

VPN L2TPによる トンネリングネットワーク

株式会社インターネット総合研究所

研究員 松本 直人

not@IRI.CO.JP

はじめに

本稿は、現在盛んに取りざたされているVPN (とくにL2TP)に関して、技術的な解説を行う事を目的とする。

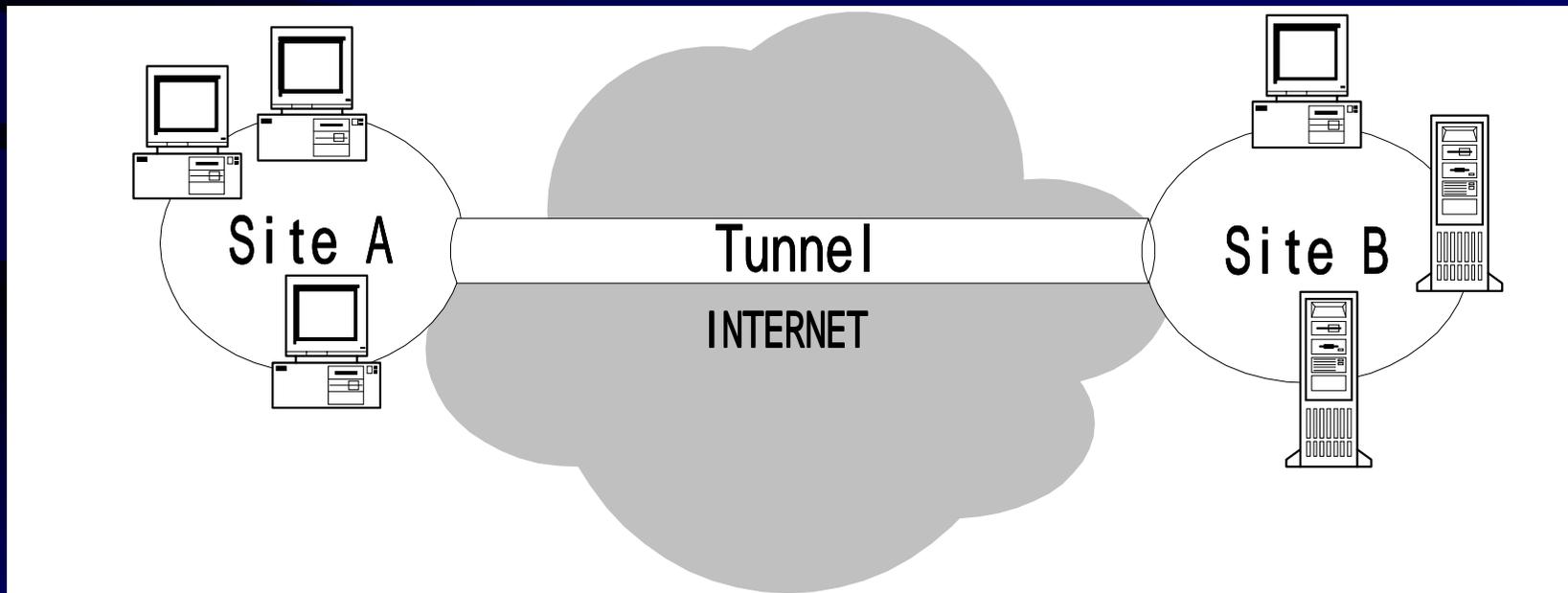
本稿は、VPN関連技術に関してI-D(Internet Draft)およびRFCから多くの引用を行っている。技術詳細に関しては、I-DおよびRFCから得る事が望ましい。

