Cours de sécurité

Sécurité des niveaux liaison et réseau
Réseaux Privés Virtuels ‘RPV’
VPN ‘Virtual Private Networks’

Gérard Florin
- CNAM -
- Laboratoire CEDRIC -

Plan

- Généralités sécurité liaison / réseau et VPN
- Le niveau liaison
  - Transmission en sécurité de niveau liaison
  - Réseaux privés virtuels: VPN de niveau liaison
- Le niveau réseau
  - IPSEC : Transmissions en sécurité et tunnels
  - Réseaux privés virtuels de niveau réseau: VPN en MPLS
- Conclusion
- Bibliographie

Sécurité liaison/réseau et VPN

Généralités sécurité niveaux liaison et réseau et VPN

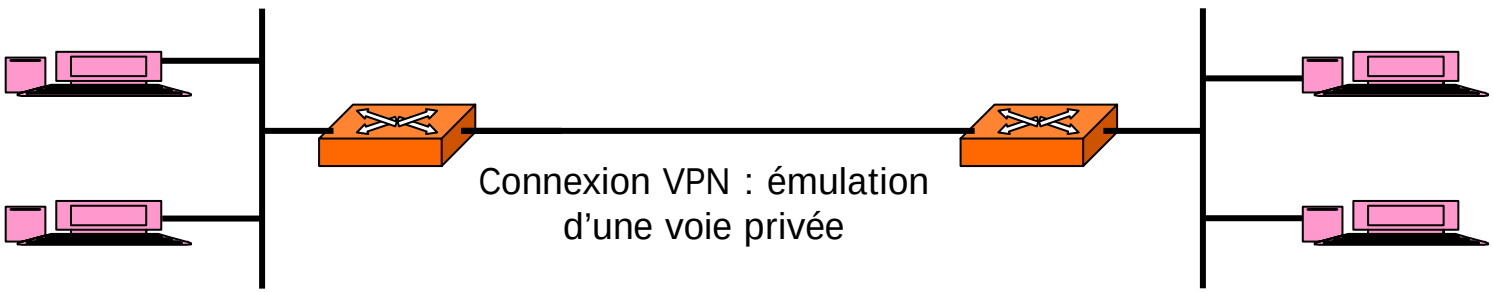
1 - Protocoles de sécurité associés aux niveaux liaison et réseau

- **Objectif :** réaliser des fonctions de sécurité pour un niveau.
- **Fonctionnement en mode ‘transport’ :**
  - Les fonctions de sécurité sont appliquées à la charge utile d’une trame ou d’un paquet.
- **1 Authentification**
  - Le problème le plus souvent traité car aux niveaux liaison et réseau on contrôle que des utilisateurs peuvent accéder à un réseau.
  - Très grand nombre de solutions proposées au niveau liaison.
  - Solutions également très correctes au niveau réseau IPSEC
- **2 Confidentialité**
  - Peu de propositions au niveau liaison avant les réseaux sans fils.
  - Renouvellement des besoins avec les réseaux sans fils.
  - Solutions très correctes au niveau réseau avec le protocole IPSEC
- **3 Intégrité**
  - Pratiquement rien au niveau liaison sauf réseaux locaux .
  - Solutions très correctes au niveau réseau IPSEC.

2 - Protocoles de sécurité associés aux réseaux privés virtuels : VPN

- **Une solution VPN**

- **Solution fonctionnellement équivalente à :**



Réseaux Privés Virtuels – VPN : Définitions de base

Objectif : réaliser un réseau privé sécurisé en utilisant l'infrastructure d'un réseau partagé (ouvert).

- **1 Réseau ('network')**
  - Interconnecter un ensemble de **systèmes informatiques dispersés.** Résoudre des **problèmes de commutation / routage (niveau 2 / 3).**
- **2 Privé ('private')**
  - **Transporter des flots de messages** d'une communauté **'privée'** de façon indépendante de ceux d'autres usagers.
  - Les usagers doivent recevoir une **garantie de sécurité (confidentialité, intégrité ou protection) sur leurs données.**
  - Les usagers autorisés peuvent communiquer en utilisant des **adresses, une topologie, un routage privés.**
- **3 Virtuel ('virtual')**
  - **Le réseau physique** ne correspond pas forcément au réseau visé.
  - **Le réseau privé est réalisé en partageant les ressources** d'un (ou de plusieurs) fournisseur d'accès.

Motivations pour les VPN : Deux objectifs principaux

- **1 Communications sécurisées sur une infrastructure partagée.**
  - **Sécurité visée : mécanismes de protection**

    => implantation en modifiant des protocoles de réseaux classiques.
    - **Solutions:** adressage et routage privé offerts par des mécanismes de protection garantis par un constructeur de routeur et un fournisseur d'accès.
  - **Sécurité visée : mécanismes pour la confidentialité et l'intégrité**

    => protocoles de sécurité utilisant des techniques de cryptographie.
    - **Solutions:** authentification, chiffrement en confidentialité, signatures.

- **2 Economies de coûts en partageant des plates-formes de communication à haut débit.**
  - **Efficacité du partage de voies physiques à haut débit:** coût des communications très réduit dans un réseau partagé (type l'Internet).
  - **Solutions alternatives non VPN : construire sa propre infrastructure** complètement privée en louant des liaisons spécialisées ou des circuits => surcoûts de location, d'administration.

Motivations pour les VPN : Trois autres objectifs importants

- **3 Communications fiables : sûres de fonctionnement 'dependable'.**
  - **Critères :** Disponibilité, fiabilité, sécurité ('safety'), maintenabilité.
  - Sûreté assurée par les redondances du réseau (maillage du réseau sous-jacent) => utilisation de protocoles de routage multi-chemin.

- **4 Performances pour des infrastructures extensibles (qui passent à l'échelle, 'scalable').**
  - **Critères : Temps de latence** (temps jusqu'au commencement de la réponse à une requête), **temps de réponse total , débit. Possibilité d'accroître la taille du réseau privé (extensibilité).**
  - **Performances en VPN:** souvent beaucoup de surcharges (protocoles supplémentaires, algorithmes cryptographiques).

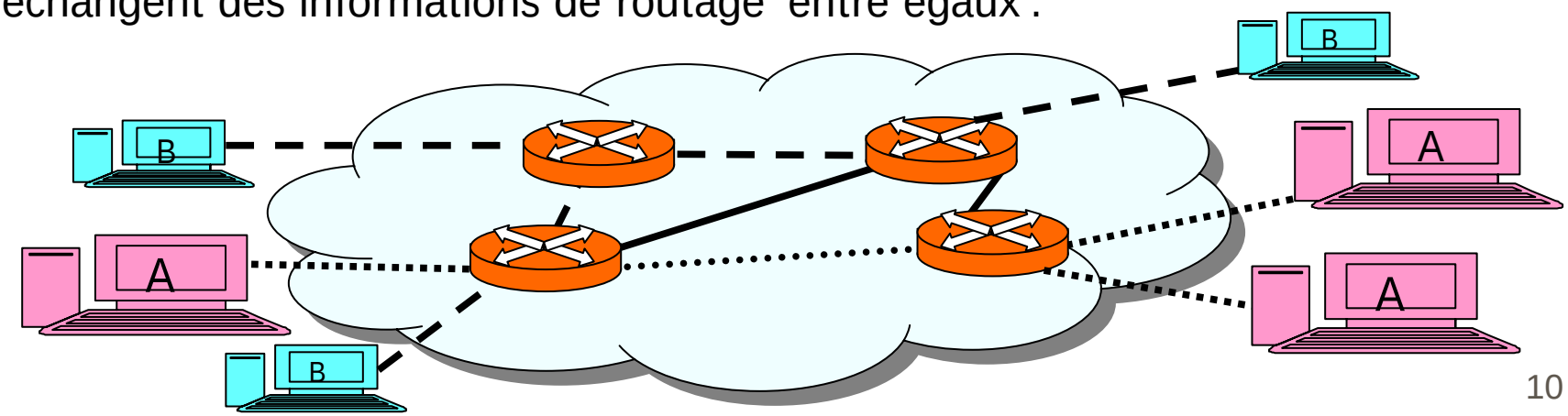
- **5 Solutions pratiques ('flexible') : les VPN : sont souvent considérés comme difficiles à gérer.**
  - **Facilité, simplicité** d'établissement des connexions et de l'administration.

Classification des solutions VPN

- **A) Classification selon le niveau du modèle OSI.**
  - **VPN de niveau liaison** (éventuellement même de niveau physique).
  - **VPN de niveau réseau.**
  - VPN de niveau transport.
  - VPN de niveau application.
- **B) Classification selon l'approche de sécurité**
  - **Protection:** Solutions de niveau 3 en routage pair à pair ('VPN Peer to peer'), de niveau (1) ou 2 ou 3 en recouvrement (VPN 'overlay')
  - **Authentification, Confidentialité, Intégrité :** Solutions de niveau quelconque (2,3,4,7) basées sur l'utilisation de tunnels ('Secure VPN Tunnelling').
- **C) Nombreux choix possibles selon des critères qualité :**
  - Analyse des risques couverts ou non par une implantation.
  - Possibilités de passage à l'échelle de la solution.
  - Complexité d'implantation puis de maintenance. …..

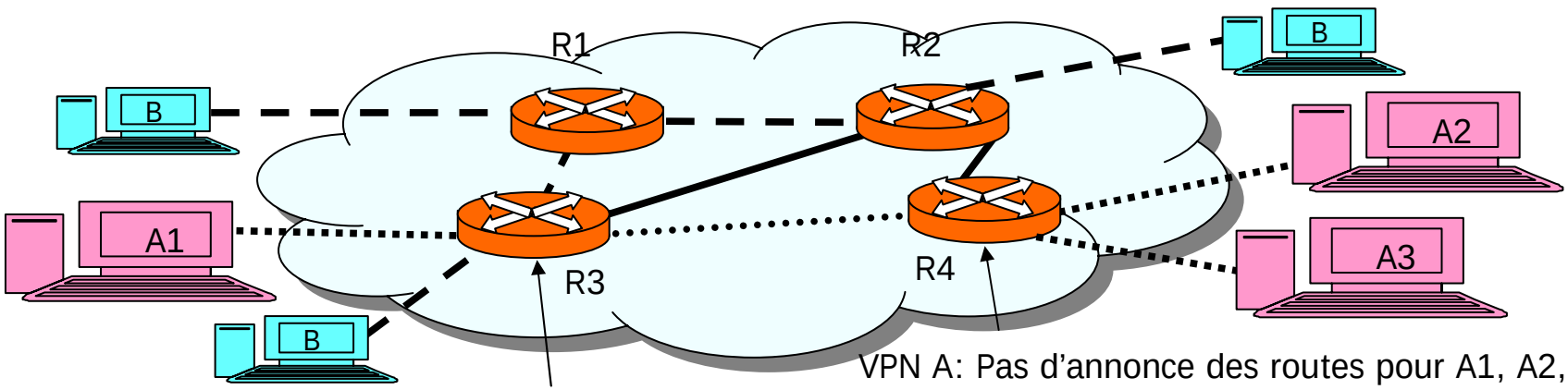
1) VPN de protection: Solution des VPN ‘pair à pair’ ‘peer to peer’

- **1) Approche de VPN (niveau 3) basée sur le contrôle d’accès (routage) :**
  - On parle quelquefois de ‘Trusted VPN’, VPN de confiance.
  - Solution implantée essentiellement dans les **VPN MPLS: L3VPN.**
- **2) Construction de groupes fermés d’usagers** d’un réseau => VPN
  - Sur la figure groupe A rose, B bleu.
- **3) Un routage est défini pour chaque groupe (VPN)**
  - Sur la figure VPN A : routes en traits pointillés courts ou VPN B : traits pointillés longs.
- **4) Idée de routage pair à pair :** Le routage dans un VPN pair à pair est réalisé comme dans les routages Internet classiques (RIP, OSPF,...): les routeurs voisins échangent des informations de routage ‘entre égaux’.



Implantation des VPN Pair à pair : filtrage de routes ('Route Leaking')

- **Contrôle d'accès (protection) appliqué au routage : pour chaque VPN et dans chaque routeur gestion de la liste des routes autorisées (en fait une C-liste liste de capacités pour des routes).**
  - Les routes associées à un VPN ne sont pas annoncées à l'extérieur.
  - Les routes extérieures au VPN ne sont pas annoncées dans le VPN.
  - La protection dans le VPN est réalisée par l'impossibilité d'acheminer des paquets (dans les deux sens, intérieur extérieur) avec des adresses externes au VPN (absence d'infos dans la table de routage du VPN).



VPN A : Pas d'annonce des routes pour A1, A2, A3, à R1 et R2. Annonce pour R4.

VPN A: Pas d'annonce des routes pour A1, A2, A3, à R1 et R2. Annonce pour R3.

2) Solution VPN en mode tunnel : Notion de tunnelage ‘Tunneling’

- **Notion de tunnel :** utiliser un protocole pour acheminer des messages d’un autre protocole.
  - **Encapsulation des messages du protocole transporté** dans des messages du protocole transporteur.
  - **Solution fréquente en réseau.**
- **Architecture en couches des réseaux (OSI) :** encapsuler des messages de **niveau N+1** dans des messages de **niveau N** (inférieur).
- **Différence mode tunnel et modèle OSI:**

  Tunnel = encapsuler des messages **d’un niveau donné** dans des messages du **même niveau ou de niveaux supérieurs.**

Les trois protocoles associés pour réaliser un tunnel

- **1) Le protocole 'porteur' utilisé ('Carrier Protocol'):**
  - Le protocole d'un réseau existant permettant d'acheminer des informations => N'importe quel protocole robuste et répandu.
  - **Exemples :** Surtout les protocoles de l'Internet PPP/IP/TCP/HTTP mais aussi ATM.
- **2) Le protocole d'encapsulation ('Tunneling Protocol'):**
  - Le protocole qui est ajouté pour encapsuler les données usagers en les sécurisant => le protocole qui réalise les objectifs VPN de sécurité.
  - **Exemples :** GRE, voir la liste sur le transparent suivant etc...
- **3) Le protocole transporté ('Passenger Protocol'):**
  - Le protocole utilisateur que l'on souhaite acheminer.
  - Exemples : un protocole Internet IP ou un protocole non Internet IPX, NETBIOS/NetBeui .... dans le protocole IP.

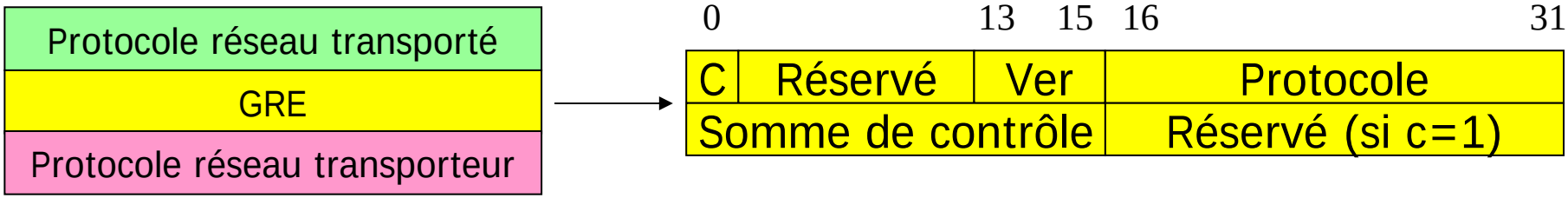
Exemples de protocoles de tunnelage sans sécurité

- **GRE** : **Generic Routing Encapsulation** (niveau 3 sur un autre niveau 3) (RFC 1701): uniquement dédié aux tunnels.
- **PPPoE** : Point to Point Protocol over Ethernet (niveau 2 sur niveau 2).
- **PPPoA** : Point to Point Protocol over ATM (niveau 2 sur niveau 2).
- **IP in IP Tunneling** : IP (V4) encapsulé dans IP (V4) (niveau 3 sur niveau 3) (RFC 1853).
- **6to4** : Tunnelage de IPV6 sur IPV4 (niveau 3 sur niveau 3).
- **IEEE 802.1Q** : Ethernet VLANs (niveau 2 sur niveau 2).
- **DLSw** : Data Link Switching SNA over TCP (niveau 7 sur 4).
- **XOT** X.25 over TCP : (niveau 3 sur niveau 4).

Le tunnel générique : GRE ‘Generic Routing Encapsulation’

- **GRE** : Origine Cisco, norme RFC 1701 (1994) modifiée RFC 2784 (2000).
- **Objectifs :** permettre d’encapsuler n’importe quel protocole sous GRE.
- **Problèmes résolus par GRE** : **en version de base.**
  - **Utiliser un code protocole IP** : pour extension GRE (47).
  - **Création d’une structure de données assez simple essentiellement pour identifier le protocole transporté**.
  - **Exemples** d’encapsulation de protocoles : ICMP=1, IP=4
  - **Codes types GRE gérés par l’IANA** RFC 1700 : la liste est en ligne www.iana.org.
- **Problèmes résolus en version étendue**:
  - **Contrôle d’erreurs** à fenêtre glissante sur le tunnel (numéros de séquences, d’acquittements)
  - **Autres indicateurs.**

GRE : Description de l'entête dans la version de base



- **C :** Présence ou absence de la somme de contrôle (cheksum).
- **Réservé :** Bits réservés pour un usage futur.
- **Ver :** numéro de version (zéro actuellement).
- **Protocole :** contient un code numérique définissant le protocole transporté.
- **Somme de contrôle :** la même somme de contrôle que celle de IP portant sur l'entête GRE et le paquet transporté (si le bit c est à 1).

- **Conclusion:** Un protocole très simple
  - Utilisé avec les tunnels L2TP ('Layer 2 Tunneling Protoclol').
  - Peut être remplacé par l'obtention d'un code type protocole en IP.

