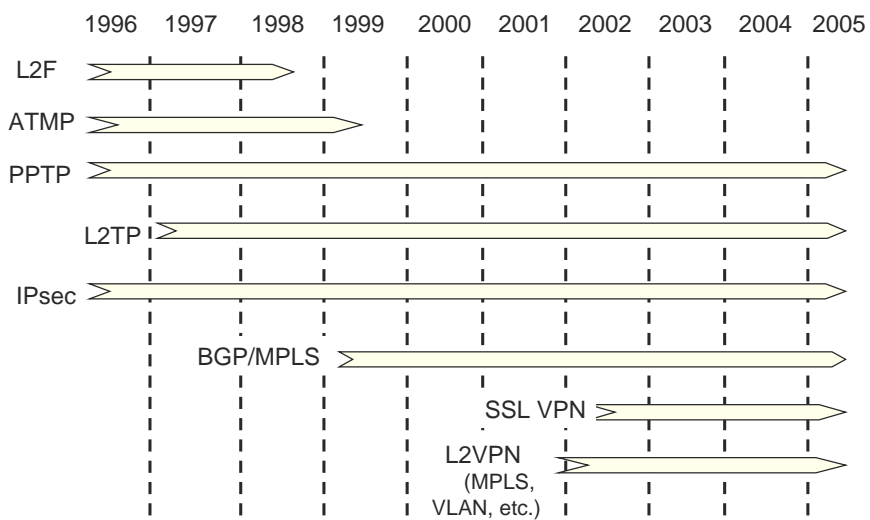


T27 : VPN 再考

~ 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.