プレゼンテーションの流れ

- VPNとは
- L2TPとは
- トンネルの管理方法
- セキュリティ問題
- 運用における問題点
- まとめ

VPNとは

- VPN = Virtual Private Network
- Internet上に仮想私設網を構築



VPNの種類

- Network-to-Network型
- End-to-End型
- Virtual Dialup Service型...etc

VPNの基本要素

- トンネリング技術
- 暗号化技術

L2TPとは

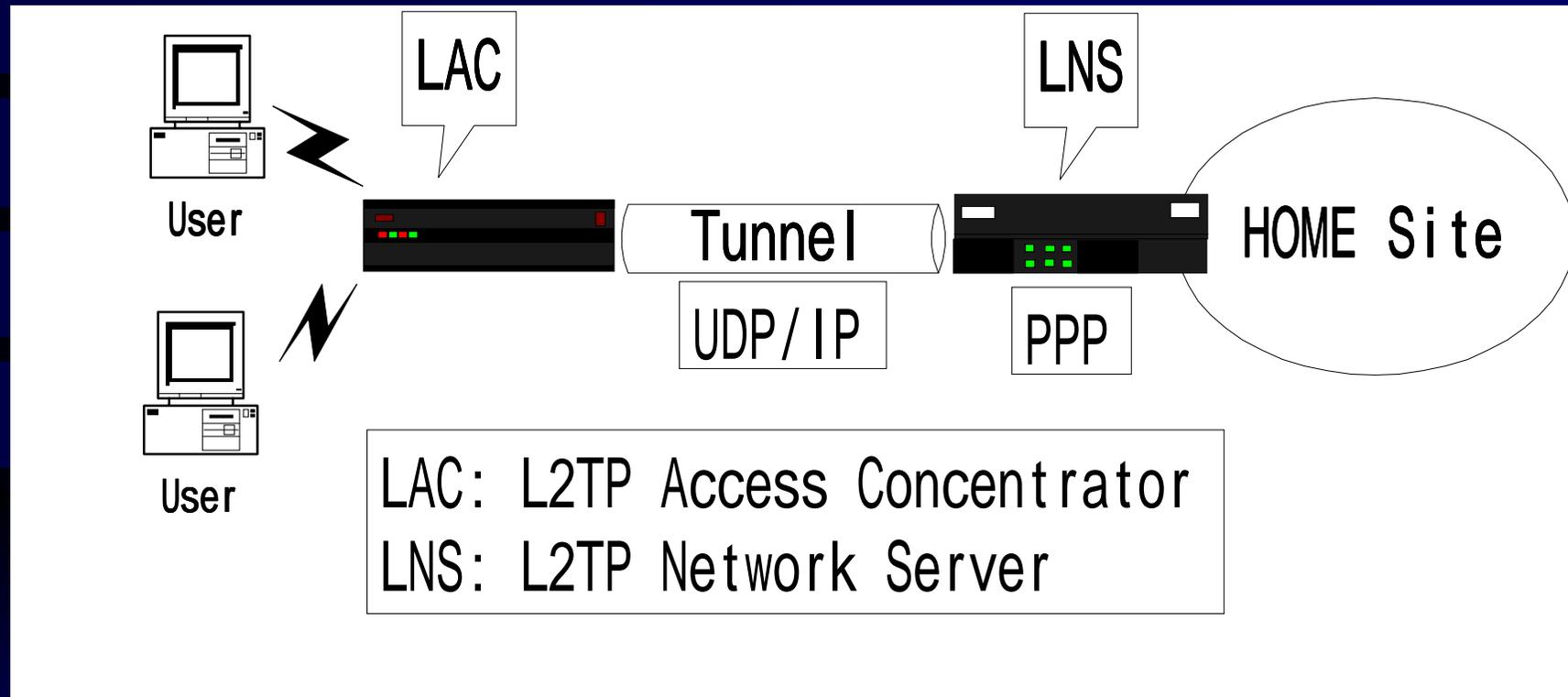
L2TP: draft-ietf-pppext-l2tp-11

- トンネリング
- ISPの既存接続資源を共有
- 既存ユーザーとVirtual Dialup
ユーザーを共存

L2TPプロトコル概要

- PPP Datagramをカプセル化
- カプセル化データをUDPパケットとして搬送
- PPP Datagramをカプセルから抽出
- PPP上でLCP/NCPの処理を実行