Protocoles de tunnelage avec sécurité : VPN en mode tunnel

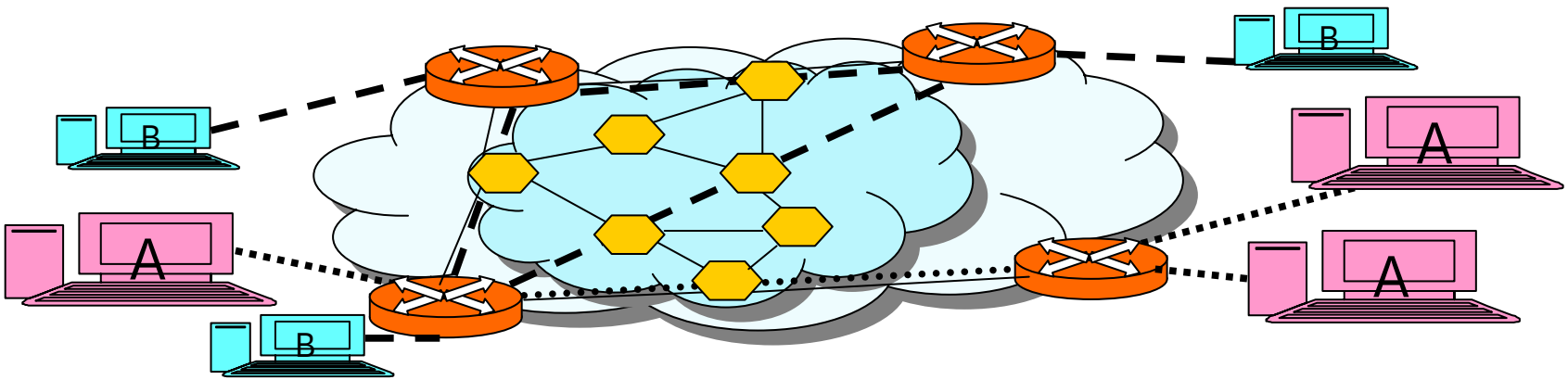
- **Pour construire une approche VPN en mode tunnel :**
  - **Partir d'un protocole de tunnelage** : GRE avec si nécessaire un protocole d'extension donnant de nouvelles fonctions.
  - **Parmi ces nouvelles fonctions :**
  - Introduire des fonctions de sécurité (authentification, confidentialité , intégrité ...).
  - Transformant des protocoles transporteurs et transportés non sécurisés en un ensemble sécurisé.
  - On parle alors de **tunnel sécurisé**, **VPN en mode tunnel**, **'Secure VPN'.**

Exemples de protocoles de tunnelage avec sécurité VPN

- **1 VPN Tunnels de niveau liaison** en point à point.
  - **L2F :** 'Layer Two Forwarding' (RFC 2341) Cisco (obsolete).
  - **PPTP :** 'Point to Point Tunneling Protocol' (RFC 2637) Microsoft.
  - **L2TP :** 'Layer 2 Tunneling Protocol' (RFC 2661) Cisco.
- **2 VPN Tunnels de niveau réseau.**
  - **Tunnels VPN à recouvrement** (« overlay ») en circuits virtuels.
    - Tunnels sur réseaux ATM ou relais de trame.
  - **IPSEC :** 'IP Security'
    - Deux modes : Transport = sécurisation , Tunnel = IP sur IP.
- **3 VPN Tunnels de niveau transport.**
  - **Sécurisation** de niveau transport utilisable en mode tunnel : SSL 'Secure Socket Layer'
  - Exemple de tunnel : IP sur SSL
- **4 VPN Tunnels de niveau application.**
  - **IP sur SSH** (**S**ecure **SH**ell), **PPP sur SSH**, **IP sur HTTPS**

Cas des VPN à recouvrement ('VPN Overlay')

- **1) Solution considérée encore comme des VPN, VPN 'overlay' réalisés par un niveau 2 (L2VPN) :** des accès externes prennent en charge le trafic et l'acheminent au moyen d'un réseau sous-jacent considéré comme de niveau liaison (point à point ou réseaux à circuits virtuels X25, ATM, FR, MPLS).



- **2) Utilisation de circuits virtuels permanents PVC ou commutés SVC pour interconnecter des points d'accès (routeurs) => d'où l'idée d'overlay.**
  - **VPN également baptisés en anglais: 'cut through'** = coupe à travers ('travel across'/'pass over').
  - **Un peu un abus de langage** si aucun mécanisme précis de protection (contrôle d'accès), confidentialité, authentification n'est développé => cependant il faut gérer les adresses, le mode multipoint, l'encapsulation, ... (en fait un tunnel sans sécurité).
  - **Exemple :** Transport de Lan (trames Ethernet), PPP, ATM, FR, FC, ...avec MPLS PWE3 (Pseudo Wire Emulation Edge to Edge) et VPLS (Virtual Private LAN Services).

Protocoles de sécurité

Protocoles de sécurité et VPN au niveau liaison

Protocoles de sécurité

VPN de niveau liaison

Protocoles de sécurité

Protocoles de sécurité associés au niveau liaison

Introduction

I Protocoles de confidentialité de niveau liaison.

II Protocoles d'authentification de niveau liaison.

Sécurité au niveau liaison : Introduction

- **Définition de base des protocoles de liaison :** aucune sécurité
- **Besoins qui s'expriment au niveau liaison:**
  - **Essentiellement : Contrôle d'accès à des réseaux.**
    - Réseaux d'entreprise devant protéger leurs accès
    - Fournisseurs de transport de données (FAI) offrant un service payant.
  - **Echange de données protégées en confidentialité.**
  - **Plus rarement : contrôle d'intégrité (plutôt réseaux locaux)**
- **Réseau pratiquement le seul considéré : Internet**
  - **Les protocoles de liaison concernés sont PPP et réseaux locaux.**
- **Principal problème traité: authentification des usagers** (autorisation des accès pour les services offerts par l'Internet).
  - **Authentification au moment de l'accès au réseau Internet:** protocoles en cause niveau liaison (PPP, Ethernet, Wifi).
- **Autre problème traité : confidentialité.**

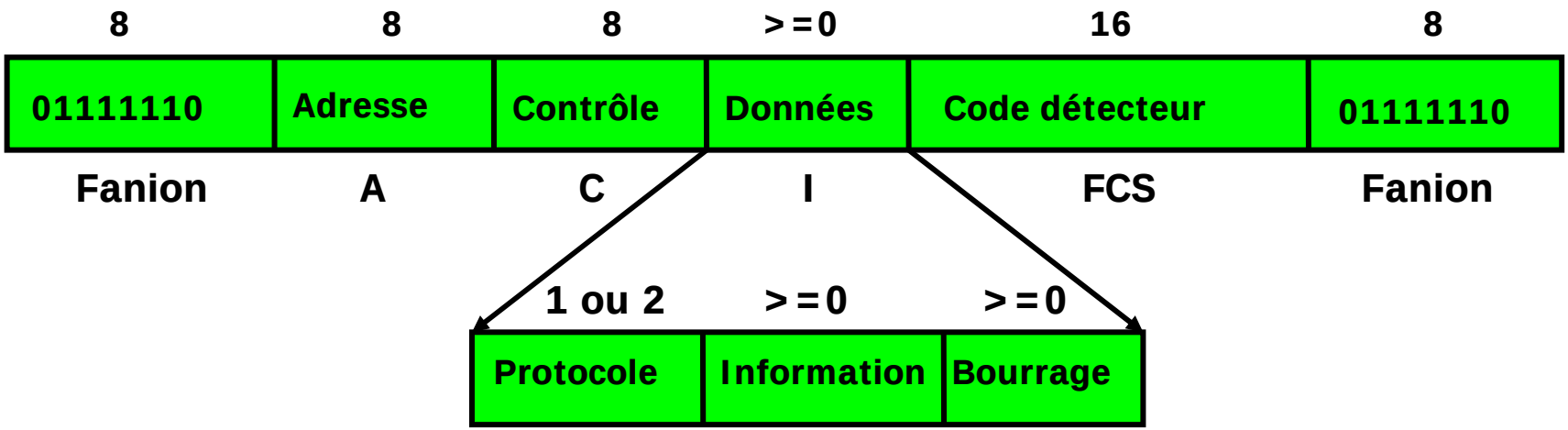
Rappels : le protocole PPP

- **Mode de base:** le plus répandu (‘PPP in HDLC Framing’)
  - Délimitation des trames.
  - Détection d’erreurs et destruction silencieuse.
- **Protocole de contrôle de liaison** : LCP

  ‘Link Control Protocol’ protocole de mise en connexion avec négociation, tests, fermeture de connexion.
- **Protocoles NCP :** ‘Network Control Protocols’ pour supporter des fonctions de niveau 3
  - Exemple IPCP Internet : distribution d’adresses IP.

Format des trames PPP

- **PPP** protocole support d'extensions d'authentification, de confidentialité.
- **Trames de sécurités incluses dans des trames PPP** (format type HDLC).



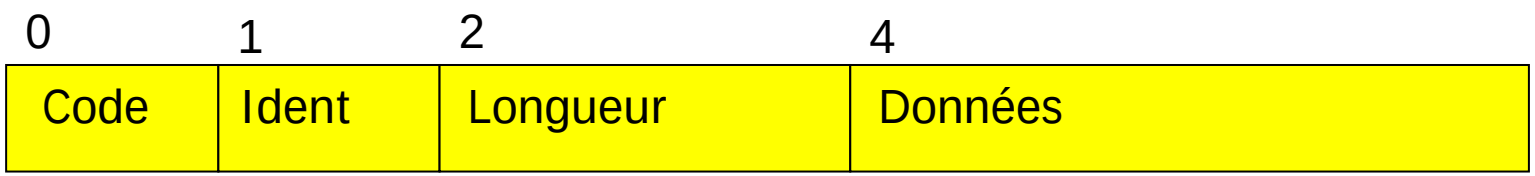
- **Zone protocole:** permet de le multiplexage de différents flots de messages associés à des protocoles différents associés à PPP (suite des protocoles PPP).

Exemples de codes :

IP	0x0021
LCP	0xC021
PAP	0xC023
CHAP	0x0223
MPPE	0x00FD

Rappel : Protocole LCP ‘Link Control Protocol’

- **LCP est la partie contrôle de liaison PPP: gestion de connexion, authentification …**
- **Le format des trames LCP est utilisé pour LCP mais aussi pour les protocoles de sécurité**
  - La partie données d’une trame PPP dans le cas LCP.
  - Format des trames PAP, CHAP mais aussi format des messages RADIUS.



- **Code (‘Code’)**
  Sur un octet le type d’un message LCP.
- **Identificateur (‘ Identifier’)**
  Sur un octet il permet d’associer les requêtes et les réponses.
- **Longueur (‘Length’)**
  Sur deux octets, la longueur totale des infos LCP incluant le code, l ‘identificateur et la donnée.
- **Données (‘Data’)**
  La zone données est vide ou son format de la zone est défini par le code. Elle est généralement composée d’attributs (de variables transportées) selon une représentation classique type, longueur, valeur (attributs typiques un nom d’usager, un mot de passe …).

Protocoles de sécurité associés au niveau liaison

Protocoles de confidentialité

1 Protocoles associé à PPP
- **DESE , 3DESE**
- **Microsoft MPPE**

2 Protocoles avec les réseaux locaux

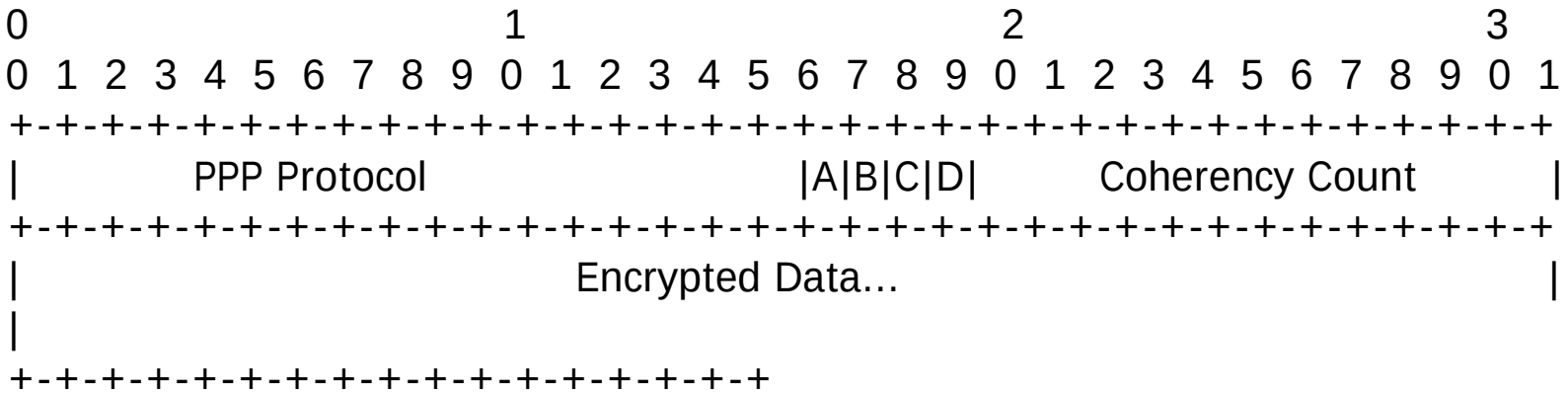
1 Confidentialité basée sur le DES
DESE : PPP DES Encryption Protocol

- **Cadre général :** le protocole ECP Encryption Control Protocol qui permet de sélectionner en PPP une méthode de chiffrement (RFC 1968 juin 1996)
- **Chiffrement en DES** : **DESE (DES E**ncryption**)**
  - Version 2 RFC 2419 (septembre 1998) : type = 3 (Version 1 RFC 1969 type=0, obsolete)
- **DESE** : Solution de type CBC Cipher Block Chaining
    - $C[i] = DES (P[i] \oplus C[i-1])$
- **Vecteur d'initialisation C[1] :** un nonce transmis en clair.
- **Autres caractéristiques**
  - **Règle de bourrage :** pour alignement blocs de 8 octets pour le DES.
  - **Numéro de séquence :** pour le décodage en cas de perte de trame.
- **Autre protocole** : 3DESE RFC 2420 basé sur 3DES (type =2)

2 Confidentialité basée sur RC4 : MPPE Microsoft Point to Point Encryption

- **MPPE :** RFC 3078 (mars 2001).
- **Voisin de la confidentialité Wifi WEP** :
  - **Chiffre RC4** (de RSA Security).
  - **Correction de défauts** du WEP.
- **Longueur de clé privée négociable :** choix possibles 40 ou 128 bits.
- **La clé RC4 MPPE est changée fréquemment :**
  - La fréquence de changement dépend d'une négociation (la clé change éventuellement pour chaque trame).

Format de la trame MPPE



- **Protocole : 0x00FD** Valeur figurant pour la confidentialité MPPE après la phase de négociation PPP (négociant également la compression).
- **Bit A :** tables RC4 réinitialisée avant la transmission de la trame (donc le destinataire doit réinitialiser pour déchiffrer).
- **Bits B, C :** inutilisés.
- **Bit D :** indique une trame chiffrée ou en clair.
- **Coherency Count** : un numéro de séquence qui permet de conserver la synchronisation sur la clé utilisée (changements fréquents de clé).
- **Encrypted data:** La charge utile chiffrée.

Changement de clé en MPPE

- **Problème de la réutilisation de la même clé en RC4 sur une donnée :** le chiffre est cassé.
- **MPPE : une méthode pour générer des clés** successives en utilisant un hachage itéré (hachage utilisé SHA).
- **StartKey** est la première clé utilisée (clé d'origine).
- **SessionKey** est la nouvelle clé secrète utilisée pour générer la clé RC4 à chaque changement de clé.
- **InterimKey** est une clé temporaire pour chiffrer une phase de trafic.
- **La table du chiffre RC4** est réinitialisée à partir de InterimKey:

  rc4_key(RC4Key, Length_Of_Key, InterimKey)
- **La nouvelle clé secrète** sessionKey est obtenue par chiffrement RC4 de InterimKey:

  SessionKey = rc4(RC4Key, Length_Of_Key, InterimKey)

Changement de clé en MPPE algorithme de calcul de la nouvelle clé

- void GetNewKeyFromSHA(IN unsigned char *StartKey, IN unsigned char *SessionKey, IN unsigned long SessionKeyLength OUT unsigned char *InterimKey)

```
{
unsigned char Digest[20]; ZeroMemory(Digest, 20);
SHAInit(Context);
SHAUpdate(Context, StartKey, SessionKeyLength);
SHAUpdate(Context, SHApad1, 40);
SHAUpdate(Context, SessionKey, SessionKeyLength);
SHAUpdate(Context, SHApad2, 40);
SHAFinal(Context, Digest);
MoveMemory(InterimKey, Digest, SessionKeyLength);
}
```

- SHAInit(), SHAUpdate() and SHAFinal() sont des procédures de calcul de SHA Secure Hash Algorithm (initialisation, calcul, terminaison)

Confidentialité au niveau liaison dans les réseaux locaux

- **Essentiellement réseaux locaux sans fils WIFI**.
- **Versions successives** : WEP , WPA, WPA2

- **Solutions traitées dans le cours** sur la sécurité du WIFI.

Protocoles de sécurité associés au niveau liaison

Protocoles d'authentification

1 Protocoles de base PAP/CHAP

Protocole PAP 'Password Authentication Protocol'

Protocole CHAP 'CHallenge Authentication Protocol'

2 Protocole RADIUS

'Remote Authentication Dial-In User Service'

3 Protocole TACACS

'Terminal Access Controller Access Control System'

4 La famille des protocoles EAP

'Extensible Authentication Protocol'

Protocoles d'authentification

1 Protocoles de base

Protocole PAP 'Password Authentication Protocol'

Protocole CHAP 'CHallenge Authentication Protocol'

PAP : 'Password Authentication Protocol'

- **PAP - RFC 1334 Octobre 1992 : un protocole d'authentification simpliste :** authentification à mots de passe en clair sur le réseau.

- **Protocole:**
  - **Types de trames PAP**
    1 Authenticate-Request
    2 Authenticate-Ack
    3 Authenticate-Nak
  - Emission par le demandeur d'un **Authenticate_request** avec un attribut **mot de passe en clair**.
  - Acceptation du site distant par **Authenticate_ack** (mot de passe **correct)**.
  - Rejet par **Authenticate_nak** (mot de passe **incorrect**).

- **Très faible sécurité de la circulation des mots de passe en clair compte tenu de la nature du réseau Internet.**

- **Variante propriétaire : SPAP '**Shiva Password Authentication Protocol'
  - **PAP** sans améliorations très significatives.