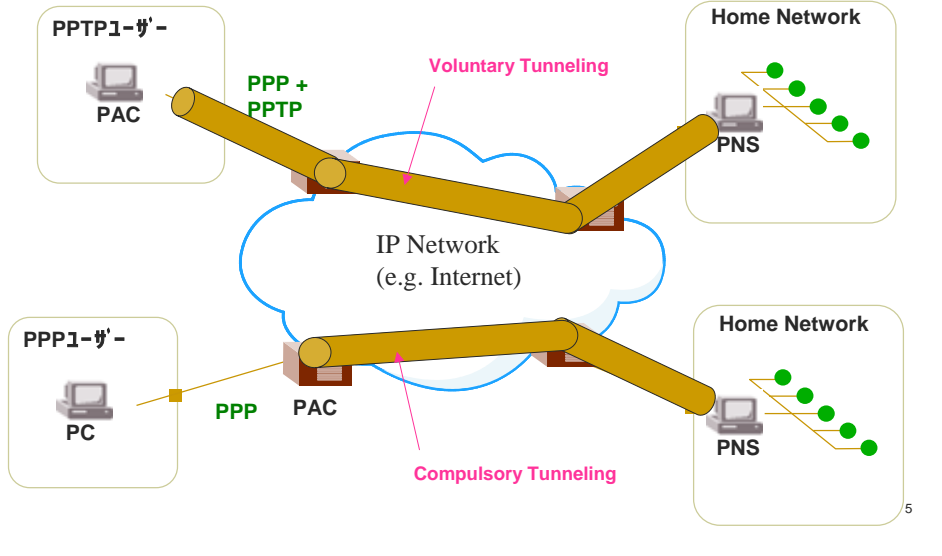
3

PPTP

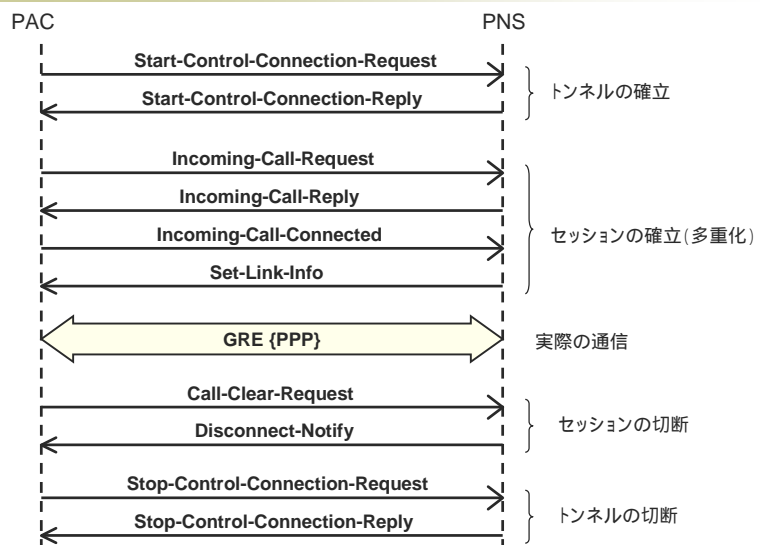
- **P**oint to **P**oint **T**unneling **P**rotocol
- RFC 2637 (Informational)
 - Microsoft
 - 3Com
 - Ascend (Lucent)
- 幅広いサポートプラットフォーム
 - Windows 系
 - MacOS X
 - ブロードバンドルーター
 - ...

4

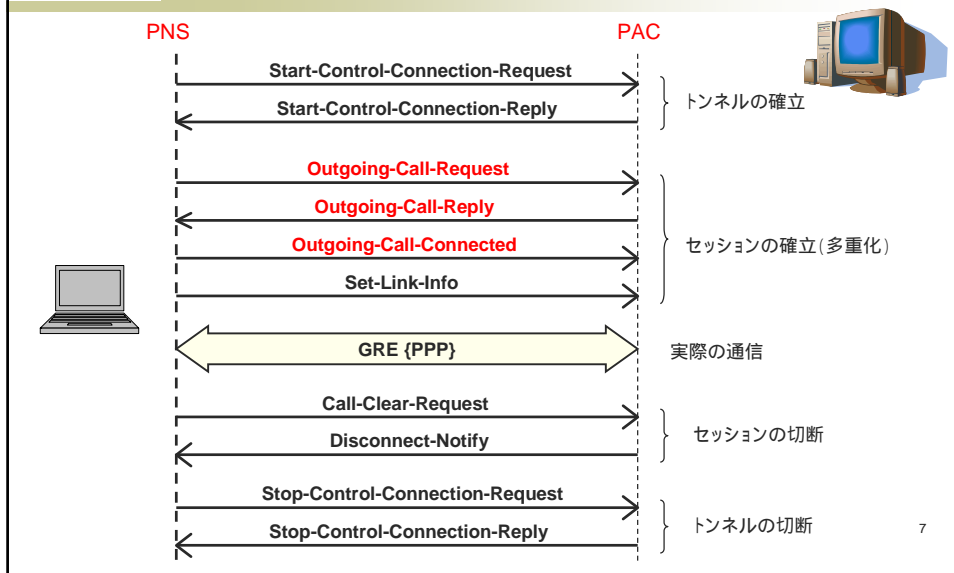
PPTPによるVPN



PPTPの動き

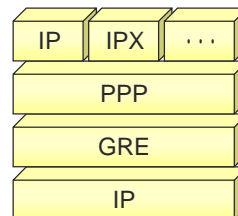


MicrosoftのPPTPの動き



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)

