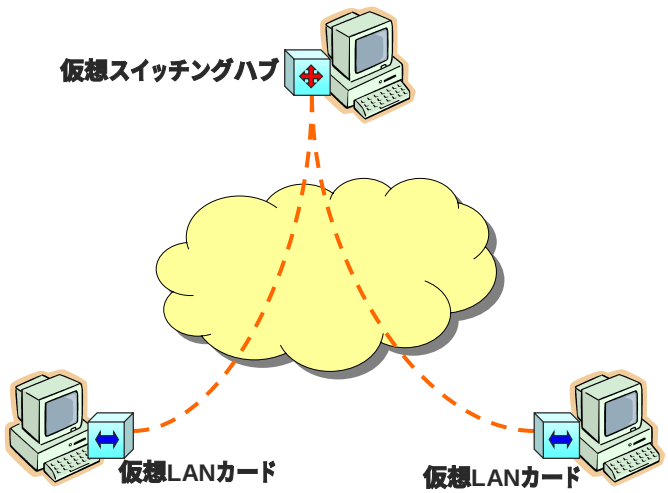
SoftEther とは

- 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 ネットワークを形成することができる
- http://www.softether.com

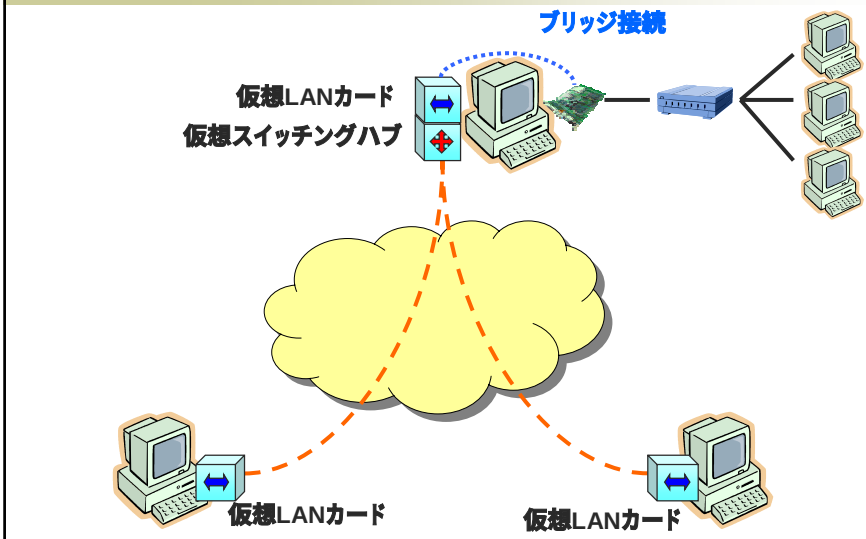
なぜ今SoftEtherが注目されるのか？

- (はからずも) 非常に"うまい"デビューを果たした！？
- お手軽さがウケている
- が、なかなかよくできている
- 純国産だけに応援したい
- …

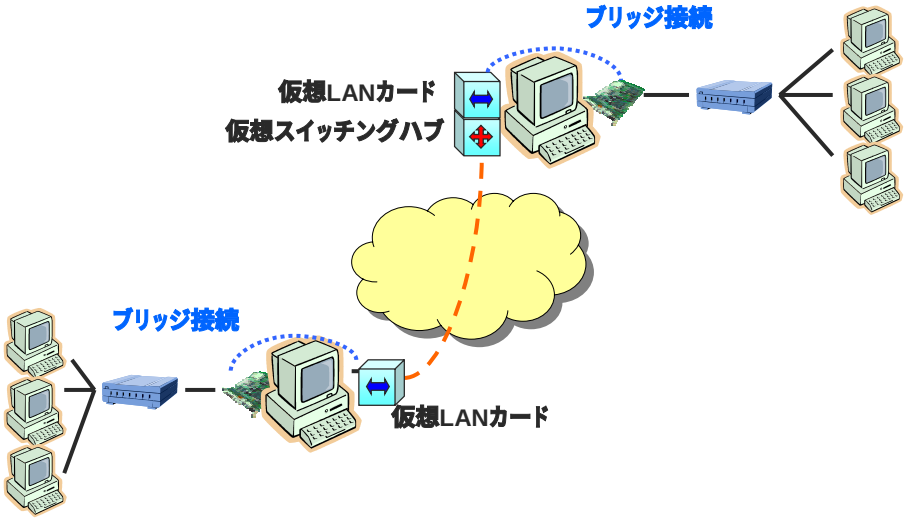
SoftEther トポロジー (PC to PC)



SoftEther トポロジー (PC to LAN)



SoftEther トポロジー (LAN to LAN)



SoftEther いろいろ

- 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

SoftEther 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

SoftEtherをIETF的に見ると・・

- VPLS（Virtual Private LAN Service）
  - ただし、Provider Provisioned (Compulsory)ではなく、Voluntary
  - PEという概念がない（i.e. CEベース）
- Ethernet Pseudo Wire Emulation