CHAP : ‘CHallenge Authentication Protocol’

- **CHAP** (RFC 1994 Aout 1996) : un protocole d’authentification à mots de passe qui **améliore** la sécurité du protocole PAP en échangeant **les mots de passe chiffrés** sur le réseau.
- **Principe général : protocole avec défi ‘challenge’**
  - **B s’authentifie auprès de A**
  - **Un message "challenge"** est émis par A vers B qui s’authentifie.
  - **Ce message comporte un nonce** c’est à dire une valeur dans l’idéal imprévisible et unique (par exemple dépendant du temps et d’un secret).
  - **B répond en envoyant le mot de passe et le nonce** haché au moyen d’un fonction de hachage à sens unique (MD5 par défaut).
  - **Le mot de passe doit être conservé en clair** sur A pour permettre la vérification (le calcul par A de la fonction de hachage).
  - **L’authentification étant correcte** : A renvoie une acceptation sinon un rejet.
- **Intégration PPP :**
  - CHAP type de protocole PPP : 0x0223 . Structure des trames LCP;

CHAP : Eléments du protocole

- **Types de messages utilisés**
  1 Challenge
  2 Response
  3 Success
  4 Failure
- **Message ‘Challenge’ : Principal attribut**
  - **Le défi ‘challenge’ (le nonce) :** une valeur aléatoire déterminée par le demandeur qui est imprévisible et unique.
- **Message ‘Response’ : Principaux attributs**
  - **A) Le nom d’usager**,
  - **B) le MD5 (16 octets de MD5) de la chaîne**

  Identificateur, Mot de passe secret, nonce (la valeur de challenge)
- **Messages ‘Success’ ou ‘Failure’**
  - Deux messages sans attributs (simplement typés) pour indiquer que la valeur reçue correspond à la valeur calculée ou non.

CHAP : Sécurité

- **CHAP résiste aux écoutes** des mots de passe (‘sniffing’).
- **CHAP résiste aux attaques de répétition**.
- **CHAP ne résiste pas** à une écoute puis attaque à dictionnaire.
- **CHAP est incapable de résister à toute attaque de type insertion** d’un programme dans le flot des échanges qui peut aussi modifier les messages (‘active wiretapping’, ‘spoofing’).
- **CHAP est peu pratique pour une utilisation distribuée**
  - **Obligation de stocker les mots de passe en clair.**
  - **Le service d’authentification doit être réalisé dans tous les points d’accès** à un réseau (NAS, routeurs ...) **=> Améliorations nécessaires.**
- **Variante propriétaire ARAP**
  - **ARAP ‘**Appletalk Remote Access Protocol’
  - Protocole bidirectionnel (Authentification mutuelle client serveur)
  - Avec challenge/réponse utilisant le DES pour le hachage.
- **Variante propriétaire MS-CHAP (‘**MicroSoft CHAP’)

Authentification MS-CHAP

- **MS-CHAP V1 RFC 2433 Microsoft PPP CHAP Extensions**
  - Pour éviter de stocker le fichier des mots de passe en clairs sur le serveur CHAP on transmet aussi un hachage (selon une méthode propriétaire) du mot de passe.
  - Le haché est comparé à un fichier de mots de passe hachés.
  - Problème: faiblesse de la fonction de hachage retenue par Microsoft.
- **MS-CHAP V2 RFC 2759 Janvier 2000 Microsoft PPP CHAP Extensions V2**
  - Correction des faiblesses de sécurité du hachage.
  - Utilisation d'une valeur aléatoire à hacher avec le mot de passe.
  - Réalisation d'une authentification mutuelle (dans les deux sens client serveur et serveur client).
  - Abandon de la transmission directe du mot de passe haché.
  - Possibilité : attaque force brute/à dictionnaire.

Scénario d'échange avec MS-CHAP V2

- **Demande_serveur_client** : vérification_d'authentification avec identifiant_de_session, chaîne_aléatoire1 (cad un nonce1)
- **Réponse_client_serveur :** nom d'utilisateur, haché (chaîne_aléatoire1 , identifiant_de session, mot_de_passe), chaîne_aléatoire2) (cad un nonce2)
- **Authentification du client :** vérification par le serveur de la réponse du client.
- **Réponse_serveur_client :** succès ou d'échec , haché(chaîne_aléatoire2, la réponse hachée du client, mot de passe).
- **Authentification du serveur :** vérification par le client de la réponse du serveur.
- **En cas de succès début des échanges.**

Protocoles d'authentification associés au niveau liaison

2 Protocole RADIUS

Remote Authentication Dial-In User Service

Radius : Généralités

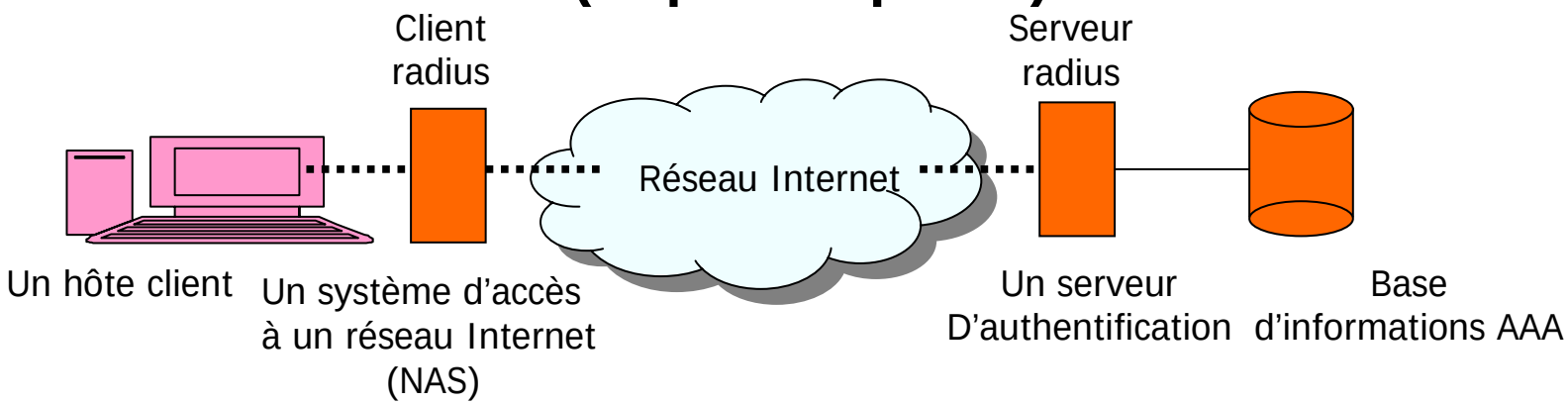
- **Radius 'Remote Authentication Dial In User Service':** Société Linvingston donné à la communauté Internet : **RFC 2138 (1997) dernière version RFC 2865 (2000)**

Objectifs poursuivis

- **1- Proposer une approche centralisée de l'authentification**
  => Solution souhaitée dans de nombreux cas (prestataires d'accès...)
- **2- Proposer une authentification à mot de passe originale** (propre à RADIUS) mais proposer aussi de pouvoir utiliser plusieurs autres méthodes existantes au choix (PAP, CHAP, Kerberos ....).
  => On peut ainsi choisir un protocole plus ou moins sûr.
- **3- Etendre les fonctions d'authentification** à des fonctions plus larges **AAA**
  - **'Authentication' :** Vérification d'identité
  - **'Authorization' :** Contrôle des droits
  - **'Accounting' :** Comptabilité

Le client – serveur radius

Radius fonctionnement client-serveur (requête réponse)



- **Client Radius** : a priori un serveur d'accès à Internet ou à un service Internet au niveau liaison PPP.
  - Cas le plus fréquent : le client RADIUS est un serveur de communication **NAS** '**N**etwork **A**ccess **S**erver'
  - Egalement possible un routeur ou un pare_feu ou une application nécessitant une authentification: telnet, rlogin
- **Serveur Radius** : un site centralisé implantant le service AAA.
  - Un serveur RADIUS peut agir comme un proxy client pour un autre serveur RADIUS.

Principes généraux Radius

- **Principes de sécurité**
  - **Les échanges RADIUS sont sécurisés par une clé secrète partagée** entre client et serveur, qui ne circule sur le réseau que hachée.
  - **Les usagers sont authentifiés par un mot de passe** qui ne circule sur le réseau que haché.
- **Protocole extensible**
  - **Tous les échanges utilisent des attributs typés :** syntaxe de transferts type, longueur, valeur.
  - **De nouveaux attributs peuvent être ajoutés** sans modifier l'existant.
  - **Mécanismes d'authentification variés :** dans le cadre RADIUS on peut utiliser PPP/**PAP**, PPP/**CHAP**, UNIX/**login** (local ou NIS), ou d'autres authentifications (**Kerberos**).

Acheminement des messages Radius

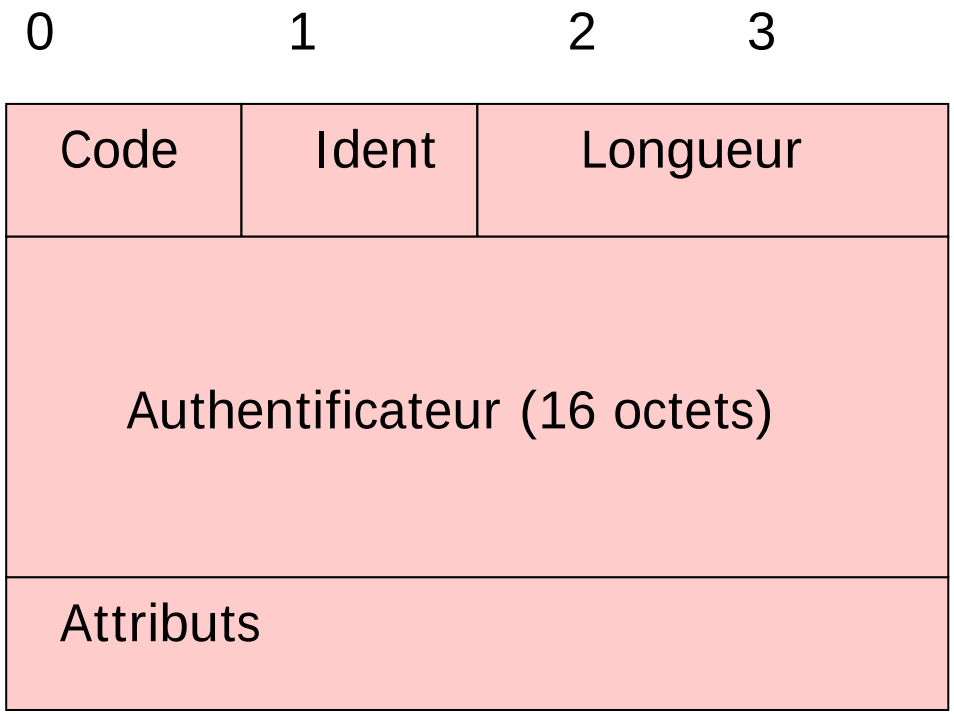
- **Utilisation d'un transport Internet**
  - Un seul serveur Radius par réseau.
  - Besoin d'acheminement des messages RADIUS entre clients et serveur Radius très éloignés.
  - Utilisation naturelle de l'infrastructure **Internet au niveau transport**.
- **Choix de UDP**
  - UDP est plus rapide.
  - Le protocole Radius est sans état 'stateless'.
  - UDP simplifie l'implantation du serveur.

  => Chaque message RADIUS est encapsulé dans la zone donnée d'un segment UDP (port numéro 1812).

Tolérance aux pannes en Radius

- **Tolérer les pertes de messages avec UDP**
  - Conservation d'une copie des messages et utilisation de temporisateurs de retransmission.
- **Tolérance à la panne du serveur Radius**
  - Mise en place d'une architecture en redondance passive de serveurs Radius.
  - Serveurs primaires et secondaires.
  - Si une requête vers le primaire échoue après quelques tentatives le secondaire est sollicité

Format des messages Radius



- **Code:** Identifie le type du message.

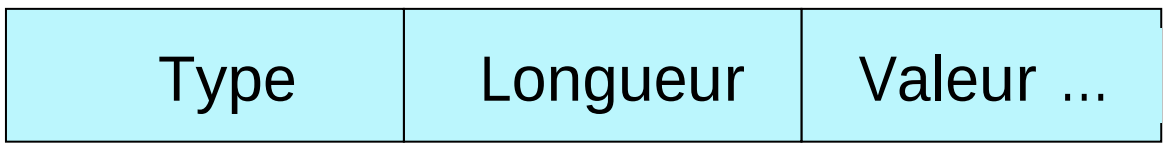
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

- **Identificateur ('identifier') :** associe requêtes et réponses (un octet).
- **Longueur ('length') :** longueur de toutes les zones données (deux octets).

Informations importantes des messages Radius

- **Authentificateur (‘Authenticator’):** utilisé pour authentifier la réponse du serveur et pour protèger les mots de passe (nonce) (16 octets).

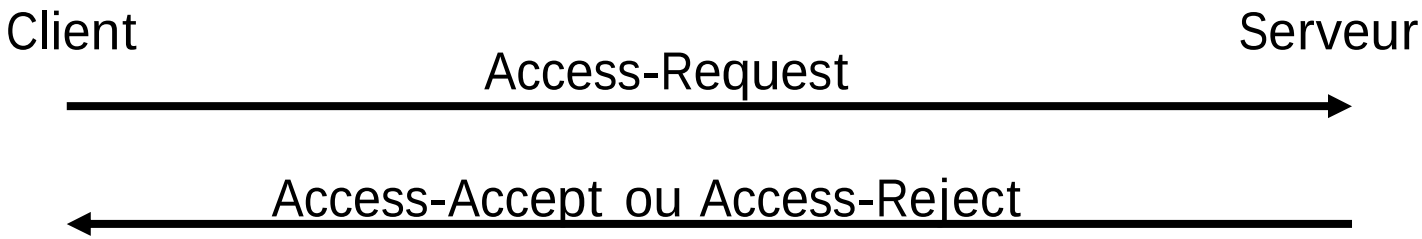
- **Attributs (‘Attributes’):** format (type, longueur, valeur) utilisés pour véhiculer toutes les informations nécessaires.



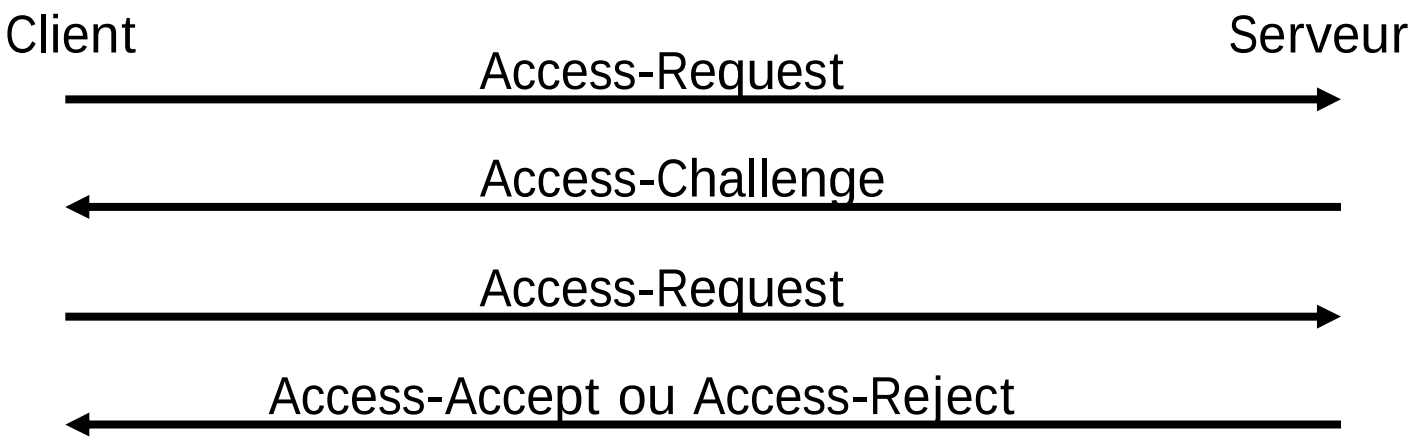
1 User-Name
2 User-Password
3 CHAP-Password
4 NAS-IP-Address
5 NAS-Port
6 Service-Type
7 Framed-Protocol
8 Framed-IP-Addres
9 Framed-IP-Netmask
10 Framed-Routing
11 Filter-Id
12 Framed-MTU
13 Framed-Compression
14 Login-IP-Host
15 Login-Service
16 Login-TCP-Port
17 (unassigned)
18 Reply-Message
19 Callback-Number
20 Callback-Id
21 (unassigned)
22 Framed-Route
23 Framed-IPX-Network
24 State
25 Class
26 Vendor-Specific

Les échanges de messages Radius en authentification

- **Version de base**



- **Version complète**



Authentification simple: Message Access-Request

- **Deux attributs principaux :**
  - **Attribut de type nom d'usager** : pour identifier l'usager.
  - **Attribut de type mot de passe** : contient le mot de passe usager protégé par :

    MD5 (secret , authentificateur) **XOR** Mot_de_passe
  - **MD5** : **fonction de hachage à sens unique** pour créer un MAC de 16 octets.
  - **XOR** : **ou exclusif avec le mot de passe** de 16 octets (cas particulier pour les mots de passe de plus de 16 octets)
- **Sécurité : le serveur vérifie la connaissance du secret et du mot de passe**
  - **Seul un client autorisé connaît le secret**.
  - **L'authentificateur introduit de la variabilité /** entropie dans MD5.
  - **MD5 protège le secret**.
  - **XOR ou exclusif** avec un nombre aléatoire protège le mot de passe.

Authentification complète: Message Access-Challenge

- **L'authentification complète avec challenge du client vis à vis du serveur RADIUS**
  - Une authentification **renforcée.**
  - Exemple de la norme : pour l'utilisation d'une carte à puce.
- **Message Access-Challenge**
  - **Comporte un authentificateur de réponse** : il permet l'authentification du serveur vis-à-vis du client.
  - **Un attribut type** '**state**' contient une chaîne binaire définie à la discrétion du serveur (un nonce, le challenge).
  - **Un attribut type** '**reply_messag**e' contient une chaîne une chaîne de caractère explicative.

Authentification complète: Vérification par le serveur

- **A la réception de ‘access-challenge’ :** le client doit répondre par ‘access-request’ comme dans la première transmission avec:
  - **un nouvel identificateur**
  - **un nouvel authentificateur**
  - **la chaîne binaire fournie par l’attribut state doit être ajoutée au mot de passe.**
- **A la réception de ‘access-request’ :**
  - un calcul identique à celui de l’access-request simple est effectué par le serveur.
  - qui accepte ou rejette la demande d’authentification par ‘access-accept’ ou ‘access-reject’.

Authentification du serveur par rapport au client

- **Dans les messages Access-Accept, Access-Reject, Access-Challenge :** présence du champ authentificateur calculé comme un authentificateur de réponse.
- **Valeur du 'Response Authenticator'**
  - **MD5** (Code , Identificateur, Longueur, Authentificateur requête, Attributs de la réponse ,Secret partagé).
  - **Ce hachage calculé par le serveur et vérifié par le client** permet d'authentifier le serveur qui est le seul à connaître le secret partagé.
  - **Les identificateurs et l'utilisation de l'authentificateur** contenu dans le précédent message access-request du client protègent des répétitions.

