Les Réseaux Privés Virtuels (VPN)

Définition d'un VPN

Un VPN est un réseau privé qui utilise un réseau publique comme backbone

- Seuls les utilisateurs ou les groupes qui sont enregistrés dans ce vpn peuvent y acceder.
- Les données transitent dans un tunnel après avoir été chiffrées.
- Tout se passe comme si la connexion se faisait en dehors d'infrastructure d'accès partagé comme Internet.

Objectifs et caractéristiques des VPN

- Étanchéité du trafic entre les différents réseaux privés virtuels
- Sécurité des communications :
  - Confidentialité (chiffrement des données)
  - Authentification (utilisateurs ou DATA)
- Notion de qualité de service
  - Type best effort dans le cas de simples tunnels créés par l'utilisateur
  - QOS bien meilleure dans le cadre d'une offre VPN d'opérateur
- Coût :
  - Permet de réduire les coûts liés à l'infrastructure réseau des entreprises par la mise en place d'une liaison vpn

Le tunneling

- Le VPN est basé sur la technique du tunnelling:
  - Processus d'encapsulation, de transmission et de désencapsulation.
  - Consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire.
  - La source chiffre les données et les achemine en empruntant ce chemin virtuel.
- Les données à transmettre peuvent appartenir à un protocole différent d'IP.
- Le protocole de tunnelling encapsule les données en rajoutant une entête permettant le routage des trames dans le tunnel.

Sommaire

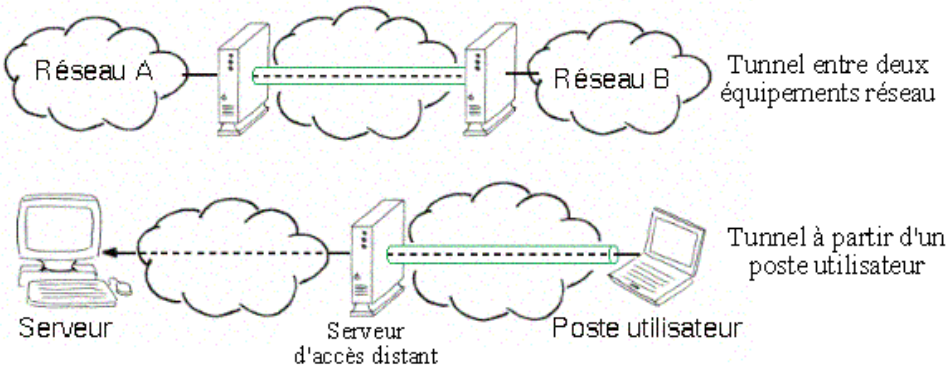
- Principes de "tunneling"
- Principaux usages des VPN
- Protocoles de "tunneling" des VPN
  - Rappel sur PPP
  - Protocoles PPTP, L2TP
- Sécurité des connexions VPN

Rappel, Tunneling

- Caractéristiques :

Un tunnel sert à transporter des données d'un point A vers un point B, au sens où les données qui "entrent" dans le tunnel en A "ressortent" nécessairement en B.

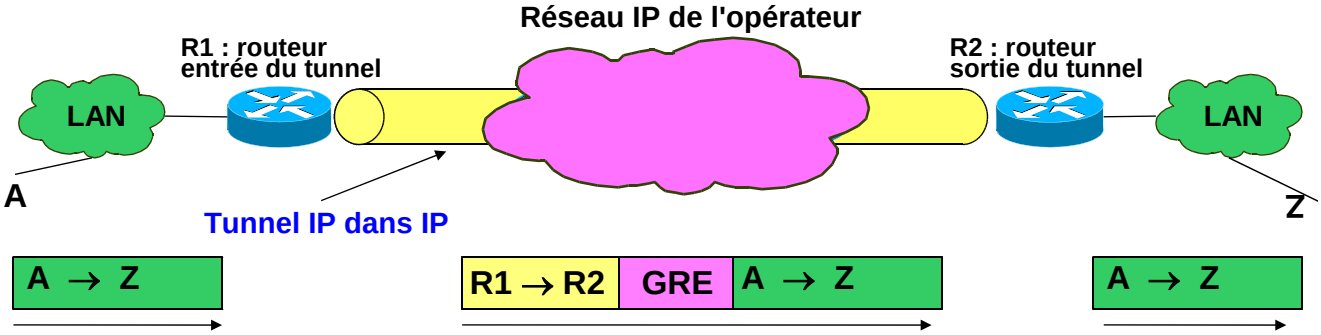
- Exemples :



Tunnels – Principe de fonctionnement

- Le transport de données se fait par encapsulation :
  - Extrémité du tunnel: données à transporter insérées dans un **paquet de protocole de "tunnélisation"**, puis dans un **paquet du protocole de transport** de données.
  - L'autre extrémité du tunnel: données extraites du protocole de "tunnélisation" et poursuivent leur chemin sous leur forme initiale.