9

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

10

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

11

L2TP

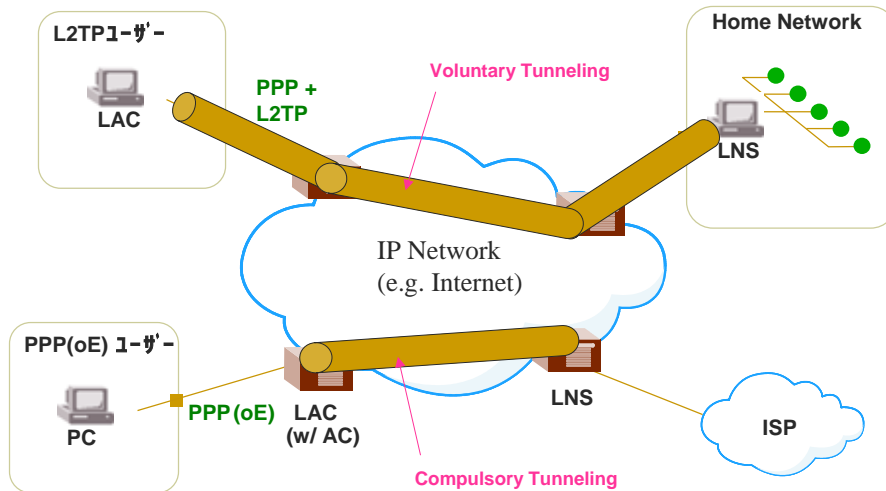
- Layer 2 Tunneling Protocol
- RFC 2661 (Standard Track)
 - Cisco
 - Ascend (Lucent)
 - Microsoft
 - Redback
- L2F + PPTP
 - メッセージフォーマット、LCP関連機能 ← L2F
 - 発呼の概念、フローコントロール ← PPTP
- Windows 2000 以降の Windows に搭載

12

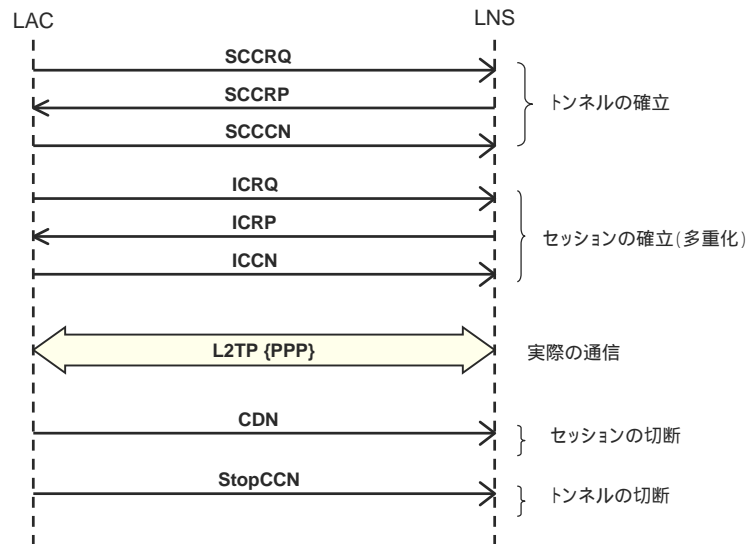
L2TPの特徴

- 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



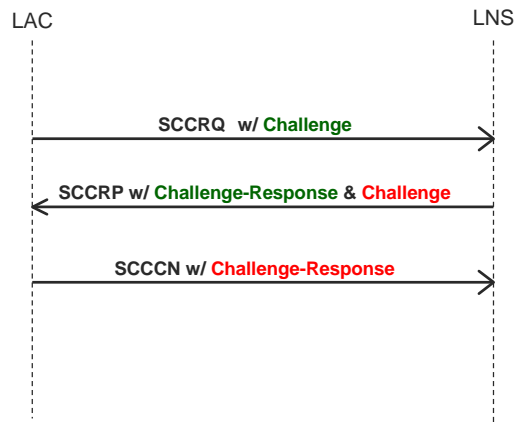
15

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

16

トンネル認証の動き



17

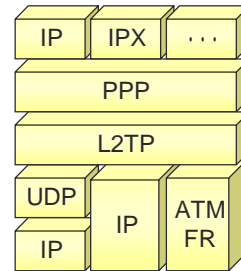
L2TPの適用箇所

- 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)

18

Quick Review (L2TP)

- シグナリング
 - 何の上にも乗る
 - 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.