Protocole Radius : Conclusion

- **Protocole très largement utilisé**
  - Par les **prestataires d'accès Internet**.
  - Dans les **réseaux Intranet**.
  - Pour sa **gestion centralisée des informations AAA.**
- **Très nombreuses fonctions d'administration, de configuration ou de comptabilité :**
  - **Associées à la possibilité d'échanger** un grand nombre d'attributs par exemple des certificats.
  - **Fourniture d'adresse IP** par un serveur centralisé.
  - **Gestion d'informations comptables** en vue de la facturation (temps de connexion).
- **RADIUS n'est plus de niveau liaison**
  - **Activé au niveau liaison** avec des formats de message de liaison.
  - **RADIUS utilise UDP** et est en fait un protocole d'application.
- **Pour fonctionner un client RADIUS doit déjà avoir accès au réseau.**

Protocoles d'authentification associés au niveau liaison

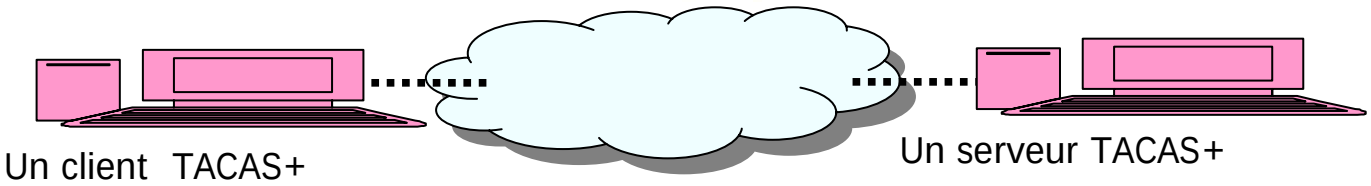
3 Protocoles TACACS
TACACS, XTACACS, TACACS+

Terminal Access Controller Access Control System

Introduction TACACS

- **Tacacs se place sur le même créneau que RADIUS.**
  - Authentification **centralisée.**
  - Fonctions **AAA**
- **Tacacs est un protocole CISCO**
  - **Diffusion industrielle** liée aux produits CISCO.
- **Trois versions successives:**
  - **TACACS, XTACACS, TACACS+**
- **Dernière version TACAS+** => version d'actualité.
  - **Incompatible** avec les précédentes versions.
  - **Reprend de nombreux aspects** (les meilleurs aspects) de **Radius**.
  - Venant après RADIUS Tacacs+ peut proposer **des éléments d'amélioration.**

Un exemple d'échange avec le protocole TACACS+



START (authentication) : usager essayant de se connecter

REPLY (authentication) : demande de nom d'usager

CONTINUE (authentication) : réponse de nom d'usager

REPLY (authentication) : demande de mot de passe

CONTINUE (authentication) : fourniture du mot de passe

REPLY (authentication) : réussite ou échec de l'authentification

REQUEST (authorization) : usager demande accès au shell

RESPONSE (authorization) : statut de l'autorisation d'accès (oui ou non)

REQUEST (accounting) : début d'une session

RESPONSE (accounting) : acquittement début de session enregistré

..... Suite des requêtes réponse d'autorisation etc

REQUEST (accounting) : fin d'une session

RESPONSE (accounting) : acquittement fin de session enregistré

Conclusion TACACS+ : comparaison avec RADIUS

- **1) Méthodes très similaires au niveau sécurité.**
- **2) Mais TACACS+ utilise TCP** (RADIUS utilise UDP).
  - TACACS: meilleur contrôle d'erreur et meilleur gestion de congestion.
  - TACAS plus coûteux et plus lent.
- **3) TACACS+ encrypte toute la charge utile** des messages (tous les attributs) pas uniquement le mot de passe.
- **4) TACACS sépare les requête d'authentification** des requêtes d'autorisation ou de comptabilité
  - Radius mélange les attributs concernant les fonctions AAA dans les messages.

Protocoles d'authentification associés au niveau liaison

4 La famille des protocoles EAP ('Extensible Authentication Protocol')

1 EAP de base
2 EAPOL
3 EAP-MD5
4 LEAP
5 EAP-SIM
6 EAP-TLS
7 EAP TTLS
8 PEAP

Protocole EAP
Pourquoi une nouvelle solution

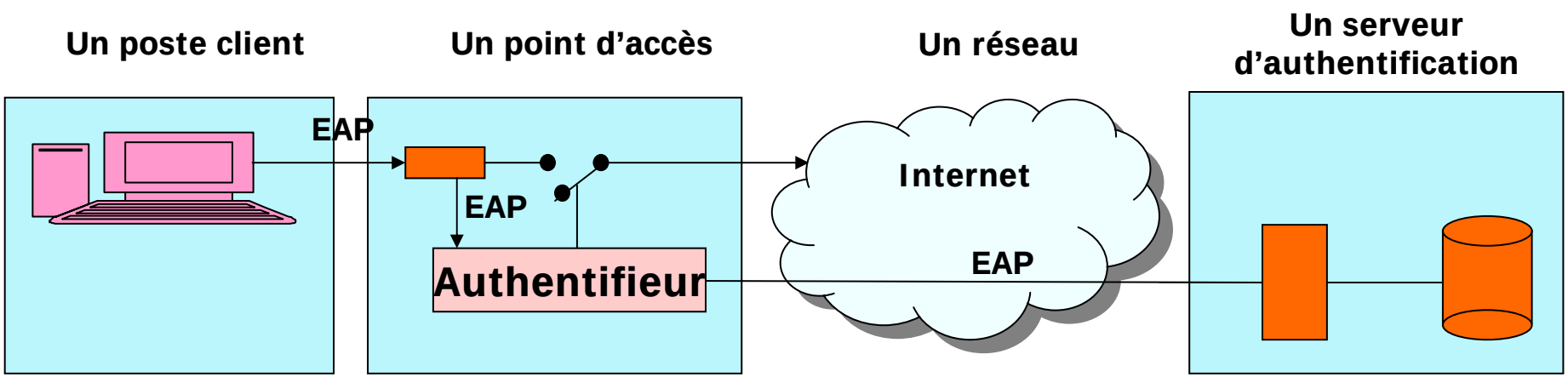
- **1) Rappel de l'évolution des points de vue sur l'authentification.**
  - 1) La génération des protocoles intégrés à PPP (PAP/CHAP): problème chaque point d'accès doit être un serveur d'authentification.
  - 2) La génération des protocoles d'accès à des serveurs d'authentification (RADIUS/TACACS).
- **2) EAP contrôle l'accès en PPP** d'un poste de travail à un réseau avec une approche à trois entités :
  - **Un client** : qui n'a pas encore l'accès au réseau et communique en PPP,
  - **Un point d'accès** : qui peut communiquer sur le réseau avec un serveur,
  - **Un serveur d'authentification** : connecté au réseau.
- **3) EAP: un protocole 'générique' pour supporter de très nombreuses variantes de protocoles d'authentification sans trop polluer PPP.**

Protocole EAP
Généralités

- **EAP: un canevas (‘framework’) pour récupérer toutes les solutions d’authentification désirées anciennes ou nouvelles.**
  - Solutions existantes (‘héritées’ ‘legacy’) : PAP/CHAP/MS-CHAP.
  - Solutions utilisant des matériels : cartes à puces ou clé USB ou cartes à jetons.
  - Mots de passe à usage unique : ‘One time passwords’ RFC 1760.
  - Authentification par clé publique : utilisant des certificats.
- **Plusieurs dizaines de versions de protocoles d’authentification déployés sous EAP.**
- **RFC 2284 mars 1998 : dernière version RFC 3748 juin 2004**
- **EAP et les réseaux locaux:** EAP d’abord défini dans le cadre de PPP est adapté aux réseaux locaux sous les références **IEEE 802.1x (EAPOL) .**

Protocole EAP
Organisation à trois entités

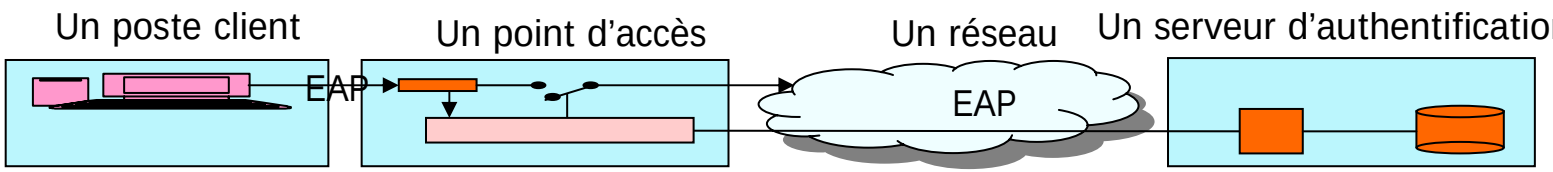
- **1) Le poste à authentifier (‘Supplicant’):** un poste client.
- **2) Le point d’accès (‘Authenticator’) :** un serveur d’accès réseau NAS, une borne Wifi AP, un routeur, un commutateur de réseau local ...)
- **3) Le serveur d’authentification (AS ‘Authentication Server’) :** typiquement un serveur RADIUS ou TACACS.



EAP : principes généraux

- **1) Quatre types de messages :** client/serveur
  - EAP-Request , EAP-Response, EAP-Success, EAP-Failure.
- **2) Messages qui servent uniquement :**
  - A acheminer des requêtes réponses dans un protocole client serveur.
  - A notifier une réussite ou un échec d'authentification.
- **3) EAP ne définit aucun mécanisme en propre d'authentification**
  - Les contenus des messages EAP sont des attributs 'transparents' .
  - On peut mettre des contenus d'un autre protocole (exemple un certificat sous la forme d'un attribut RADIUS).
- **4) Le plus important c'est d'atteindre une situation** ou après un échange de requêtes réponses on a un succès ou un échec utilisable par le point d'accès.

EAP : un échange type



Phase initiale
Echange d'identité

Request (EAP Début)

Request (Identité)

Response (Identité)

Response (identité)

Request (.....)

Phase principale
Echanges de données d'authentification

Request (.....)

Response (.....)

Response (.....)

.....

Success

Phase finale
Notification

Success

Protocole EAP sur réseaux locaux : EAPOL EAP Over Lans IEEE 802.1X

- **EAP défini à l'origine** : uniquement pour des liaisons PPP (accès réseau par modems, ADSL, liaisons spécialisées).
- **Objectif EAPOL :** transmettre des messages EAP sur des réseaux locaux (filaires Ethernet ou sans fil Wifi) pour supporter tous les protocoles d'authentification EAP sur LAN.
- **EAPOL définit un nouveau type de protocole :** champ type de la trame IEEE 802 Ethernet pour que les 4 messages EAP puissent être transmis sur réseau local.
- **Normalisation dans les réseaux locaux :** IEEE 802.1X.
- **Utilisation EAPOL significative dans les réseaux WIFI :** normes de sécurité WPA Wireless Protected Access.

Protocole EAP-MD5

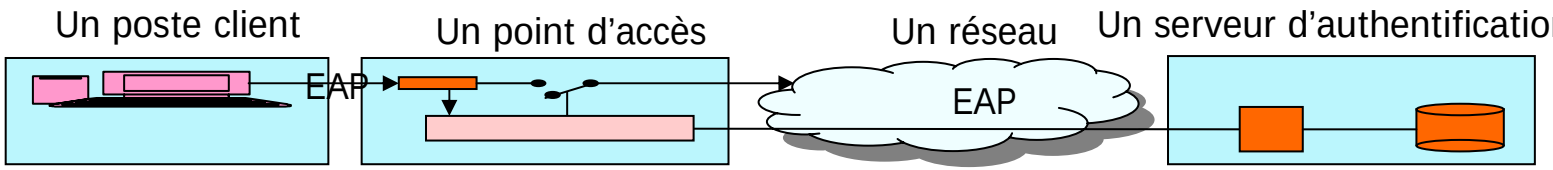
- **EAP-MD5:** la méthode d'authentification la plus basique transportée par EAP.
- **Très similaire à CHAP**.
  - Le serveur transmet un nonce (une valeur aléatoire de défi).
  - Le client concatène le mot de passe et le nonce et le hache en MD5. Retourne cette valeur au serveur.
  - Le serveur vérifie le hachage.
- **Solution sensible aux écoutes** du trafic suivie d'une attaque hors ligne par dictionnaire ou par force brute.

Protocole LEAP ‘Lightweight-EAP’

- **Solution Cisco:** pour améliorer la sécurité trop faible du WEP
- **Première implantation de EAP et 802.1X** pour réseaux sans fils.
- **Solution à mot de passe secret partagé basée sur MS-CHAP.**
- **On échange également une clé de session :** échange sécurisé par le secret partagé MS-CHAP.

- **Comme MS-CHAP** : ne résiste pas aux écoutes et attaque par dictionnaire ou force brute.

LEAP : scénario d'un échange



Phase initiale
Echange d'identité

Request (Identité) ← Request (Identité) ←

Response (Identité) → Response (Identité) →

S= défi aléatoire nonce

Phase principale
Echanges de données d'authentification
Du client

Request (S) ← Request (S) ←

Response (MS_CHAP(S,pw)) → Response (MS_CHAP(S,pw)) →

Success ← Success ←

C= défi aléatoire

Phase
D'authentification
du serveur et
d'échange de clé

Request (C) → Request (C) →

Response (MS_CHAP(c,pw)) ← Response (MS_CHAP(C,pw)) ←

Choix d'une clé A

Protocole EAP-SIM
EAP-Subscriber Identity Module

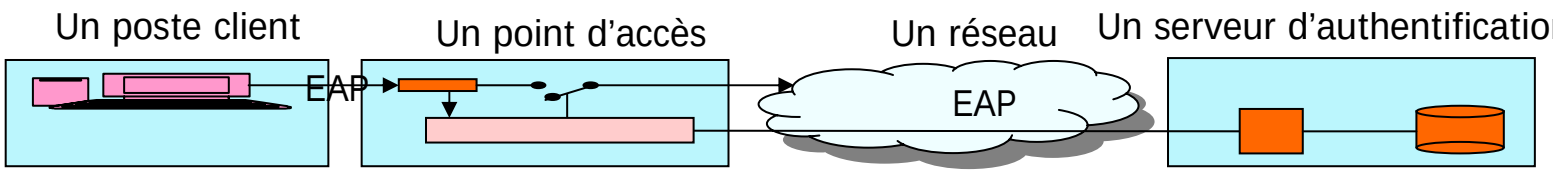
- **Utilisation d'une carte à puce.**
- **Protocole défini pour des téléphones GSM**

  => carte SIM des téléphones portables GSM
- **Utilisation possible également en WIFI**.
- **Authentification EAP-SIM** : différente de l'authentification GSM de base (protocoles A3-A5).
- **Utilisation du secret de la carte SIM** partagé avec le point d'accès pour une authentification challenge/réponse puis dérivation d'une clé de session.

Protocole EAP-TLS RFC 2716 (EAP-Transport Layer Security)

- **TLS Transport Layer Security (RFC 2246) définit une méthode d'authentification pour le niveau transport :**
  - Une méthode est basée sur les clés publiques.
  - Nécessité de certificats client et serveur.
  - Autres solutions possibles aussi (clés secrètes pré partagées).
- **Partie authentification de TLS et échange de clé de session :** portée sous EAP.
  - **Client et server s'authentifient mutuellement :**.
  - **Terminaison par l'échange de clé secrète de session :** notion de 'pre-master key' p et de master key .
- **Solution recommandée** pour un bon niveau de sécurité (à condition de vérifier les certificats).

Protocole EAP-TLS: un scénario de fonctionnement



Request (Random)

Générer c= random

Response (c)

Générer s= random

Request (s,certificat_serveur)

Générer p= random

Response (RSA_cle_publique_serveur(p), certificat_Client, signature_client)

Authentification du client

Request (TLS_finished, HASH (contenu_messages_précédents dont p))

Authentification du serveur

Response (TLS_finished)

Success

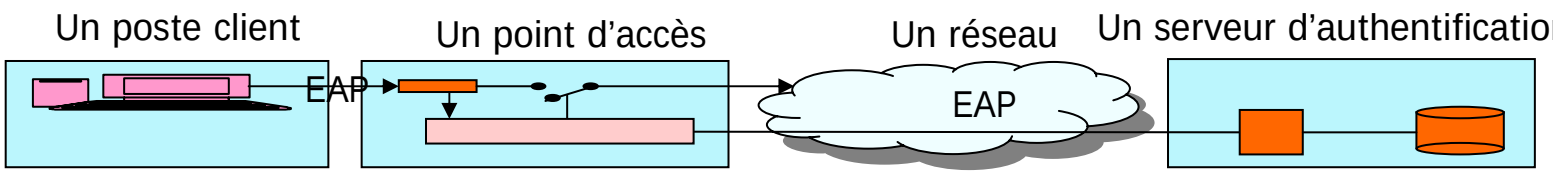
Success

Clé maitresse partagée HASH (c,s,p)

Protocole EAP-TTLS
EAP-Tunneled Transport Layer Security

- **Méthode utilisant le début du protocole TLS**.
- **Pour éviter d'avoir à gérer des certificats clients:** création d'une connexion TLS chiffrée en utilisant la clé publique serveur (les échanges EAP sont protégés par la clé de session échangée selon la méthode TLS).
- **Poursuite de l'authentification** : généralement par une méthode à mot de passe
  - **Liste des principales méthodes supportées en TTLS** : PAP, CHAP , MS-CHAP, MS-CHAPV2, EAP-MD5, EAP-GTC, EAP-TLS.
  - **EAP-GTC Generic Token Card** : RFC 2284 Une solution générale EAP pour transporter des infos d'authentification fournies par des cartes à jetons (token cards). Dans la pratique GTC achemine un couple usager:mot-de-passe.

Protocole EAP-TTLS: un scénario de fonctionnement



Request (Random)

Générer c= random

Response (c)

Générer s= random

Request (s,certificat_serveur)

Générer p= random

Response (RSA_cle_publique_serveur(p))

Clé maitresse partagée K= HASH (c,s,p)

Request (K (message_d_un_protocle_d_authentification))

Response (K (message_d_un_protocle_d_authentification))

Authentification du client

Success

Success

Protocole PEAP ‘Protected-EAP’

- **Solution propriètaire** très voisine de EAP-TTLS proposée par Microsoft, CISCO et RSA Security: se différencie surtout par le format des données transportées.
- **Comme EAP-TTLS** : utilisation de la clé publique serveur pour échanger une clé de session et chiffrer en confidentialité des échanges EAP.
- **Deux authentifications souvent citées** : PEAPv0/EAP-MSCHAPv2 , PEAPv1/EAP-GTC (mais sont aussi possibles EAP-MD5, EAP-SIM, EAP-TLS)
- **Utilisation de EAP-PEAP** dans le Wifi : standards WPA , WPA2 Wired Protected Access.