Tunnels – Principe de fonctionnement



- Un tunnel est créé entre R1 et R2 :
  - Configuré dans les routeurs d'entrée et de sortie
- Le paquet ip privé (avec adresses IP privées) est encapsulé dans un paquet IP public:
  - Les adresses de R1 et R2 sont des adresses publiques
- Tunnel IP dans IP :
  - Le protocole GRE permet d'encapsuler les papquets IP dans IP
  - L'entête GRE permet d'annoncer le type de paquet encapsulé (IPv4)

Tunnels – Principaux protocoles

Différents protocoles:

- Passenger Protocol – Les données originales (IP…) à transmettre.
- Encapsulating Protocol – Le protocole (GRE, IPSec, PPTP, L2TP) utilisé pour encapsuler les données originales.
- Carrier Protocol – Le protocole employé par le réseau pour transporter les données.

The original packet (Passenger protocol) is encapsulated inside the encapsulating Protocol, which is then put inside the carrier protocol's header (usually IP) for transmission over the public network.

- Le protocole d'encapsulation peut assurer également le chiffrement des données.

Tunnels – Protocoles niveau 2, 3 & 4

- Protocoles de niveau 2 : PPTP, L2TP tous les deux encapsulent les données utiles (payload) dans une trame PPP qui sera transmise à travers Internet.
  - Le tunnel est semblable à une session ;
  - Les deux extrémités du tunnel doivent être d'accord et doivent négocier des variables de configuration, assignation des adresses, paramètres d'encryptions et/ou de compression ;
  - Un mécanisme de gestion et de maintenance du tunnel.

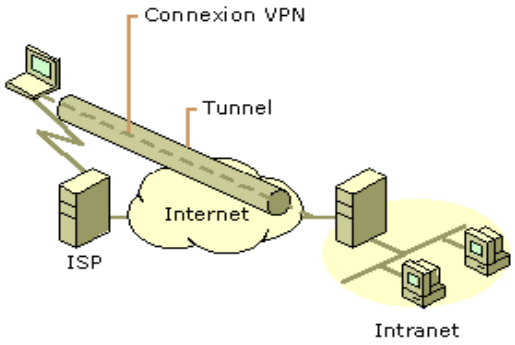
- Protocoles de niveau 3 : IPSec encapsule les paquets IP dans un autre paquet IP avant de l'envoyer sur Internet.
  - Les variables sont pré-configurées
  - Pas de phase d'entretien de tunnel

- Protocoles de niveau 4 : utilise TLS/SSL pour sécuriser les échanges au niveau de la couche Transport

VPN – Usages (1)

- VPN accès distant :
  - Permet à des utilisateurs itinérants d'accéder au réseau privé.
  - L'établissement de la connexion VPN se fait via une connexion Internet.

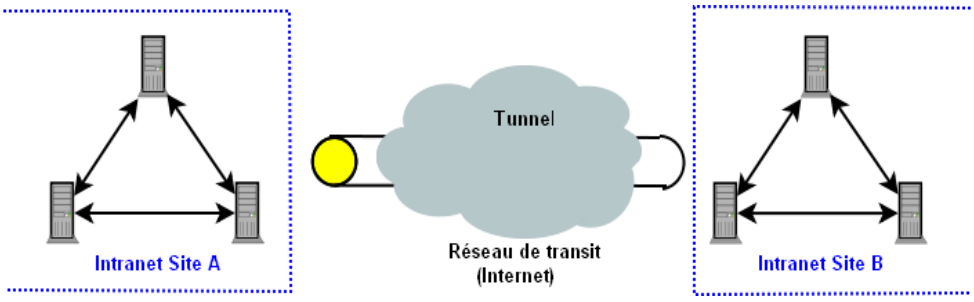
- Deux cas :
  - La connexion est établie entre le NAS (Network Access Server) de l'ISP et le serveur VPN disant.
  - La connexion est établie entre le client (client vpn) le serveur VPN distant.



Source: Virtual Private Networking in Windows 2000: An Overview. Microsoft – White paper.