19

L2TPの利点・欠点

- | | |
|--|---|
| <ul style="list-style-type: none"> ■ 利点 <ul style="list-style-type: none"> ○ 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 | <ul style="list-style-type: none"> ■ 欠点 <ul style="list-style-type: none"> ○ ユーザーが使うにはちょっと面倒 <ul style="list-style-type: none"> ■ IPsecにたよる場合 ○ 下位レイヤ独立 |
|--|---|

20

L2TPの今後

- L2TPv3
 - draft-ietf-l2tpext-l2tp-base-14.txt
 - 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

21

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) ??

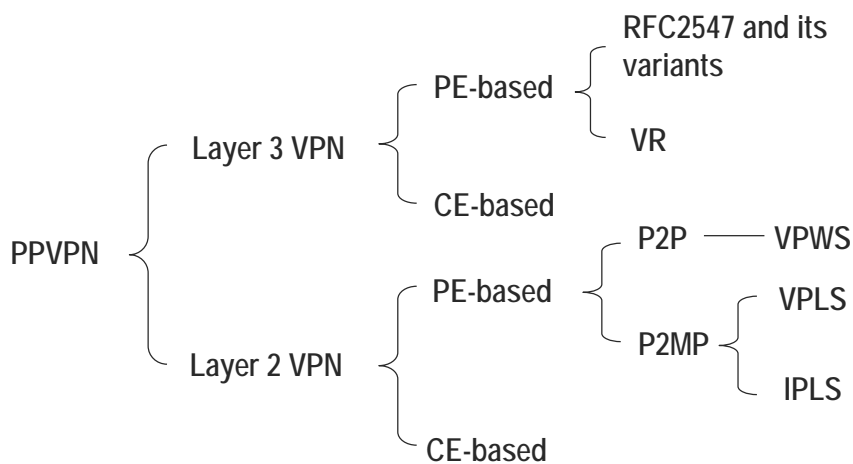
22

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

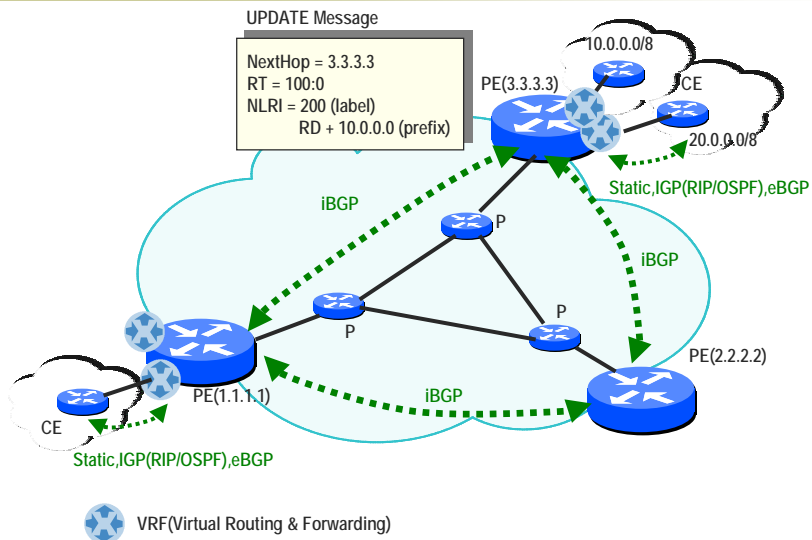
23

IETF PPVPN分類



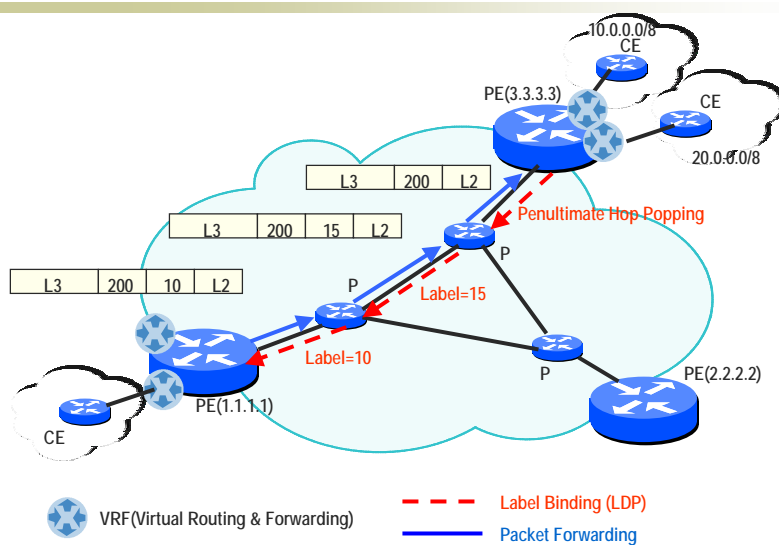
24

BGP/MPLS VPN (RFC2457) の動き (1)



25

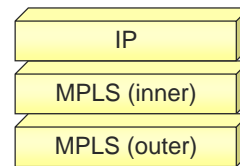
BGP/MPLS VPN (RFC2457) の動き (2)



26

Quick Review (BGP/MPLS VPN)

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



27

BGP/MPLS VPNの利点・欠点(顧客にとって)

- | | |
|--|--|
| <ul style="list-style-type: none"> ■ 利点 <ul style="list-style-type: none"> ○ 非常に透過的(おまかせモデル) <ul style="list-style-type: none"> ■ 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?? | <ul style="list-style-type: none"> ■ 欠点 <ul style="list-style-type: none"> ○ 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 |
|--|--|