Conclusion EAP

- **EAP : un cadre** pour transporter tous les protocoles d'authentification connus au niveau liaison :
  - avec PPP sur liaison spécialisée.
  - ou sur réseau local EAPOL 802.1x.
- **Beaucoup de propositions** pour supporter toutes les solutions d'authentification connues.
- **Utilisation en croissance significative**.

Sécurité de niveau liaison/réseau et VPN

Protocoles de VPN de niveau liaison

1 Point to Point Tunneling Protocol (PPTP)

2 Layer 2 Tunneling Protocol (L2TP)

Non traité Layer 2 Forwarding (L2F)

VPN de niveau liaison

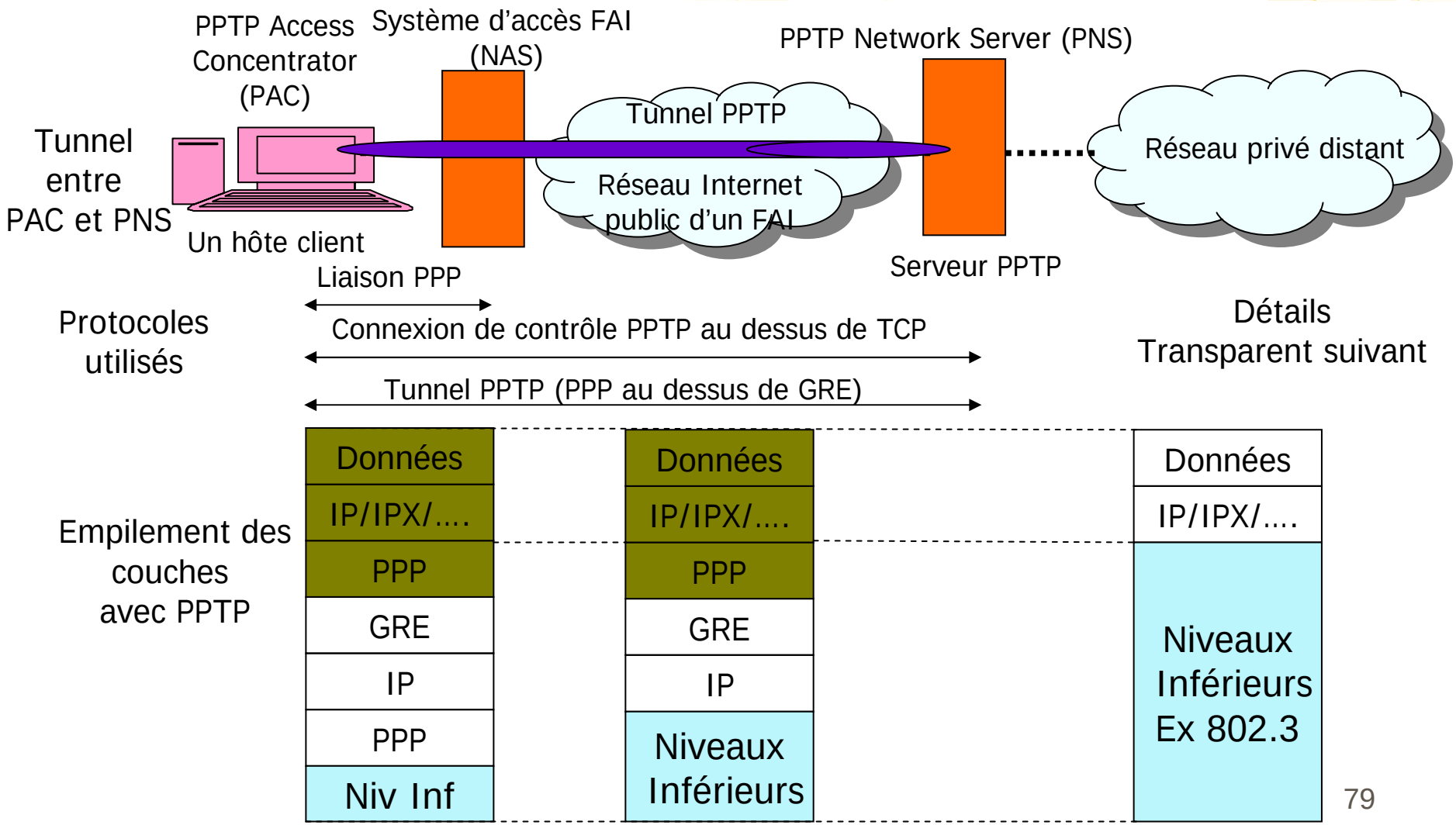
1) PPTP

‘Point to Point Tunneling Protocol’

PPTP : Introduction

- **1) Origine :** Consortium d'industriels avec Microsoft (architecture RAS Remote Access Service) mais aussi US Robotics/3COM, Ascend, etc ... **Norme :** RFC 2637 en 1999.
- **2) Objectif de base :** permettre d'acheminer des protocoles non Internet (NetBios, IPX, Appletalk...) sur un réseau Internet => encapsulation dans le protocole de liaison PPP.
- **3) Utilisation dans des communications en mode tunnel quelconques**: en fait pour les protocoles Internet IP sur PPP.
- **4) Construction de tunnels selon deux modes:**
  - **Volontaire ('Voluntary') :** le client décide de construire un tunnel jusqu'au serveur.
  - **Obligatoire ('Compulsory') :** le tunnel est imposé automatiquement.
- **5) Mise en œuvre de fonctions de sécurité** : authentification, confidentialité pour une approche VPN de niveau liaison.

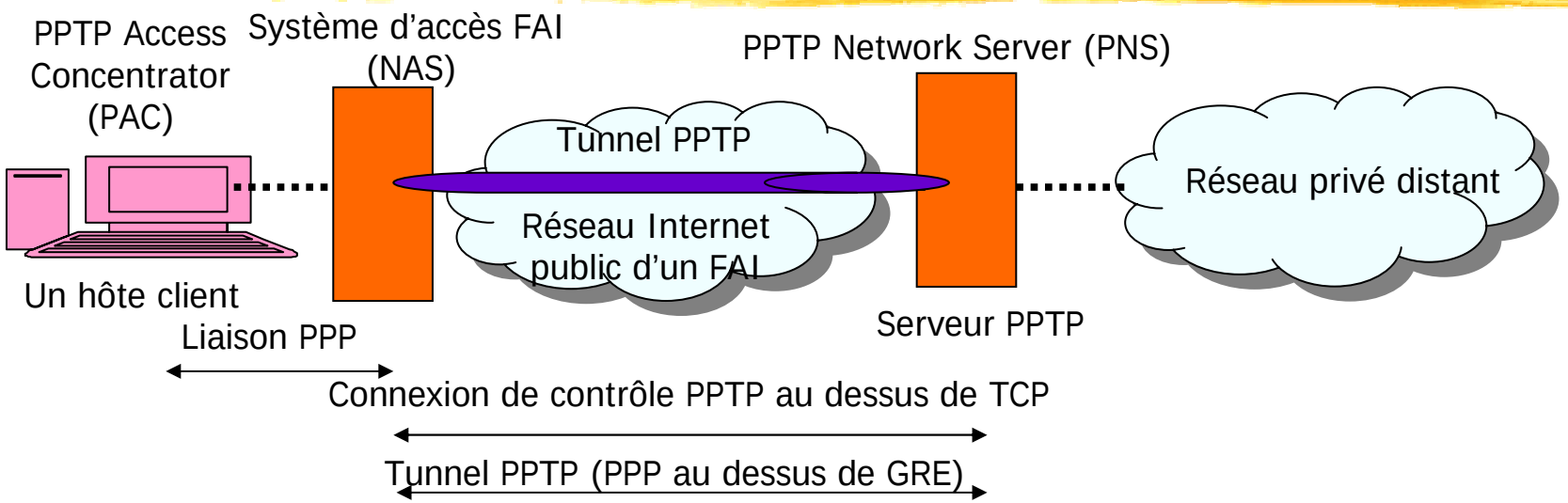
A) Architecture 'Volontaire' PPTP 'Voluntary Tunneling PPTP'

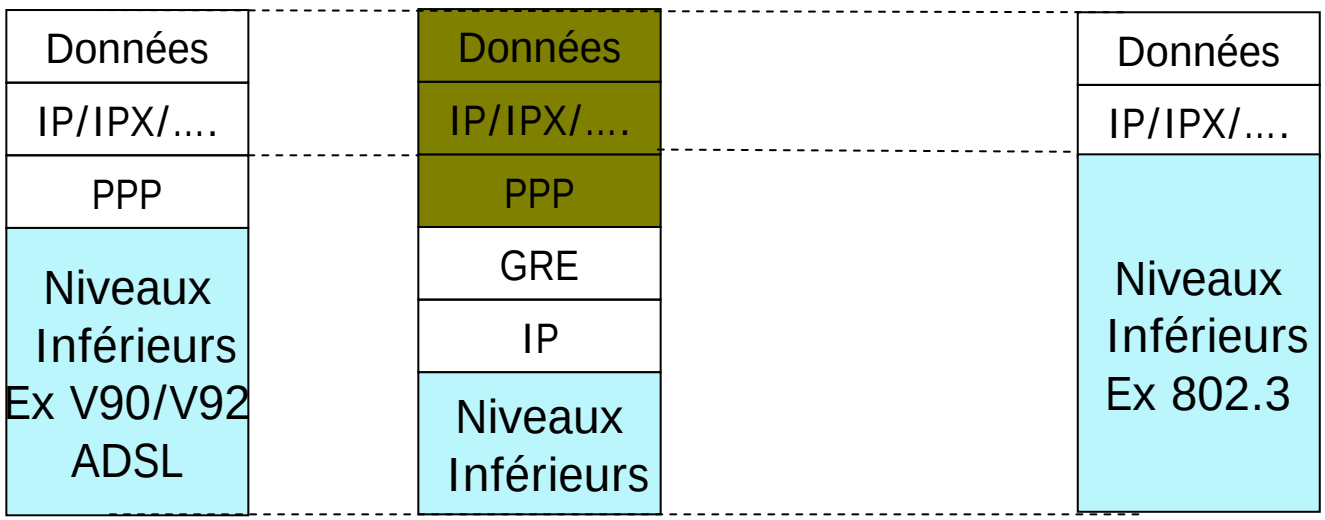


PPTP : Détails de fonctionnement en mode volontaire

- **1) Au début le client PPTP établit avec le NAS serveur d'accès une liaison PPP** : partie LCP Link Control Protocol de PPP.
- **2) Le client PPTP établit une connexion de transport TCP avec le serveur PPTP** (le PNS) : pour négocier les paramètres de fonctionnement du tunnel PPTP (notion de connexion de contrôle PPTP).
- **3) Le client PPTP peut alors fonctionner en mode tunnel** en utilisant le protocole GRE d'encapsulation.
- **4) Au dessus de GRE, le client et le serveur dialoguent en utilisant le protocole PPP, le lien PPP établi entre le client et le serveur :**
  - **Permet d'acheminer n'importe quel protocole de niveau 3** avec PPP comme protocole de niveau 2.
  - **Tout se passe comme s'il existait une liaison filaire** gérée en PPP entre le client PPTP et le serveur PPTP sans que le FAI n'ait à en connaître.

B) Architecture 'Obligatoire' PPTP 'Compulsory Tunneling PPTP'





PPTP : Aspects de Sécurité

- **1) Pas de définition particulière de sécurité** dans la RFC 2637 PPTP.
- **2) La RFC PPTP indique qu'on peut sécuriser** un tunnel PPTP est utilisant tous les protocoles de **sécurisation classiques des communications PPP.**
  - **Authentification** Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Extensible Authentication Protocol (EAP) avec par exemple EAP-TLS Transport Layer Security Protocol
  - **Confidentialité :** Encryption Control Protocol (ECP) pour négocier la confidentialité, PPP DES Encryption Protocol (DESE) ou PPP Triple DES (3DESE)

Exemple: suite de protocoles Microsoft

- **Authentification MS-CHAP 'Microsoft Challenge Authentication Protocol'**
  - En V2
- **Confidentialité MPPE 'Microsoft Point to Point Encryption'**
- **Autre possibilité : compression MPPC 'Microsoft Point to Point Compression'**

PPTP : Conclusion

- **1) PPTP transporte différents protocoles** : IP/IPX/NetBios.
- **2) Protocoles de sécurité :** les protocoles de sécurité du niveau liaison PPP => niveau de sécurité de moyen à bon en relation avec ces protocoles.
- **3) Utilisation de PPTP :** due aux difficultés de l'utilisation de IPSEC avec NAT (de même que tous les tunnels de liaison).
- **4) Limitations de PPTP**:
  - **Ne fonctionne que sur le réseau Internet.**
  - **Surcharges protocolaires liées aux choix d'encapsulation.**
  - **Surtout supporté en raison des implantations Microsoft.**
  - **Evolution vers le standard L2TP.**

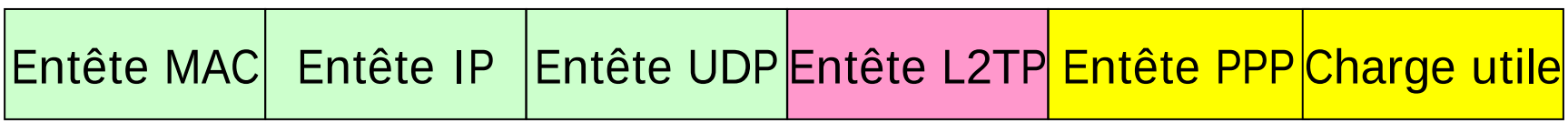
VPN de liaison

2) L2TP

‘Layer Two Tunneling Protocol’

L2TP : Introduction

- **RFC 2661 (1999) :** Support principal CISCO mais aussi Microsoft.
- **Dernière version** (mars 2005) (RFC 3931) : L2TP V3.
- **L2TP :** une amélioration des tunnels antérieurs PPTP/L2F.
- **L2TP construit des tunnels utilisables pour différents protocoles transportés et différents transporteurs:**
  - Le protocole transporté visé est surtout PPP (Point to Point Protocol)
  - Le protocole transporteur est surtout UDP/IP.



- **La meilleure sécurité L2TP est réalisée par IPSEC** : combinaison des deux protocoles sous le sigle L2TP/IPsec (RFC 3193 : 'Securing L2TP using IPsec').

L2TP : Notions associées

- **Extrémités d'un tunnel L2TP :**
  - **Client (initiateur de tunnel) :**

    LAC 'L2TP Access Concentrator'.
  - **Serveur (en attente d'ouverture de tunnels)** :
    LNS 'L2TP Network Server'.
- **Tunnels et session L2TP :**
  - Session : une communication identifiée pour des usagers de L2TP.
  - Tunnel : une communication sécurisée permettent de créer de multiples sessions à l'intérieur d'un même tunnel.
- **Types de messages dans un tunnel L2TP**
  - **Messages de contrôle L2TP** :
    - Protégés en contrôle d'erreur par L2TP.
  - **Messages de données du protocole transporté**:
    - Le contrôle d'erreur est celui du protocole transporté (souvent rien).

La sécurité en L2TP

- **1) Sécurité : aucune méthode en propre n'est définie.**

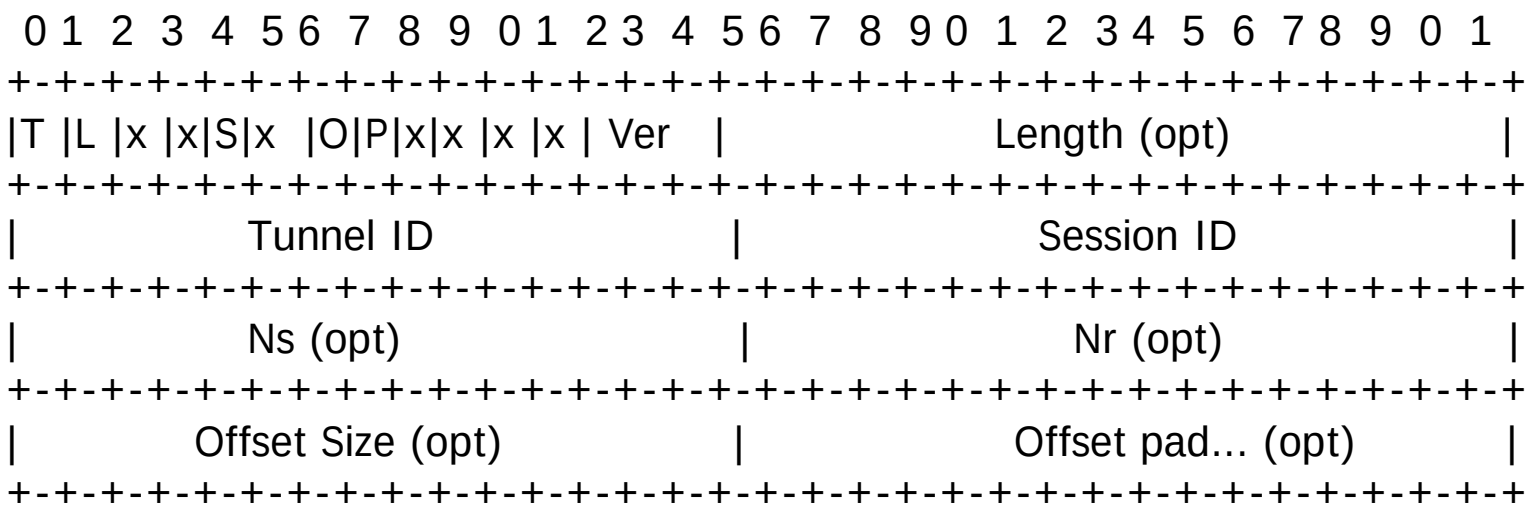
- **2) Confidentialité:**
  - Possibilité d'utiliser la confidentialité PPP (DESE, 3DESE, MPPE).
  - Recommandation RFC 3193: Utiliser IPSEC pour chiffrer le datagramme IP encapsulé.
- **3) Authentification**
  - Possibilité d'utiliser l'authentification autour de PPP (CHAP, EAP, RADIUS).
  - Recommandation RFC 3193: Utiliser IPSEC pour authentifier les entités communicantes avec le protocole de négociation IKE.