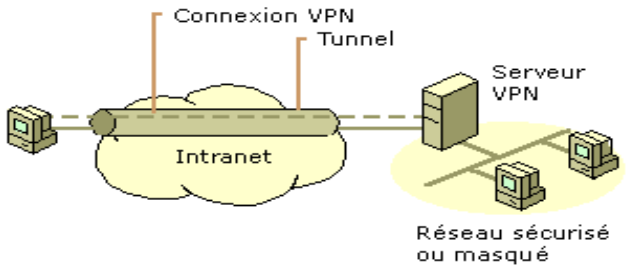
VPN – Usages (2)

- L'intranet VPN (vpn entre sites):
  - Permet de relier plusieurs sites distants au sein d'une entreprise.
  - Mise en œuvre avec des tunnels de niveau 3.
  - Garantie une authentification au niveau paquet



VPN – Usages (3)

- Accès client distant via un intranet :
  - Utilisé pour sécuriser un réseau d'un département du reste de l'intranet d'une l'entreprise :
    - ☞ Le réseau département étant séparé d'intranet par un serveur VPN .
    - ☞ Les utilisateurs doivent bénéficier des autorisations appropriées pour établir une connexion VPN au serveur VPN.
    - ☞ Pour tous les autres, le réseau du département est masqué.



Source: Virtual Private Networking in Windows 2000: An Overview. Microsoft – White paper.

Caractéristiques fondamentales d'un VPN

A Une solution de VPN devrait fournir au moins l'ensemble des caractéristiques suivantes :

- Authentification
- Cryptage des données
- Adressage
- Filtrage de paquet
- Gestion des clés
- Support Multiprotocole.

Authentification

- Seuls les utilisateurs autorisés de la connexion VPN doivent pouvoir s'identifier sur le réseau virtuel.

- Authentification au niveau utilisateur
  - Protocole PPTP (niveau 2).
  - Basée sur le schéma d'authentification de PPP (PAP, MS-CHAP-v1&v 2).

- Authentification au niveau paquet:
  - Protocole Ipsec (niveau 3).
  - Identification de la source des données transmises, non-répudiation, etc.
  - Basée sur les signatures numériques ajoutées aux paquets.

- Authentification de type EAP:
  - EAP-TLS (RFC 2716) est une méthode d'authentification forte basée sur des certificats à clés publique.

Cryptage de données

- Nécessité de cryptage des données pour protéger les données échangées entre le client et le serveur VPN
  - Le cryptage des données pour les tunnels PPTP (implémentation Microsoft) utilise le protocole MPPE (Microsoft Point-to-Point Encryption),
  - Utilise l'algorithme RSA/RC4 pour créer une clé de cryptage basée sur le mot de passe client.

Adressage

Attribuer au client VPN une adresse IP privée lors de la connexion au réseau distant et garantir que cette adresse reste confidentielle:

- Les protocoles de tunneling niveau 2 supportent une assignation dynamique d'une adresse à un client, grace au protocole NCP (Network Control Protocol).
- Les protocoles de tunneling niveau 3 Layer 3 tunneling assument une assignation statique d'une adresse aux extrémités du tunnel avant que celui-ci soit établi.

Filtrage de paquets

- Mise en place de filtres sur l'interface correspondant à la connexion à Internet du serveur VPN.
  - Autoriser seulement le trafic VPN d'utilisateurs authentifiés
  - Empêcher le serveur VPN de recevoir du trafic en dehors du trafic VPN.
  - Assurer que seuls les données cryptées autorisées pénètrent au sortent du LAN privé.

Support Multi-protocole

La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publiques en particulier IP.

Les Protocoles de tunneling niveau 2 peuvent supportent plusieurs protocoles de liaisons de données (Ethernet, PPP, FR, MPLS, etc).

Les Protocoles de tunneling niveau 3, tels que IPSEC, supportent uniquement les couches cibles utilisant le protocole IP.