28

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

29

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！

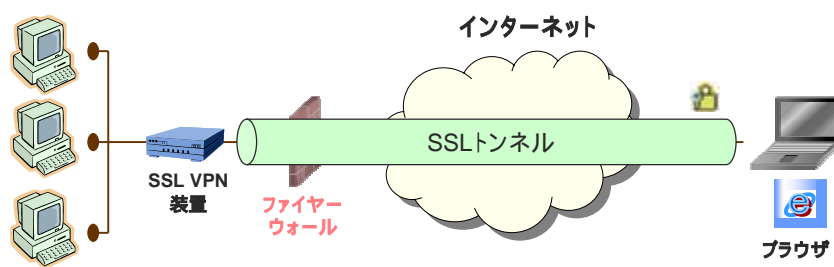
30

各種SSL VPN方式

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

31

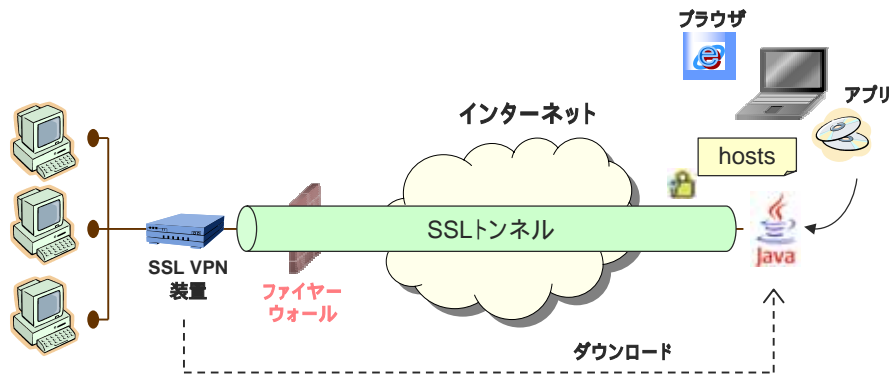
リバース・プロキシ方式



- 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

32

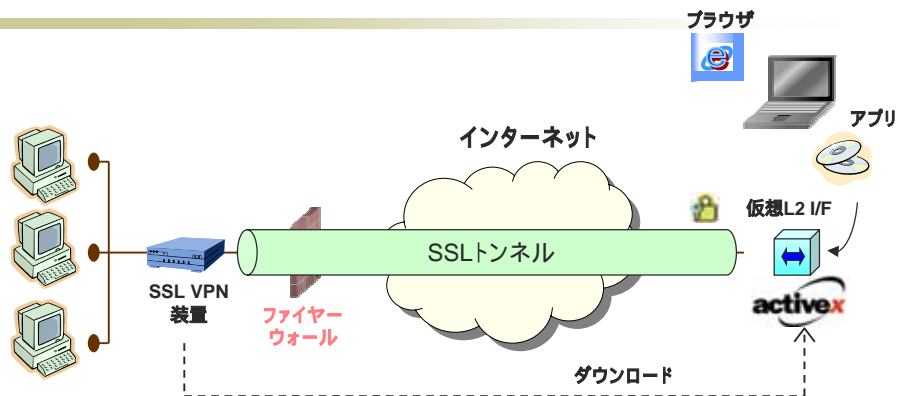
Java Applet方式



- Javaア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

33