Comparaison PPTP / L2TP

- **Les deux protocoles:**
  - Utilisent PPP comme enveloppe initiale des données usager.
  - Étendent le modèle de la liaison PPP en autorisant des communications tunnelées sur un réseau public.
  - Fonctionnent selon les architectures volontaires et obligatoires (voluntary/compulsory tunneling).
- **Réseau sous jacent**
  - PPTP ne peut fonctionner que sur une architecture Internet.
  - L2TP peut fonctionner avec UDP/IP, Frame Relay, X.25 ou ATM.
- **Gestion des tunnels**
  - PPTP gère un seul tunnel entre deux points.
  - L2TP permet de créer des tunnels multiples (avec des identifiants) et a l'intérieur des tunnels des sessions différentes (pour supporter des qualités de service différentes).
- **Sécurité**
  - PPTP ne définit aucun mécanisme particulier.
  - L2TP définit une authentification des extrémités des tunnels au moyen des mécanismes de sécurité de IPSEC.

L2TP : Approfondissement Structure de l'entête en V2

- **L2TP définit un protocole d'encapsulation original:**



T : Le type du message. L : Indique que la longueur est présente. X : Réservé pour extensions.
S : Les numéros Nr et Ns sont présents. O: L'offset est présent. P : La priorité (1 priorité forte).
Ver : Numéro de version.
Length : Longueur totale du message.
Tunnel ID : Identificateur du tunnel.
Session ID : Identificateur d'une session particulière dans un tunnel.
Nr : Numéro de séquence du prochain message attendu.
Ns : Numéro de séquence du message.
Offset size et pad : Pointeur début des données après l'entête L2TP et pointeur début de bourrage.

L2TP : Conclusion

- 1) Protocole à utiliser actuellement pour construire des tunnels de niveau liaison.
- 2) Assez largement supporté en particulier par Microsoft et Cisco.
- 3) Bénéficie de la qualité des protocoles de sécurité IPSEC.
- 4) Sans poser de problèmes avec NAT
- 5) Surcharges protocolaires liés aux choix d'encapsulation.

L2TP : Liste des principales RFC

[RFC 2661] Layer Two Tunneling Protocol "L2TP". Defines L2TP version 2.
[RFC 2809] Implementation of L2TP Compulsory Tunneling via RADIUS.
[RFC 2888] Secure Remote Access with L2TP.
[RFC 3070] Layer Two Tunneling Protocol (L2TP) over Frame Relay.
[RFC 3145] L2TP Disconnect Cause Information.
[RFC 3193] Securing L2TP using IPsec.
[RFC 3301] Layer Two Tunnelling Protocol (L2TP): ATM access network extensions.
[RFC 3308] Layer Two Tunneling Protocol (L2TP): Differentiated Services Extension.
[RFC 3355] Layer Two Tunnelling Protocol (L2TP): Over ATM Adaptation Layer 5 (AAL5).
[RFC 3371] Layer Two Tunneling Protocol (L2TP): Management Information Base.
[RFC 3437] Layer-Two Tunneling Protocol Extensions for PPP Link Control Protocol Negotiation.
[RFC 3438] Layer Two Tunneling Protocol (L2TP): Internet Assigned Numbers Authority (IANA) Considerations Update.
[RFC 3573] Signaling of Modem-On-Hold status in Layer 2 Tunneling Protocol (L2TP).
[RFC 3817] Layer 2 Tunneling Protocol (L2TP): Active Discovery Relay for PPP over Ethernet (PPPoE).
[RFC 3931] Layer Two Tunneling Protocol - Version 3 (L2TPv3).
[RFC 4045] Extensions to Support Efficient Carrying of Multicast Traffic in Layer-2 Tunneling Protocol (L2TP).

Sécurité liaison/réseau et VPN

Sécurisation des communications au niveau Réseau en IP

IPSEC ‘IP SECurity’

Gérard Florin
- CNAM -
- Laboratoire CEDRIC -

Plan IPSEC

Introduction

I Protocoles de sécurisation: AH, ESP

II Protocoles d'échange de clés: IKE

Conclusion

Bibliographie

Sécurisation IP

Introduction

Objectifs de sécurité poursuivis par IPSEC

- **Application aux échanges en IP de mécanismes pour :**
  - **1) L'authentification des émetteurs des messages**
    - Utilisation de MAC (Message Authentication Codes)
  - **2) Le contrôle d'integrité des messages**
    - Utilisation de MAC.
  - **3) La confidentialité**
    - Pour un message utilisation d'un chiffre.
    - Pour les flots de messages confidentialité dans un tunnel.
  - **4) La détection des rejeux**
    - Utilisation de numéros de séquence.
  - **5) Le traitement des attaques par déni de service**
    - Mécanisme pour le rejet de certaines demandes.
  - **6) Optionnellement anonymat des communicants**
    - Chiffrement des identificateurs des communicants (adresses IP).

IPSEC : Normalisation

- **1) Travaux sur la sécurité IP :** début des années 1990.
- **2) RFC d'origine 1995 R. Atkinson:** RFC 1825 Architecture. Détails: RFC 1826 Authentication Header, RFC 1827 IP Encapsulating Security Payload.
- **3) Différentes RFC ultérieures précisant IPSEC : RFC 2401/2412 Novembre 1998** jusqu'à RFC 4308 Cryptographic Suites for IPSEC Décembre 2005.
- **4) En IPV4 : IPSEC fonctionnalité optionnelle.**
  - Très souvent disponible**.**
- **5) En IPV6 : IPSEC fonctionnalité obligatoire.**
  - Pas de différences fonctionnelles avec IPV4.
  - Une adaptation aux formats des messages et adresses IPV6
- **6) Définition de mécanismes de compression** pour IP : IPCOMP RFC 2393 puis RFC 3173.
  - Nécessité d'une relation: la compression doit passer avant le chiffrement (si l'on chiffre au niveau 3, la compression ne marche plus après).

Eléments principaux dans IPSEC

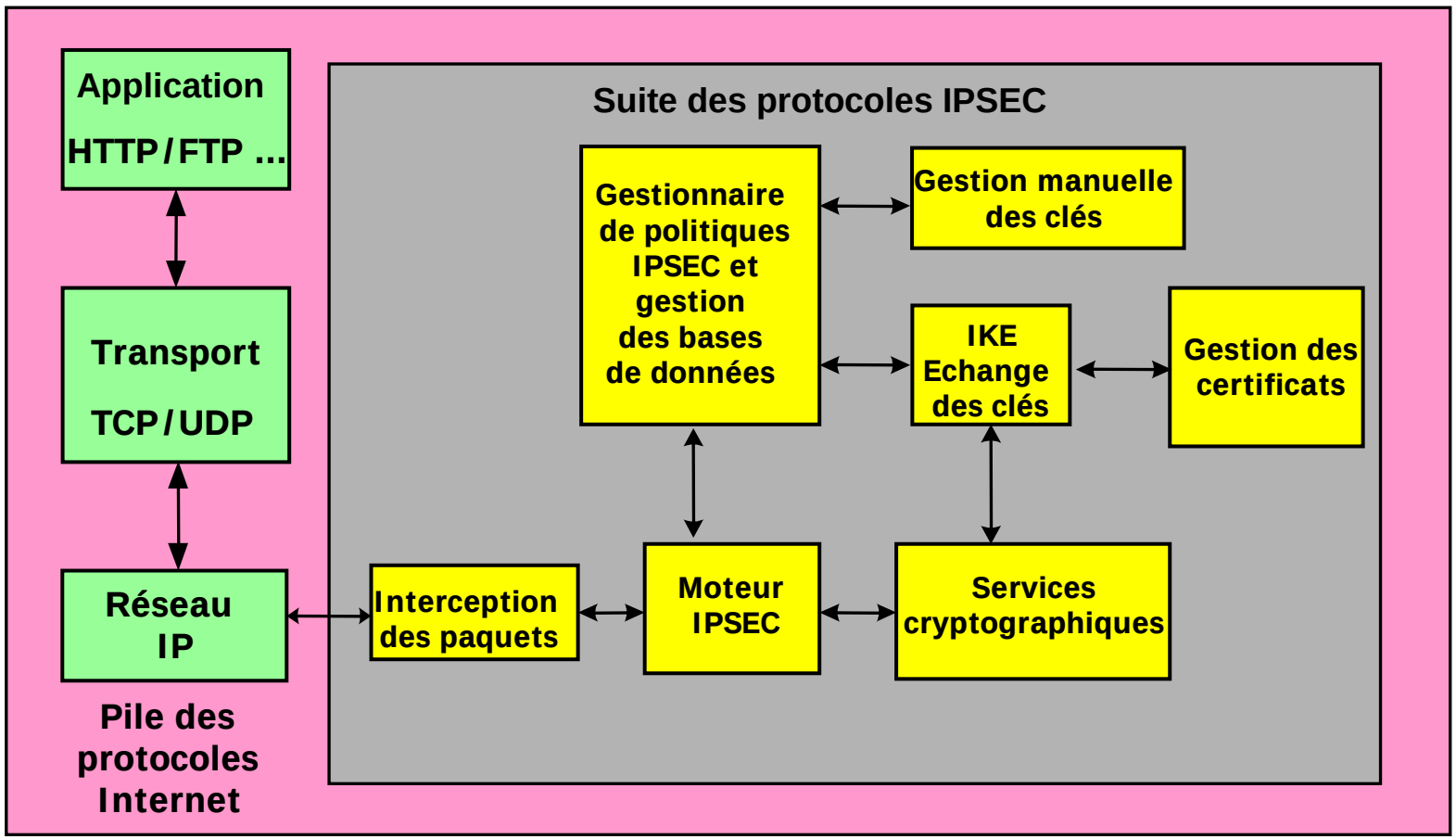
- **1) Une famille de protocoles d'échanges de clés**
  - **Internet Key Exchange (IKE)**
- **2) Deux protocoles de sécurité :**
  - **Authentication Header (AH) :** Authentification et intégrité des messages (dans une entête d'extension IP).
  - **Encapsulated Security Payload (ESP) :** Protocole de confidentialité, d'authentification et d'intégrité des messages (dans une entête d'extension et une postface).
- **3) Deux modes de fonctionnement des protocoles.**
  - **Mode Transport :** chiffrement de la charge utile IP.
  - **Mode Tunnel :** chiffrement de la charge utile et de l'entête IP.

Fonctionnalités IPSEC dans les protocoles AH et ESP

	AH	ESP Confidentialité	ESP Confidentialité, intégrité et authentification
Intégrité	X		X
Authentification émetteur	X		X
Rejet des paquets rejoués	X	X	X
Confidentialité		X	X
Confidentialité Protocolaire et de trafic (partielle)		X	X

* Parfois cité aussi dans IPSEC comme fonction IPSEC : contrôle de l'accès au réseau

IPSEC : Organisation générale



Notion de politique de sécurité : 'Security Policy'

- **1) Politique de sécurité en IPSEC**
  - Définir au préalable pour différentes communications en IP des **règles de sécurité IPSEC à appliquer : comment traiter en sécurité IPSEC un datagramme.**
- **2) Sélection d'une politique au moyen de filtres**
  - Essentiellement adresse IP source et destination.
  - Nombreuses autres possibilités (voir plus loin).
- **3) Règles de sécurité à appliquer à un datagramme :**
  - **Objectif :** définir les méthodes de sécurité à appliquer au datagramme. Interdire, Acheminer sans sécurité IPSEC ou Traiter en sécurité IPSEC.
  - **Si traitement IPSEC :** Fournir les éléments principaux AH ou ESP, transport ou tunnel, algorithmes de chiffrement à appliquer (DES , 3DES , AES-256...)...
  - **Pointer sur l'association de sécurité** qui contient toutes les données précises pour la définition et l'application de la politique de sécurité :
    - Les valeurs de clés, les fenêtres anti-rejeu etc.... (voir plus loin).
    - Si l'association n'existe pas elle pourra être créée à partir de la politique.

Sélection d'une politique de sécurité

- **Selon les implantations IPSEC il existe de nombreuses façons de sélectionner une politique** (de filtrer des datagrammes).

- **1) Adresse IP Destination :** Une adresse IP point à point, une liste d'adresses, une adresse de réseau IP.
- **2) Adresse IP Source :** Une adresse IP point à point, une liste d'adresses, une adresse de réseau IP.
- **3) Niveau de sécurité :** Dans le cadre d'une politique obligatoire (niveau non classifié, Secret ou Secret Défense).
- **4) Protocole de niveau transport :** Obtenu dans la charge utile (sélection de la politique selon le protocole de transport utilisé).
- **5) Ports Source et destination :** pour TCP ou UDP, des valeurs individuelles, des listes de valeurs ou des plages.
- **6) Classe de service IPv6 :** selon la classe de qualité de service.
- **7) Etiquette de flot IPv6 ('flow label') :** selon l'étiquette de flot IPV6.
- **8) Identifiant d'usager :** un nom de login.

SPD : Base de données des politiques de sécurité

- **1) SPD : ‘Security Policy Database’.**
- **2) Une approche de type annuaire :**
  - **Les politiques** sont créées, modifiées, détruites, et accèdées.
  - **Utilisation en recherche d’informations** pour chaque datagramme émis ou reçu (que faire du datagramme)
  - **Utilisation lors de la négociation initiale de détermination** des paramètres d’une association de sécurité.
- **3) Structuration comme une table de routage :**
  - **Principale clé une destination IP :** pour laquelle on a différents attributs qui définissent la securité à appliquer à un paquet (l’ensemble des règles de sécurité).
  - **Même stratégie que dans le routage CIDR:** recherche du plus long préfixe (si l’on a des règles pour 152.16/16 et 152.16.10/24 on choisit le plus long préfixe soit 152.16.10/24).

Notion d'association de sécurité : SA 'Security Association'

- **1) Objectif :** définir pour chaque datagramme les traitements de sécurité et leurs paramètres à lui appliquer.
- **2) Définition d'une association SA par trois valeurs principales :**
  - **Un identificateur de liste de paramètres** : Security Parameter Index (SPI) => une clé dans une base de données.
  - **Une adresse de destination IP** => une SA ne sécurise qu'une voie simplexe (deux SA pour une voie duplex).
  - **Un choix de protocole IPSEC** => choix entre AH et ESP.
- **3) A partir de l'index SPI :** on retrouve tous les paramètres nécessaires pour sécuriser un sens de communication.
- **4) Une SA est définie manuellement ou via le protocole d'échange de clés IKE.**

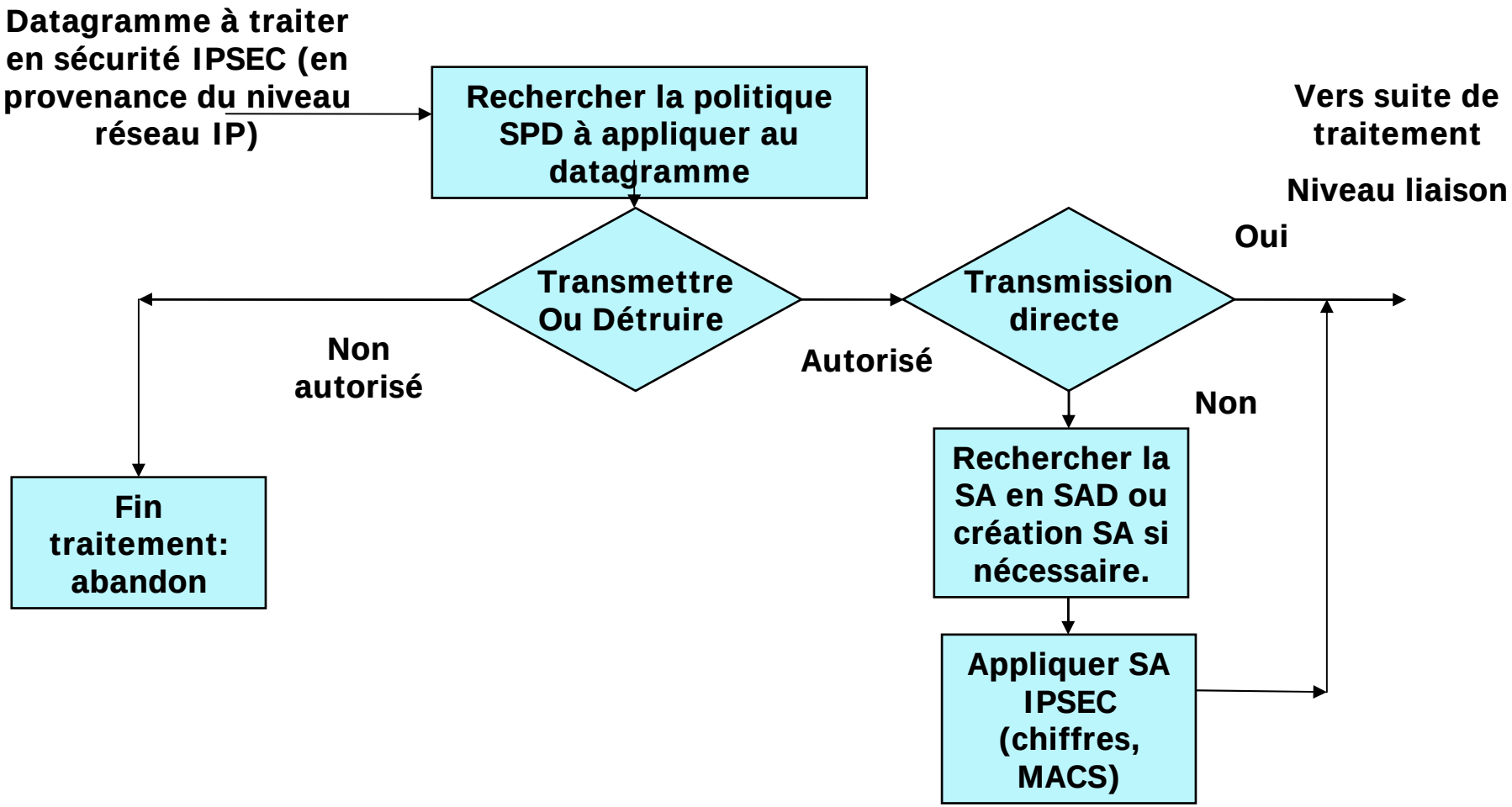
Associations de sécurité : Paramètres caractéristiques

- **Objectif : définir pour chaque datagramme les traitements de sécurité à lui appliquer.**
  - La valeur courante du numéro de séquence et la fenêtre des numéros acceptés (mécanisme anti-rejeu).
  - Le protocole IPSEC utilisé (soit AH soit ESP) en mode transport ou tunnel.
  - Informations pour le protocole AH la nature des fonctions cryptographiques utilisées: AES-128-bit en mode CBC , hachage SHA-1, la valeur des clés, leur durée de vie.
  - Informations pour le protocole ESP: nature des fonctions utilisées: AES-128-bit en mode CBC, la valeur des clés, leur durée de vie, les vecteurs d'initialisation
  - La durée de vie de l'association,
  - Le MTU de chemin, Etc ….