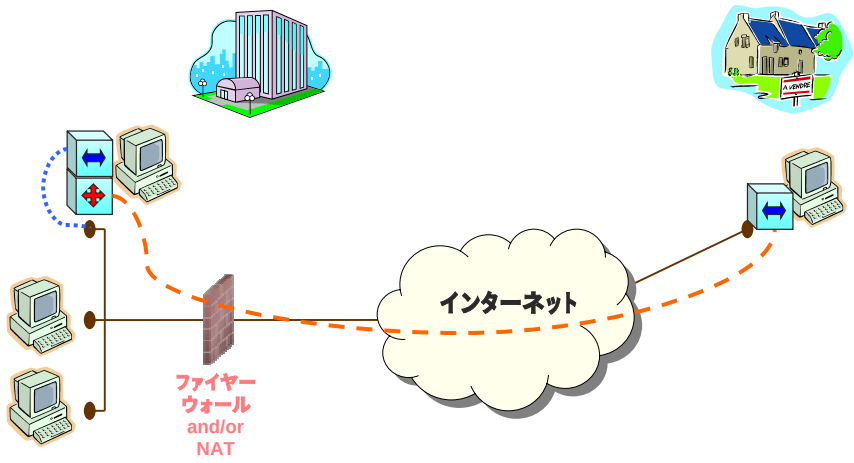
SoftEther の特徴

- 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？

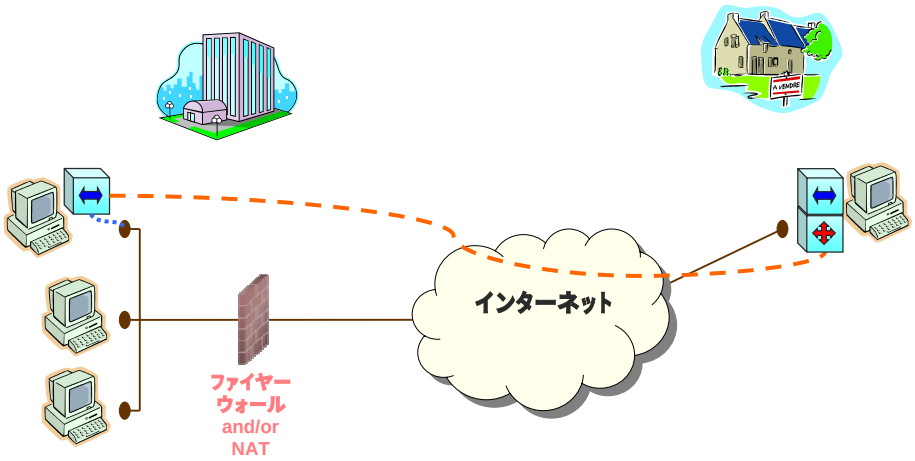
使い方いろいろ

- 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
- …

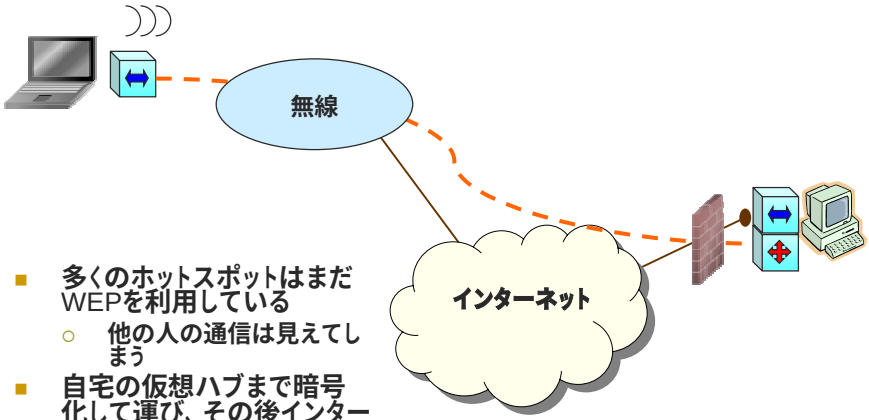
社内LANへのアクセス(1)



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

TCP over TCP is considered harmful?

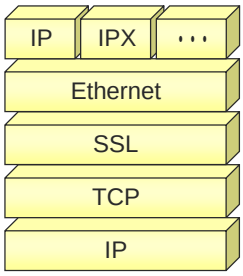
- 歴史的にはTCP over TCPはダメダメと考えられてきた
  - TCPの再送はAdaptiveである
  - 多層されたTCPの再送は独立して動く
  - もし、上位のTCPが下位のTCPよりも早く再送したら・・・
  - CIPEでの経験
    - http://sites.inka.de/sites/bigred/devel/tcp-tcp.html
- でも、工夫をするとそれほど悪くはなくなるらしい！

SoftEther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
- SoftEtherのSignature
  - 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 (SoftEther)

- **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の利点・欠点

- **利点**
  - **お手軽！**
  - **接続方法の多様性**
  - **リモートアクセス的にもVPWS的にもVPLS的にも使用することができる**
  - **無料☺**
- **欠点**
  - **お手軽！**

SoftEther 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
- 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