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

34

さて、・・・

- いままでのVPNは、
 - NATしづらかったり
 - DoS攻撃に弱かったり
 - 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
 - ・・・

37

SoftEther とは

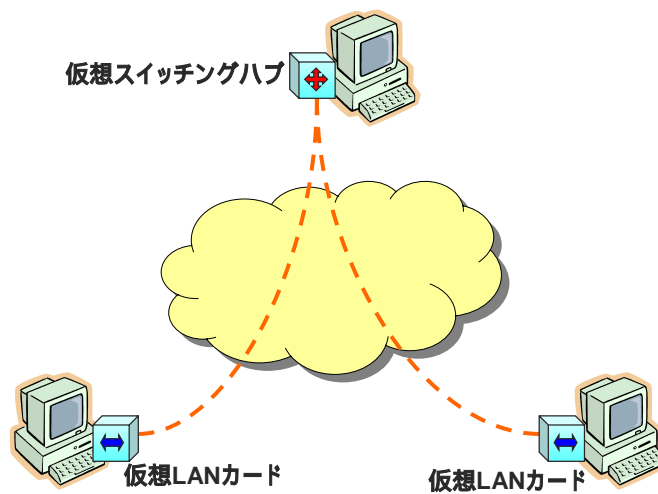
- 仮想的に (Ethernet) スイッチングハブと (Ethernet) 仮想 LAN カードを模擬
- それらを結ぶことにより Overlay ネットワークを形成することができる
- <http://www.softether.com>

38

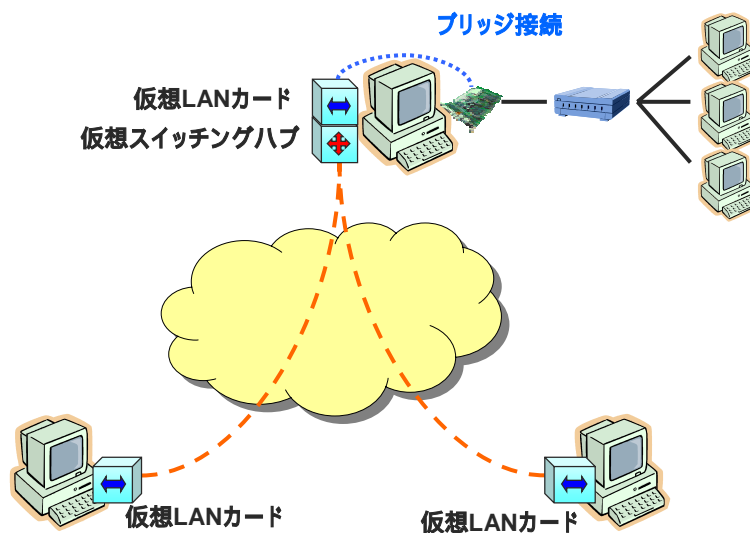
なぜ今SoftEtherが注目されるのか？

- (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
- ...