SAD : la base de données des associations de sécurité

- **SAD 'Security Association Database' :** la base de données des associations de sécurité
  - Sur un site: la liste des associations de sécurité en cours (applicables à des paquets entrants et sortants)
- **SPI 'Security Parameter Index'** : un identificateur sur 32 bits pour une association de sécurité
  - Identificateur transmis dans les entêtes de chaque paquet sécurisé.
  - Pour définir l'association de sécurité SA à appliquer à la réception d'un paquet.

IPSEC: Utilisation des bases de données



Exemple des deux bases de données de sécurité

- **SPD: Security Policy Database** :

Emetteur	Destinataire	Protocole	Port	Politique
10.10.1.1	10.10.2.23	TCP	18130	Transport, ESP, AES-256,SPI 10
10.10.1.1	10.10.2.23	UDP	*	Transport, ESP, 3DES , SPI 11

- **SAD: Security Association Database** :

Emetteur	Destinataire	Protocole	SPI	Enregistrement SA
10.10.1.1	10.10.2.23	ESP	10	Transport, ESP, AES-256, SHA-256 Clé1(AES 256 bit) ...
10.10.1.1	10.10.2.23	ESP	11	Transport, ESP, 3DES, SHA-1 Clé2(3DES 168 bit) ...

IPSEC : le mode transport

- **Un mode pour la sécurisation des protocoles de plus haut niveau que IP.**
  - La sécurisation s'applique à la charge utile d'un datagramme
  - Ce peut-être un segment TCP, UDP ou encore un message ICMP.
  - La sécurisation s'applique aussi à une sélection de champs de l'entête IP.
- **Objectif : sécuriser une communication d'hôte à hôte.**
  - Les traitements IPSEC doivent être réalisés aux deux extrémités d'un canal sécurisé.
  - Les extrémités (hôtes supports des applications) doivent connaître les protocoles IPSEC.

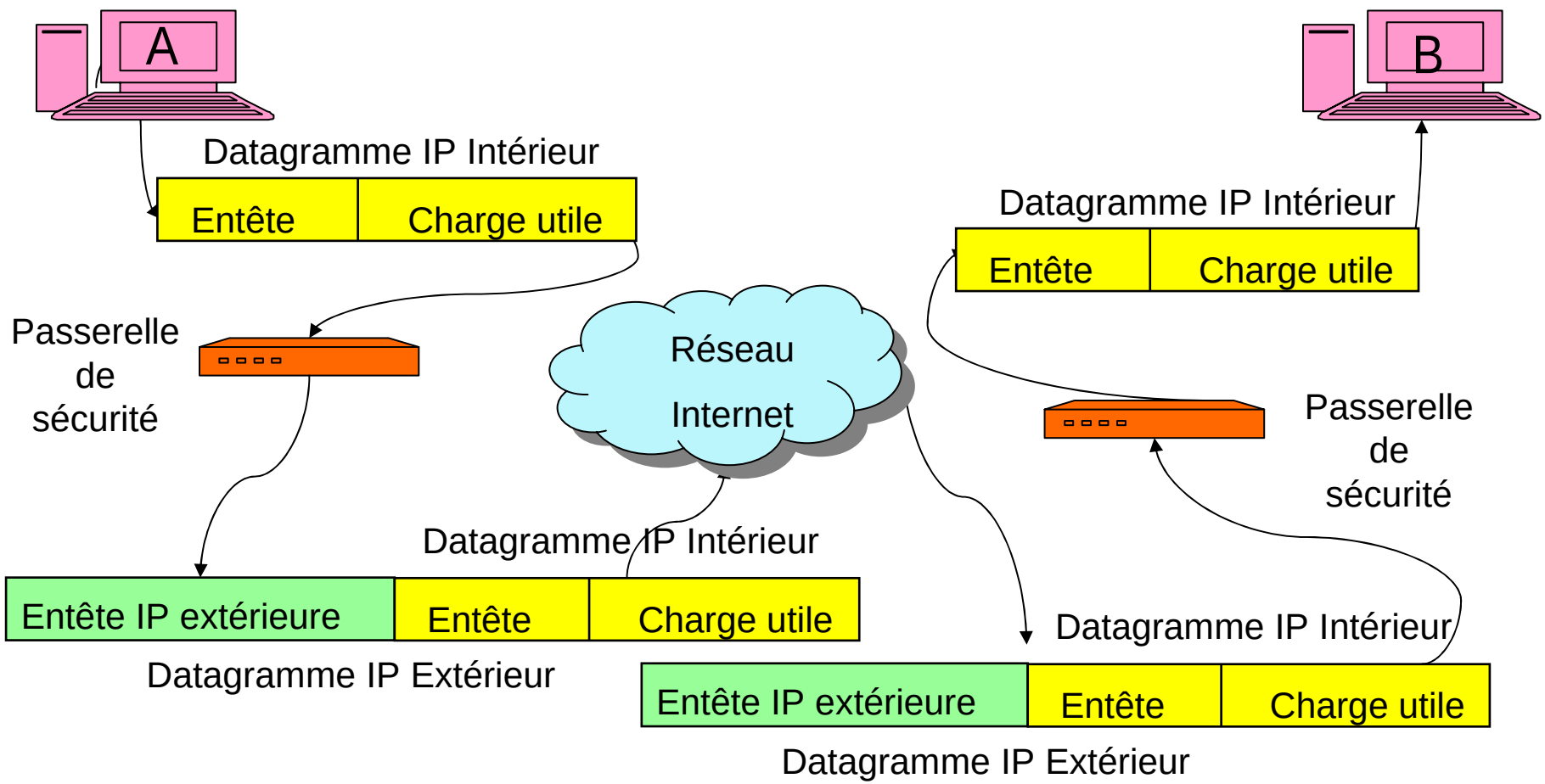
IPSEC : le mode tunnel

- **Mode tunnel: une solution d'encapsulation en vue de la sécurité**
  - **Sécurisation de la totalité d'un datagramme IP** : le datagramme 'intérieur' ('inner').
  - **Le datagramme intérieur sécurisé (avec ses zones dédiées à la sécurisation) est considéré comme une charge utile d'un nouveau datagramme** : le datagramme 'extérieur' ('outer')

- **Les traitements IPSEC sont plutôt réalisés dans des passerelles de sécurité :**
  - **Passerelle :** typiquement un pare-feux ('firewall') ou un routeur.
  - **On implante un tunnel :** de passerelle de sécurité à passerelle de sécurité plutôt que d'hôte à hôte.
  - Dans ce cas un hôte n'a pas à connaître les protocoles IPSEC.
- **Mais on peut aussi faire un tunnel d'hôte à hôte.**

- **Objectif** : une traversée du réseau se fait sans qu'on puisse intervenir sur le contenu du datagramme intérieur (par exemple on ne peut connaître les adresses IP source et destination).

IPSEC : illustration du mode tunnel



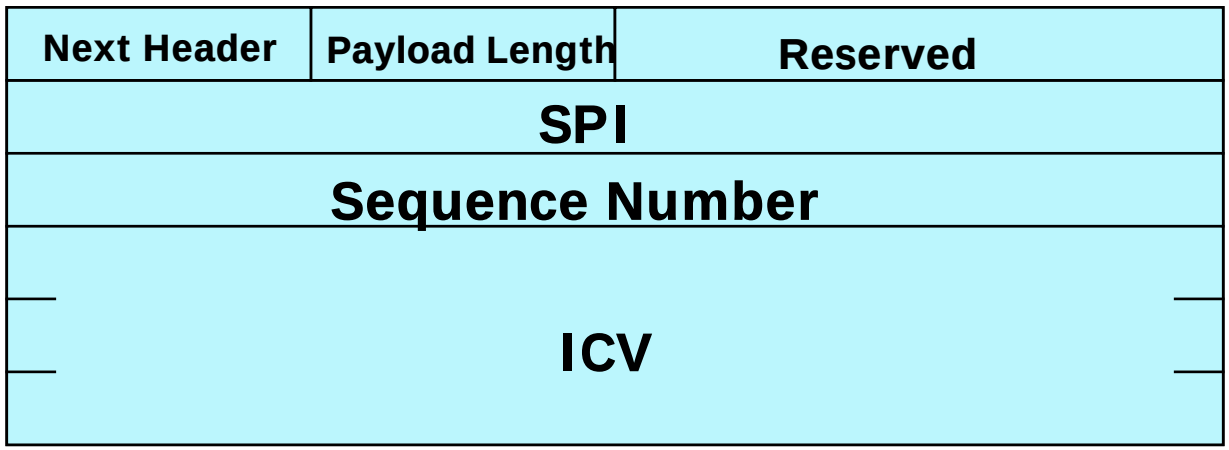
Sécurisation IP

Protocoles de sécurisation AH et ESP

Sécurité IPSEC avec AH : 'Authentication Header'

- **Généralités:**
  - Protocole pour l'authentification de l'émetteur et le contrôle d'intégrité.
  - Essentiellement basé sur des données insérées dans une entête d'extension IP : entête AH code 51.
  - RFC de base : RFC 2402 AH.
- **AH authentifie et contrôle en intégrité :** la totalité de la charge utile et la plus grande partie de l'entête IP.
  - **Permet de résister à l'usurpation d'adresse IP** (IP address spoofing) car l'adresse source IP est authentifiée.
  - **Permet de résister au rejeu** de datagrammes anciens car un numéro de séquence est ajouté et authentifié.
- **Utilisation d'un MAC** : donc nécessité d'une clé secrète partagée par les deux extrémités.

Sécurité IPSEC en AH : Format de l'entête d'extension AH



- **Payload Length** (attention problème):
  - Mesure en fait la longueur de l'entête AH en mots de 32 bits moins 2.
  - => une mesure de la taille variable de l'ICV.
- **SPI Security Parameter Index**
  - Identification de l'association de sécurité SA a utiliser pour ce paquet.
- **Sequence Number :** numéro de séquence modulo 2^{32}.
  - Un numéro de séquence obligatoire en émission.
  - Vérifié en réception si le mécanisme anti-rejeu est activé.
- **ICV Integrity Check Value :**
  - Contient le MAC (Message Authentication Code)
  - Cadré sur des mots de 32 bits (utilisation d'un bourrage si nécessaire).
  - Souvent tronqué à 96 bits (volume de données en entête d'extension IP).

Sécurité IPSEC en AH : Traitements à réaliser

- **Traitements à l'émission.**
  - Détermination de la SA (Security Association).
  - Génération du numéro de séquence (Sequence).
  - Calcul de l'authentificateur (ICV Integrity Check Value).
  - Alignement sur des mots de 32 bits (bourrage).
  - Fragmentation (si nécessaire).
- **Traitement en réception**
  - Réassemblage.
  - Détermination de l'association de sécurité.
  - Vérification du numéro de séquence.
  - Vérification de l'authentificateur ICV.

Sécurité IPSEC en AH : Protection en intégrité de l'entête

- **Zones de l'entête IP protégées en intégrité (en couleur)** => des zones stables (non modifiées).
- **Zones non protégées (en blanc):**

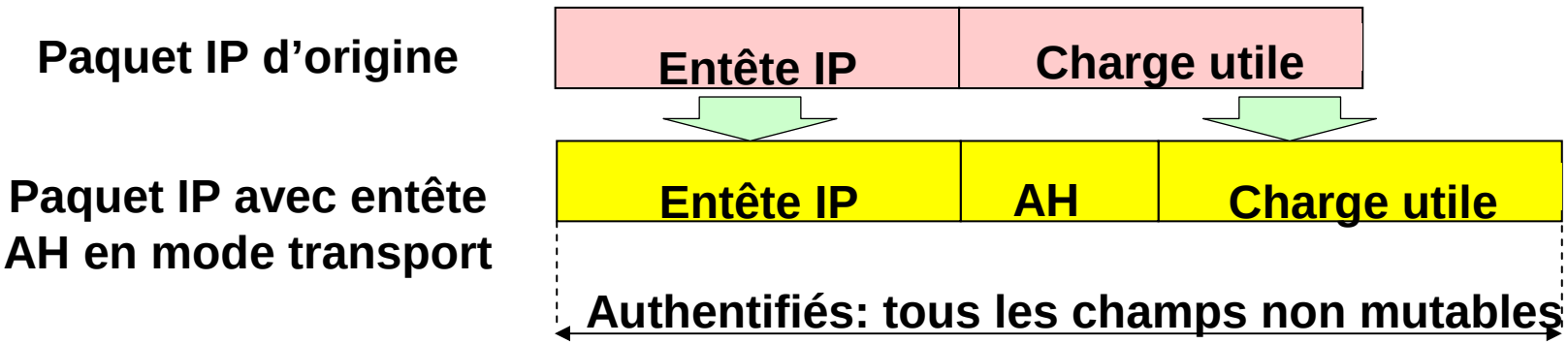
  => des zones modifiées par les routeurs.

Version	IHL	TOS	Total Length	
Identification			Flags	Fragment offset
TTL	Protocol		Header Checksum	
Source Address				
Destination Address				
Zone d'extension : options				

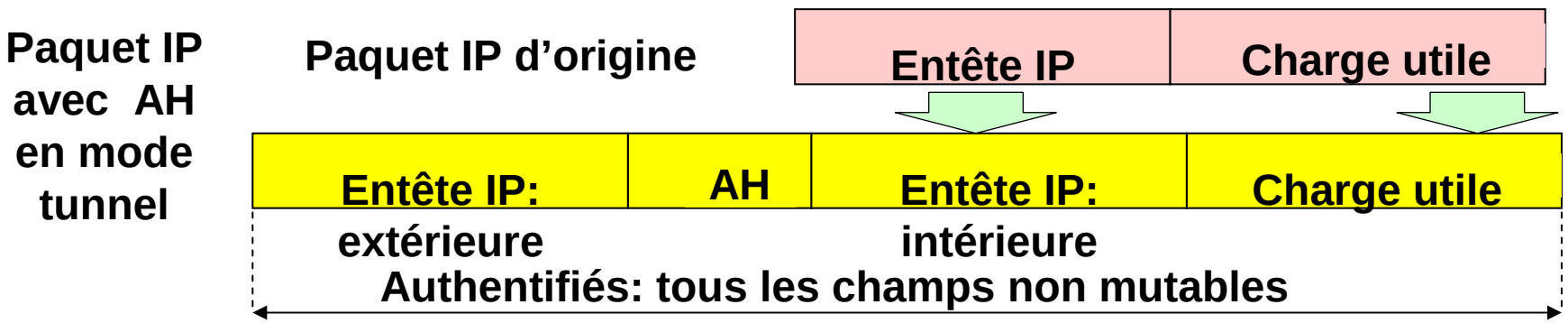
***Une solution :** Au moment du calcul les zones non protégées sont mises à 0**.**

Sécurité IPSEC en AH : Mode transport et mode tunnel

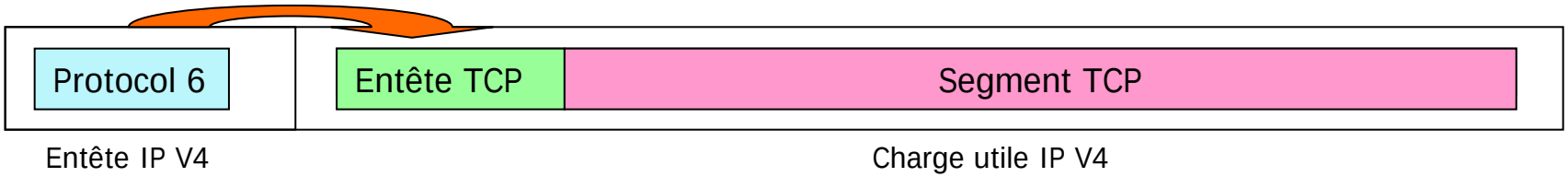
Zones protégées en mode transport



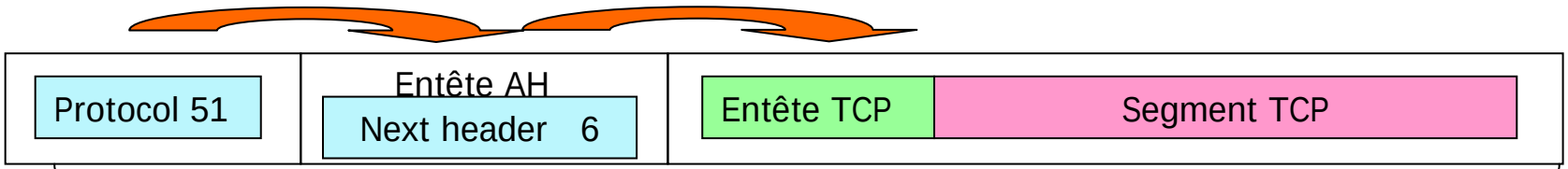
Zones protégées en mode tunnel



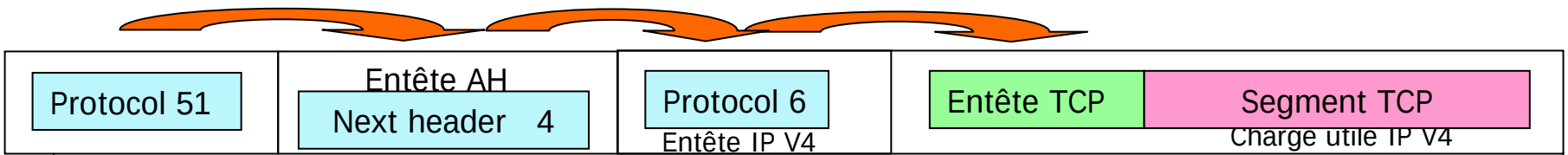
Sécurité IPSEC en AH : Schéma des entêtes d'extension