L2TPの処理イメージ



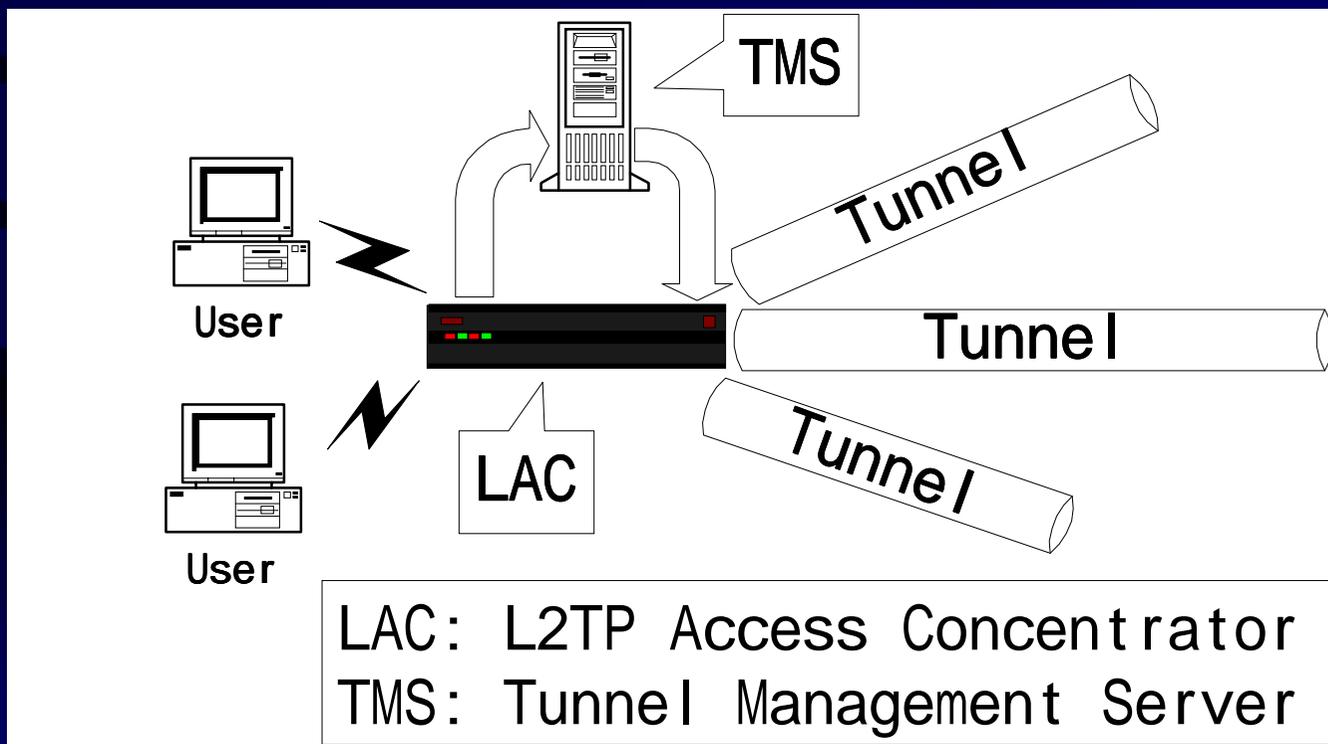
L2TPが行ってくれること

- **認証(Authentication)**
ユーザーおよびトンネルの認証を行う
- **アドレス割り当て(Addressing)**
Virtual Dialupユーザーに対して、アドレス割り当てを行う
- **使用許可(Authorization)**
ユーザーおよびトンネルの使用許可を与える
- **課金処理(Accounting)**
ユーザーおよびトンネルの課金情報を生成する

トンネルの管理方法

- トンネルの管理は、RADIUS等で行われる

RADIUS: draft-ietf-radius-tunnel-imp-03



セキュリティ問題

- L2TPには、暗号化アルゴリズムは含まれていない

PPP Encryption (Layer 2 Encryption)

IPsec (Layer 3 Encryption)

High Layer Encryption

運用における問題点

- ネットワークをまたがるセキュリティが問題
- トンネル管理は容易であるか
- ISPの管理ネットワークは安全であるか
- 暗号化の強度は高いか

まとめ

- L2TPは、すべてI-D(Internet Draft)状態
- 相互接続実績は上がっていない
- いまだVirtual Dialup Serviceは始まっていない

ちょっとCM

Network
Operational
Engineering
Laboratory



03/July/1998 JANOG2



ご静聴ありがとうございました

03/July/1998 JANOG2