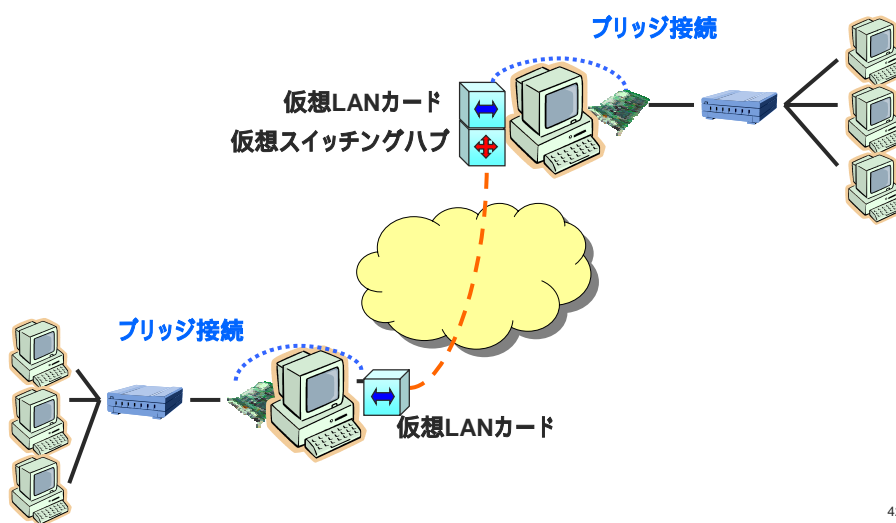
SoftEther トポロジー (PC to PC)



SoftEther トポロジー (PC to LAN)



SoftEther トポロジー (LAN to LAN)



SoftEtherをIETF的に見ると・・

- VPLS (Virtual Private LAN Service) の一種と捕らえる事ができる
 - ただし、Provider Provisioned (Compulsory)ではなく、Voluntary
 - PEという概念がない

43

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！
 - 証明書を(いまのところ)使っていない
 - 繋ぎ易さゆえの弊害？

44

SoftEther CA

- 商用版SoftEther
- 電子証明書のサポート
- “ゾーン”のサポート

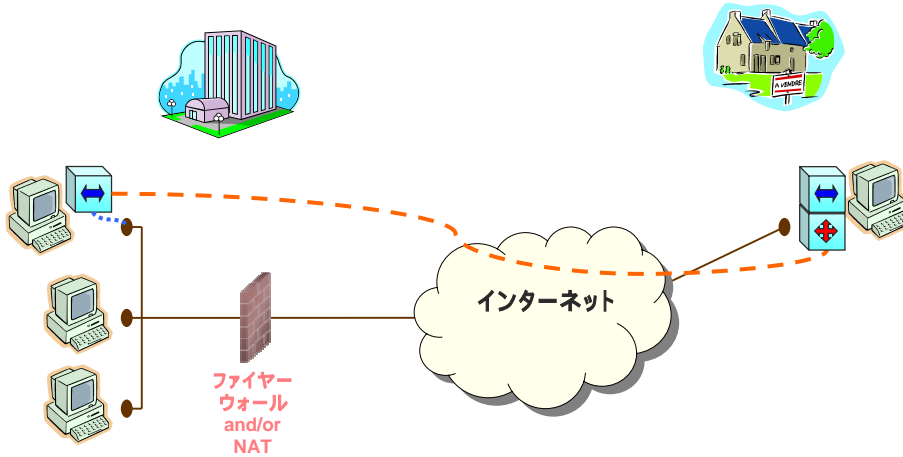
45

その他のSoftEtherの機能

- ログ機能
 - Hub (Layer2 機器)だが、Layer 3の情報も取れる
- VLAN的機能
 - ユーザーに仮想Hub IDを割り当てる
- DHCP関連機能
 - DHCPパケットのフィルタリング
 - DHCPで割り当てたIPアドレスを強制