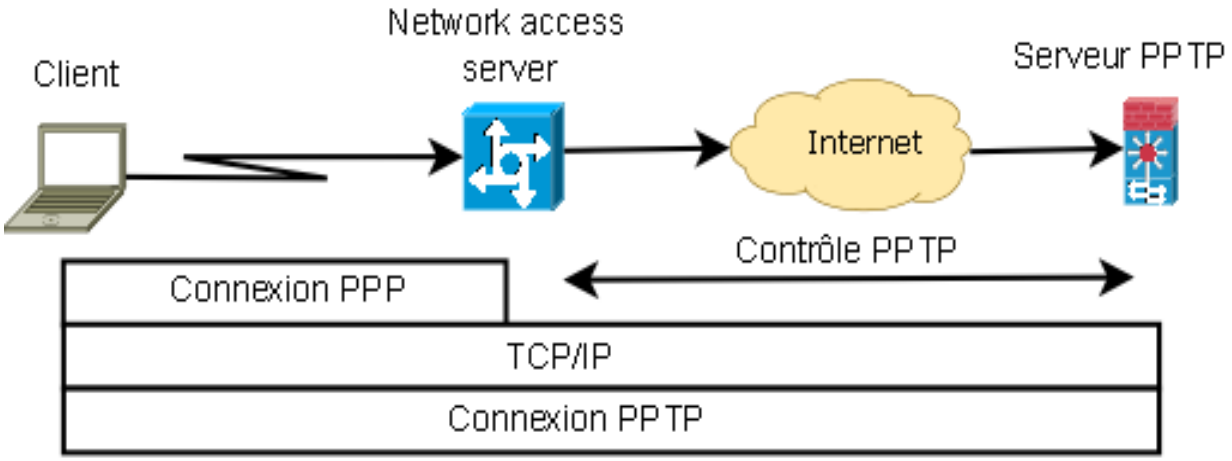
Les tunnels de niveau 2 (liaison de données)

Point-to-Point Tunneling Protocol

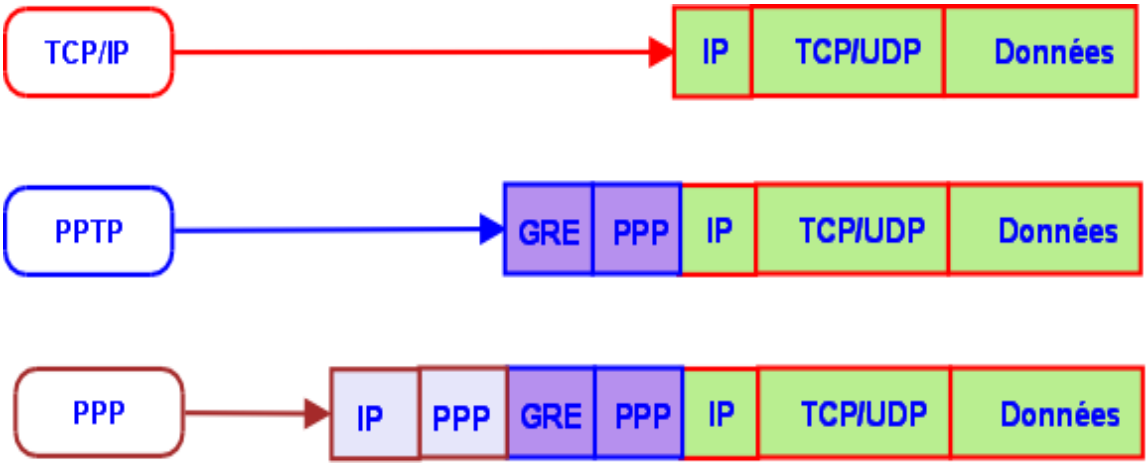
Point-to-Point Tunneling Protocol

- Protocole qui utilise une connexion PPP à travers le réseau TCP/IP pour établir une connexion vpn :
  - Le client PPTP se connecte à un serveur d'accès (NAS) chez l'ISP :
    - ☞ Initiation d'une connexion PPP vers l'ISP pour accéder à Internet.
  - Le NAS établit ensuite une connexion VPN utilisant PPTP vers le serveur VPN :
    - ☞ PPTP encapsulation des trames PPP cryptés dans des datagrammes IP grâce au protocole d'encapsulation GRE ;
- Trois composants :
  - La connexion PPP ;
  - La Connexion de contrôle PPTP ;
  - Encapsulation et transmission des données PPTP ;

PPTP : Schéma général



PPTP : Encapsulation

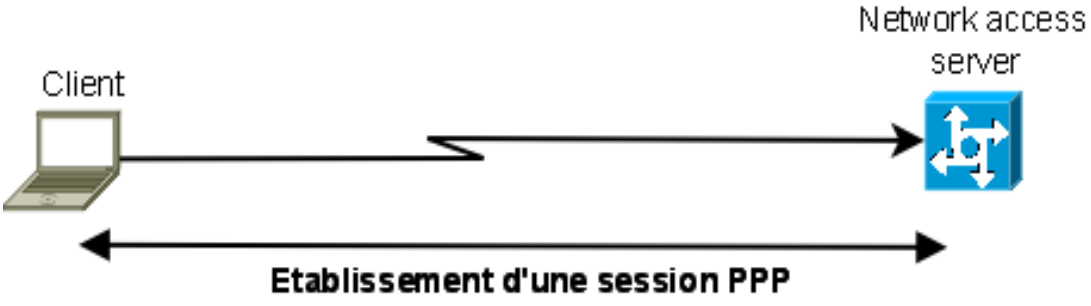


Le protocole PPP

- PPTP utilise PPP pour se connecter à un ISP (NAS).
- Protocole de niveau 2 permettant d'encapsuler des paquets IP sur une liaison point à point.
- Encapsulation de plusieurs protocoles au moyen de son composant NCP (*Network Control Protocol*) dans des trames PPP:
  - Protocoles de la couche réseau transportées dans une trame PPP
  - NCP pour chaque protocole de la couche réseau; **IPCP pour IP**
- Établissement et contrôle de la liaison avec LCP (*Link Control Protocol*):
  - Négocie et définit les options de contrôle sur la liaison de données.

Établissement d'une session PPP

- Trois phases principales :
  - Établissement de liaison ,
  - Authentification optionnelle,
  - Configuration du protocole de la couche réseau.



1. Phase d'établissement de liaison
2. Phase d'authentificationoptionnelle
3. Phase de configuration du protocole de couche réseau

Session PPP – Phase 1

- Établissement de liaison :
  - Chaque équipement PPP envoie des paquets LCP pour configurer, tester et terminer la liaison de données.
  - Les Paquets LCP contiennent un champs d'option de configuration permettant de négocier l'utilisation d'options telles que :
    - compression de certains champs PPP
    - protocole d'authentification de liaison

Session PPP – Phase 2

- Authentification optionnelle :
  - L'authentification a lieu avant d'entrer dans le phase de protocole de la couche réseau, une fois que le protocole d'authentification a été choisi.
  - Différentes méthodes d'authentification:
    - ✓ Password Authentication Protocol (PAP),
    - ✓ Challenge Handshake Authentication Protocol (CHAP),
    - ✓ Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).

Session PPP – Phase 3

- Protocole de couche réseau :
  - Les équipements PPP envoient des paquets NCP pour choisir et configurer un ou plusieurs protocoles de la couche réseau (tel que IP).
  - Choix du protocole (IPCP par exemple), assignation d'une @IP au client, envoie des datagrammes de chaque protocole sur la liaison.

Authentification PPP (1)

- PAP (PPP Authentification Protocol RFC1334) :
  - Authentification auprès du NAS par un nom d'utilisateur/mot de passe.
  - Le mot de passe circule en clair.
- Inconvénients :
  - Schéma d'authentification non sécurisé :
    - ☞ Un tiers pourrait capturer le nom et le mot de passe de l'utilisateur
    - ☞ Aucune protection contre les attaques par le rejeu n'est fournie.

Authentification PPP (2)

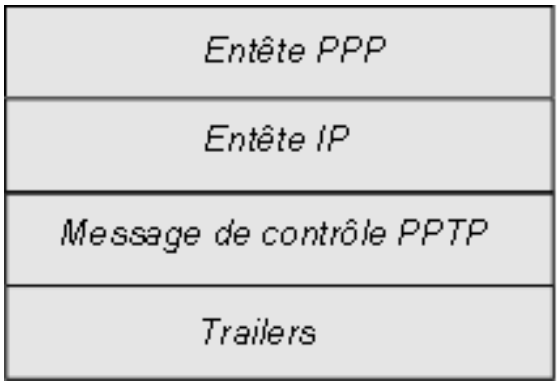
- CHAP (Challenge Handshake Authentication Protocol, RFC1994) :
  - **Challenge qui authentifie l'utilisateur auprès du NAS :**
    1. Le NAS envoie au user un "challenge" crypté avec un "secret partagé".
    2. Le user répond avec une valeur calculée en utilisant une fonction de hachage (MD5) le tout crypté avec le "secret partagé".
    3. Le NAS vérifie la réponse avec son propre calcul du hachée prévue. Si les valeurs concordent, le connexion est établie.
    4. A des intervalles aléatoires, le NAS envoie un nouveau "challenge" au user, et répète les étapes 1 à 3.
  - "challenge" CHAP = Session ID + nombre aléatoire.
  - Authentification basée sur un "secret partagé" dérivé d'un mot de passe stocké "en clair" sur le NAS.

Authentification PPP (3)

- MS-CHAP-v2 (Microsoft PPP CHAP Extensions version 2):
  - **Authentification mutuelle des deux pairs :**
    - ☞ Le NAS vérifie que le client d'accès a la connaissance du mot de passe de l'utilisateur et le client d'accès vérifie que le NAS a la connaissance du mot de passe de l'utilisateur.
  - Le serveur utilise les hachés du mot de passe du client, conservés dans une base de données, plutôt que le mot de passe "en clair".