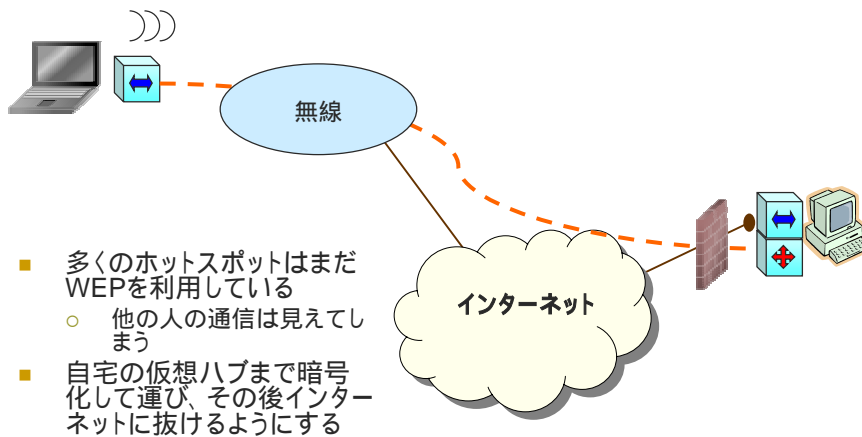
46

社内LANへのアクセス(2)



49

ホットスポットでの利用



50

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、工夫をすればそれほど悪くはなくなるらしい！

51

SoftEther VPN 2.0

- 高速化
- 負荷分散機能
- 複数の仮想Hubインスタンスのサポート
- SDKの提供

52

SoftEtherはセキュアか？

- いまのところ大きな問題は見つかっていない
 - 仮想Hubの認証は課題
- プロトコルは公開されていない
- 専門家でも“過ち”を犯すことはままある
- プロトコルを公開して多くの専門家のレビューを受ける必要がある！

53

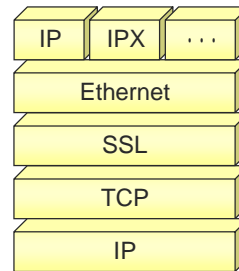
SoftEtherを発見できるか？

- 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
- 専用のアプライアンス

54

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



55

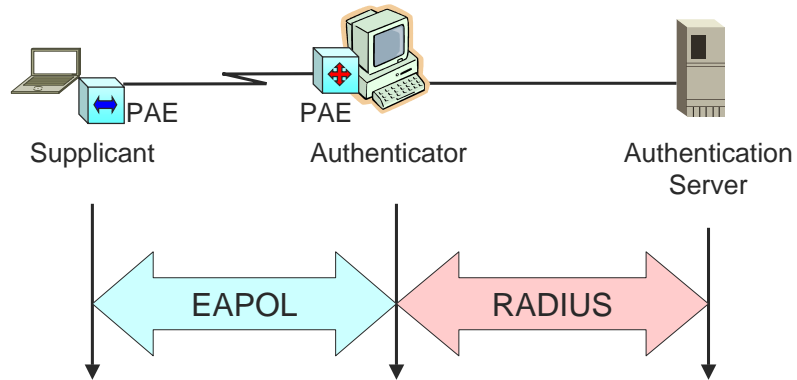
SoftEtherの利点・欠点

- | | |
|--|--|
| <ul style="list-style-type: none"> ■ 利点 <ul style="list-style-type: none"> ○ 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☺ | <ul style="list-style-type: none"> ■ 欠点 <ul style="list-style-type: none"> ○ お手軽！ |
|--|--|

56

Wish List to SoftEther

- 仮想Hubで802.1Xをサポートしてもらいたい！



57

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

58

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>
- 他にもまだまだたくさん

59

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

60

略語一覽

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