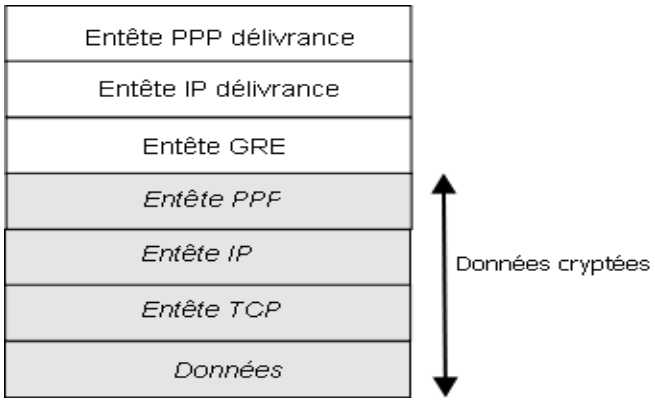
Connexion de contrôle PPTP

- Messages de contrôle entre client/serveur PPTP :
  - Établissement, maintien et terminaison du tunnel PPTP.
  - Messages transmis dans des segments TCP.
- Format d'un Message de contrôle PPTP :

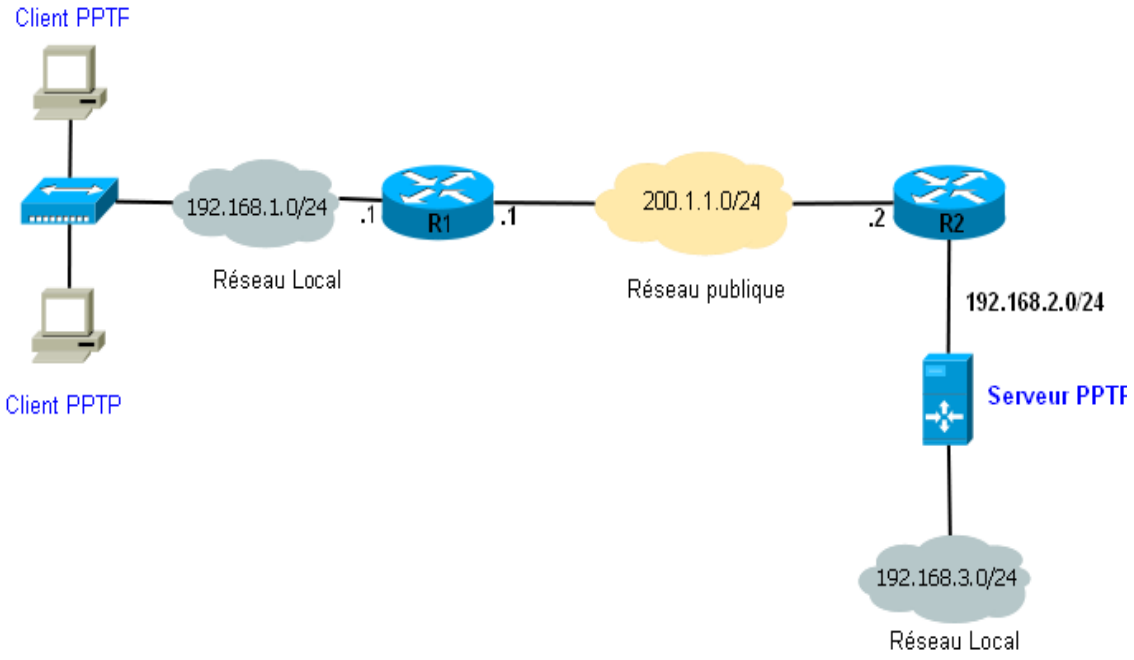


Transmission de données PPTP

- Encapsulation des trames PPP dans des datagrammes IP :
  - Datagrammes IP créés en utilisant le protocole GRE
  - → GRE : Generic Routing Encapsulation
- Format d'un datagramme IP créé par PPTP :



Scénario de la démonstration



L2F & L2TP

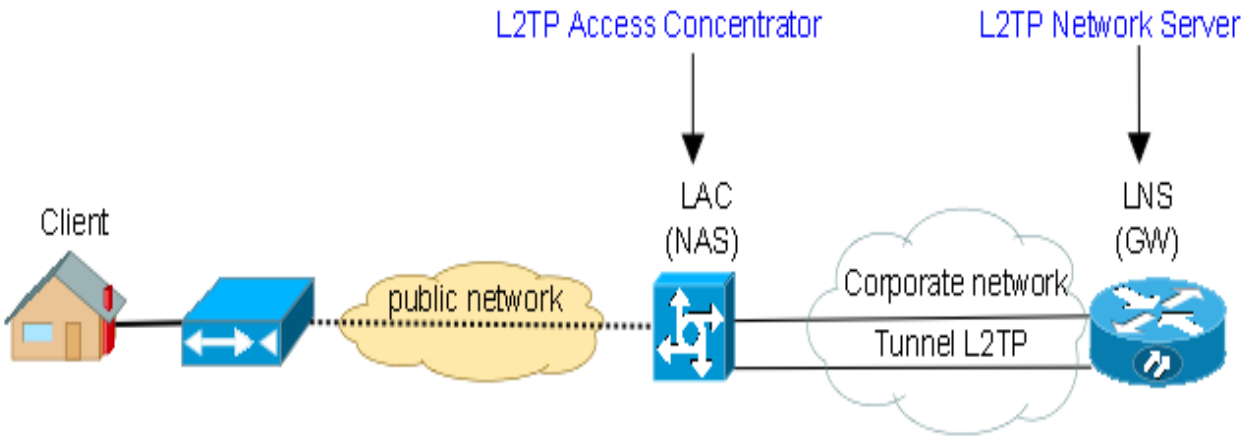
Layer 2 Forwarding

- Protocole développé Cisco Systems (RFC 2341)
- L2F fournit un tunnel sécurisé entre utilisateurs distants et la passerelle VPN
  - Authentification basée sur PPP / Chiffrement basé sur PPP
- Composants :
  - Tunnel L2F entre l'ISP et le serveur d'accès distant
  - Connexion PPP entre le client et l'ISP, que l'ISP fait suivre au serveur d'accès distant via le tunnel L2F

Layer 2 Tunneling Protocol

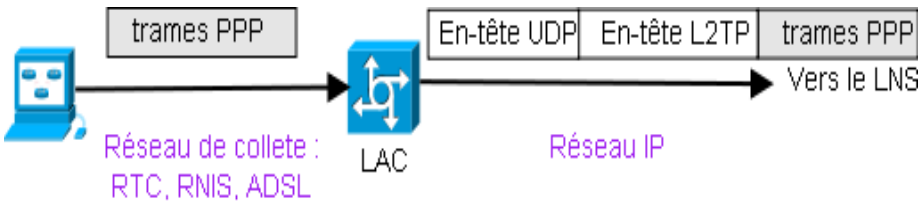
- L2TP = Fusion de PPTP et de L2F (RFC 2661)
- Transport en tunneling de trames PPP via Internet :
  - Repose sur le protocole UDP (port 1701) qui lui même repose sur IP
  - L'Encapsulation : **Layer-2-->IP--> UDP--> L2TP--> PPP--> IP**
- Deux composants :
  - **LAC (L2TP Access Concentrator)** : Client L2TP (NAS du ISP)
  - **LNS (L2TP Network Server)** : Seveur L2TP
- Tunnel entre le LAC et le LNS :
  - L'utilisateur (mobile) utilise le tunnel L2TP créé à travers internet pour se relier au réseau privé.

Schéma de l'architecture



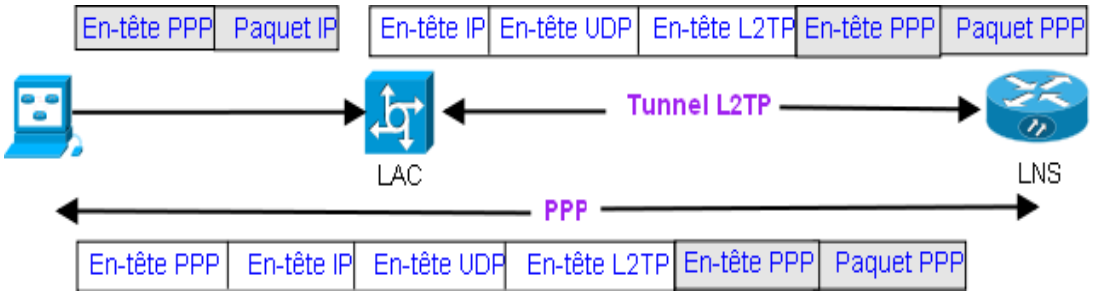
L2TP Access Concentrator

- Permet de relayer le trafic entre le LNS et l'utilisateur
  - Encapsulation de n'importe quel protocole transporté dans la trame PPP.
- Permet de négocier le LCP et l'authentification de l'utilisateur :
  - Données de négociation recueillies expédiées au LNS.



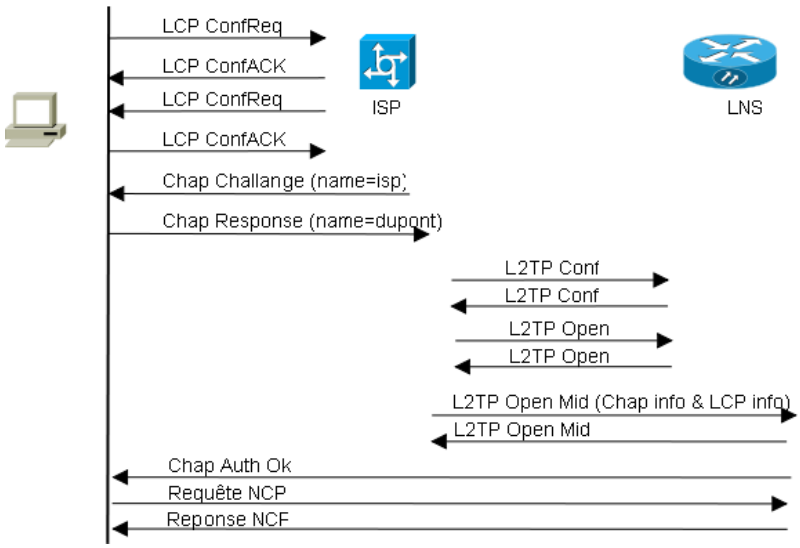
L2TP Network Server

- Équipement final de la connexion PPP

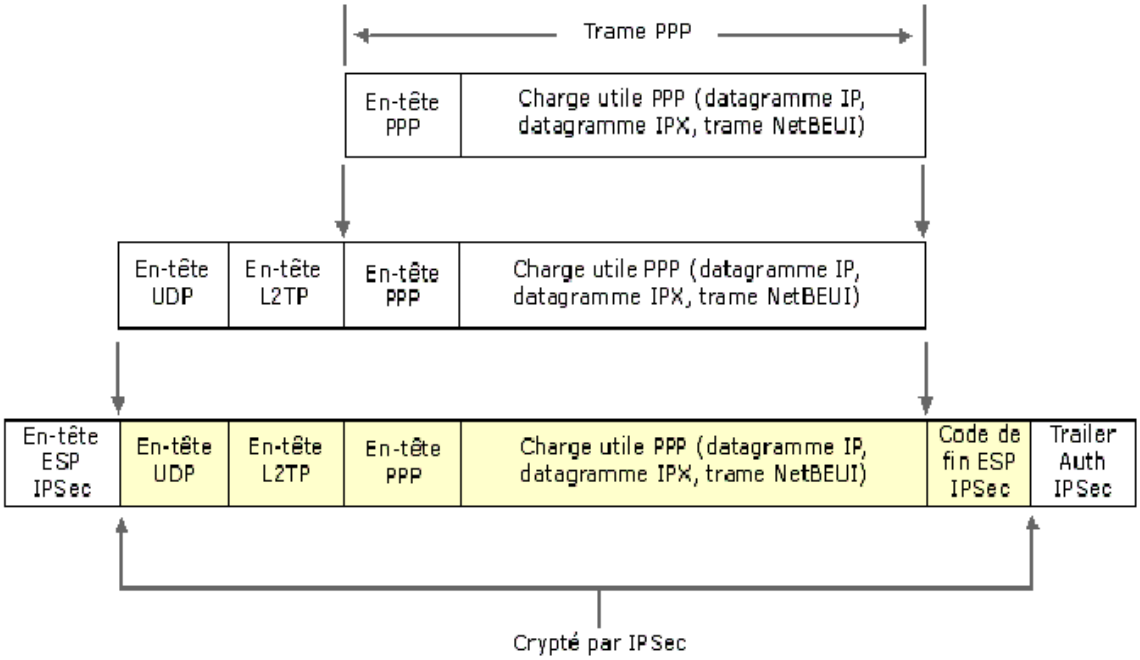


L2TP – Résumé

- Schéma protocolaire d'établissement de tunnel



L2TP/IPSec : Encapsulation



Quelques Liens

- Virtual Private Networking in Windows 2000: An Overview. Microsoft – White paper.
- Les protocoles de tunnelisation et de sécurisation des échanges. (Hervé Schauer Consultants)
- Le protocole PPP - Transparents Ghislaine Labouret (www.labouret.net/ppp)
- How Virtual Private Networks work. Cisco – White paper.
- Microsoft L2TP/IPSec VPN Client Overview
- RFC 2661 - Document de normalisation de L2TP