Datagramme IPV4 Original



Datagramme IPV4 avec AH en mode transport

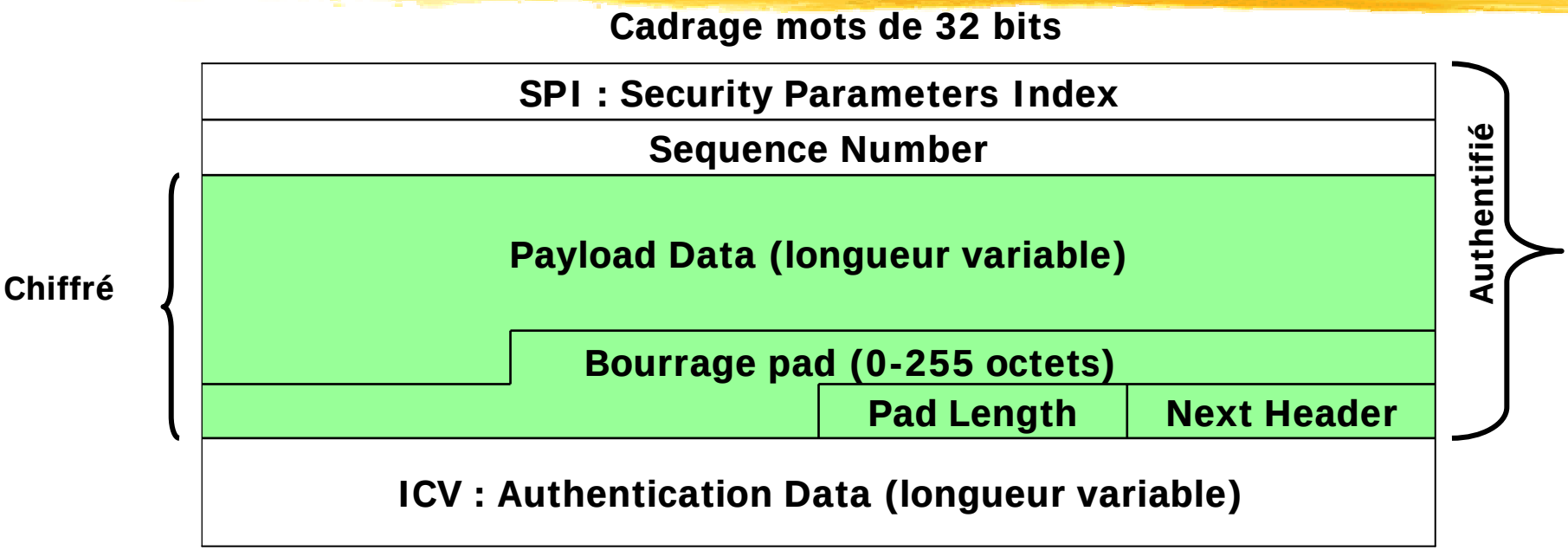


Datagramme IPV4 avec AH en mode tunnel

Sécurité IPSEC en ESP : Encapsulating Security Protocol

- **Rappel de l'objectif de ESP:**
  - Confidentialité d'un datagramme.
    - Z : en confidentialité le numéro de séquence n'est pas chiffré.
  - Authentification/intégrité d'un datagramme.
    - Z : pas d'authentification pour les champs d'entête extérieure.
  - Confidentialité du flot de données en mode tunnel.
- **Utilisation d'un chiffre** à clé secrète (symétrique) et d'un MAC basé sur une clé secrète.
- **ESP specifie une entête d'extension et une postface** : à ajouter au datagramme IP
  - Dans l'entête d'extension (code protocole 50): SPI et numéro de séquence.
  - Dans la postface: bourrage pour un chiffrement par blocs, longueur du bourrage, MAC (Authentication Code).
- **RFC de base** : RFC 1826 ESP version en cours 2406.

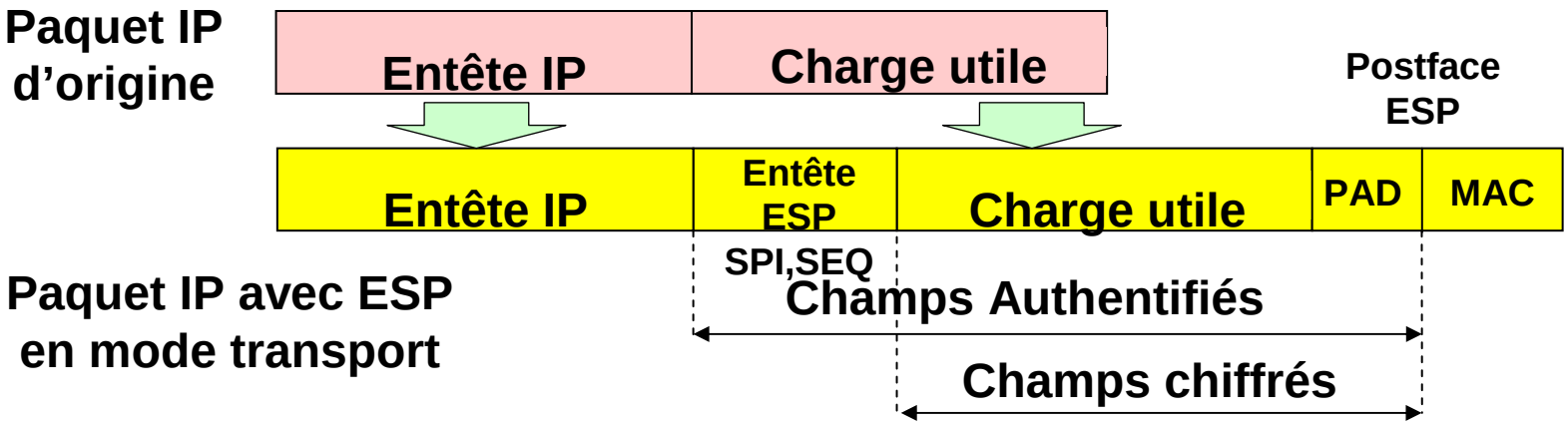
Sécurité IPSEC en ESP : Format des différents champs



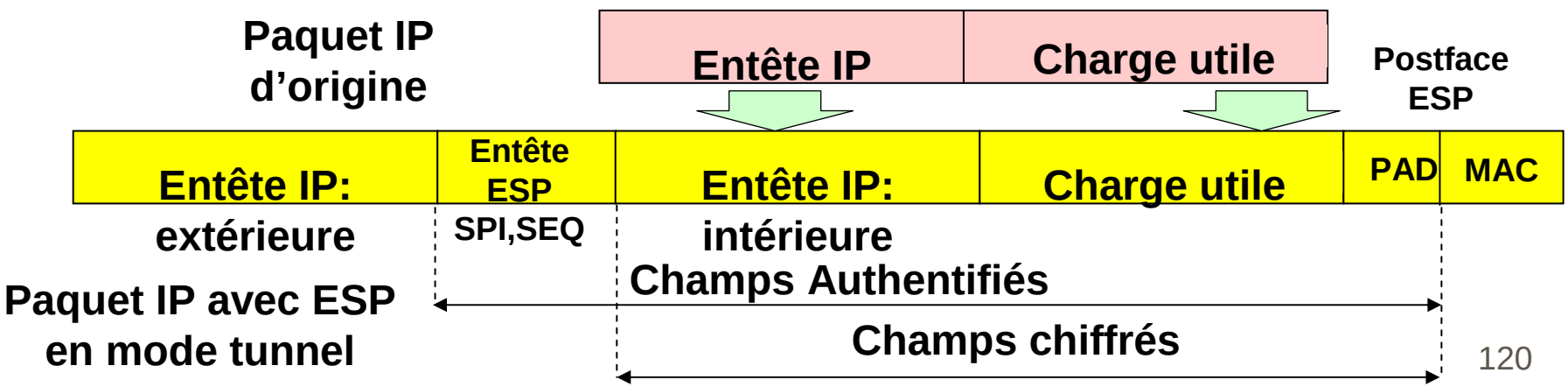
- SPI et numéro de séquence: 32 bits comme en AH.
- Payload : charge utile (par exemple un segment TCP).
- Bourrage 255 octets max avec un octet de longueur de bourrage).
- Prochain entête (next header): à la fin (peu habituel).
- Données d'authentification : ICV (un MAC).

Sécurité IPSEC en ESP : Mode transport et mode tunnel

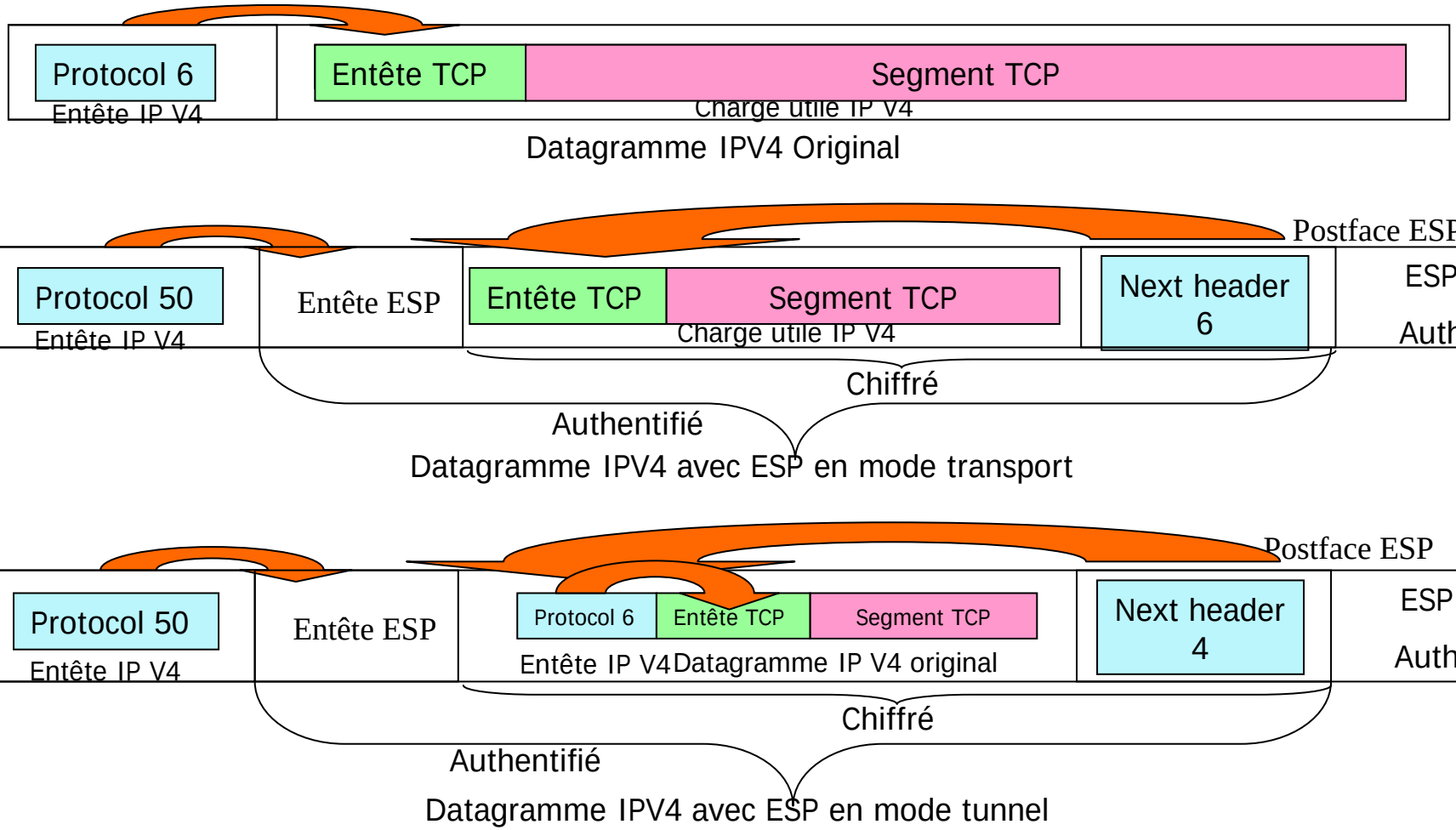
Zones protégées en mode transport ESP



Zones protégées en mode tunnel ESP



ESP : Structure des datagrammes et des entêtes d'extension



Stratégies anti-rejeu en IPSEC

- **1) Applicable à AH ou ESP.**
- **2) Utilisation du numéro de séquence sur 32 bits.**
  - Numéro initialisé à **zéro**.
  - On **incremente** pour chaque nouveau datagramme émis.
  - **Evénement repassage par 0** du numéro de séquence (‘wrap around’): choix d’une nouvelle clé secrète.
- **3) Protection des modifications du numéro par le MAC.**
- **4) Utilisation d’une gestion de fenêtre glissante :** fenêtre de réception qui accepte les messages dans le désordre (receiver’s sliding window).
  - **Taille** de fenêtre recommandée 64 (taille > 32 => pas trop de rejets inutiles).
  - Les datagrammes **anciens à l’extérieur de la fenêtre sont ignorés** (en dessous du niveau bas) => ce sont des rejeus.
  - Les datagrammes **nouveaux dans la fenêtre sont acceptés une fois** => pour éviter les rejeus ou les retransmissions normales.
  - Les messages nouveaux **à l’extérieur de la fenêtre au dessus du niveau haut** sont vérifiés et acceptés s’ils sont corrects.
  - La fenêtre **glisse** jusqu’à ce que son niveau haut corresponde au dernier message reçu correctement.

Combinaison des modes AH et ESP Utilisation de plusieurs SAs

- **1) ESP avec authentification n'authentifie pas certains champs.**
  - Parties fixes de l'en-tête IP (en mode transport).
  - Nouvel en-tête IP (en mode tunnel)
- **2) ESP chiffre avant d'authentifier**
- **3) Solution 1: Appliquer ESP (sans authentification) puis AH (nécessité de deux SA's)**
  - On authentifie les parties fixes de l'en-tête IP
- **4) Solution 2: Appliquer AH puis ESP (sans authentification) (deux SAs)**
  - On authentifie les données directement (avant le chiffrement)
  - L'entête d'authentification AH est ensuite protégée par le chiffrement.
- **5) Autres cas à plusieurs applications d'IPSEC :**
  - Empilement d'utilisation IPSEC (ex tunnel entre deux routeurs + tunnel entre deux applications).

Sécurisation IP

Les protocoles d'échange de clés

IKE Internet Key Exchange

Objectifs généraux de IKE

- **1) Protocole pour la négociation**
  - Des caractéristiques de sécurité.
  - Des paramètres des protocoles de sécurité.
- **2) Protocole d'authentification des entités communicantes**
  - Les identités restent cachées.
- **3) Protocole de génération et d'échange de clés secrètes** de façon sécuritaire.
- **4) IKE => la gestion dynamique des associations de sécurité** : création, modification, destruction (vs manuelle).
- **5) Les attaques prises en compte**
  - **A) Déni de service**. **B) Rejeu. C) Attaque du milieu.**
  - **D) Secret parfait des clés** (PFS Perfect Forward Secrecy) : des clés utilisées antérieurement ou postérieurement par le protocole ne peuvent être dérivées de la clé en cours d'utilisation (Diffie-Hellman).

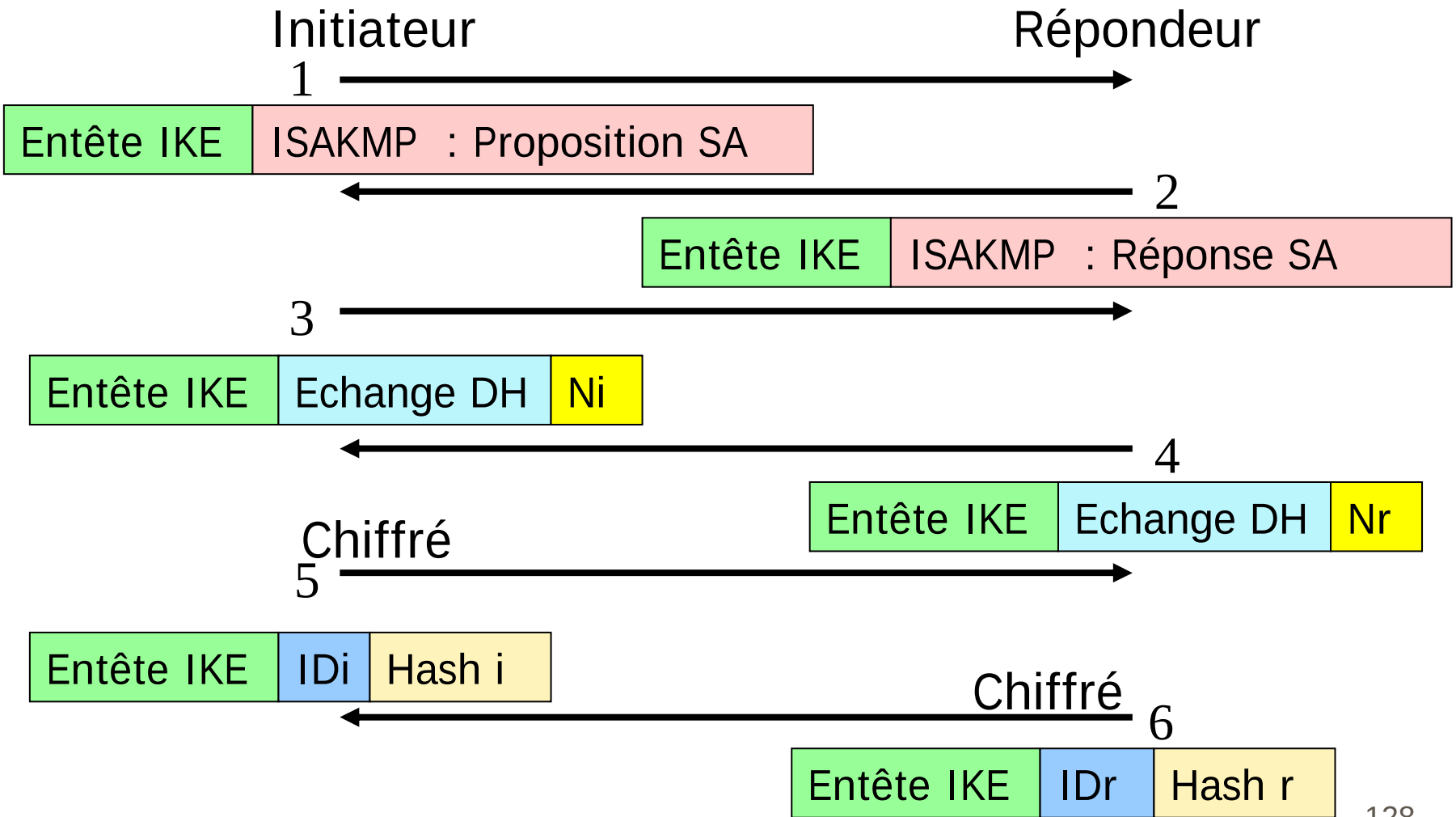
Caractéristiques de IKE

- **1) IKE** (RFC 2407, 2408, 2409, 2412) **: protocole de négociation de paramètres de sécurité** défini pour IPSEC mais utilisable dans d'autres contextes.
- **2) IKE : un protocole de niveau session**
  - IKE est indépendant de IP.
  - IKE utilise le transport **UDP sur le port 500.**
- **3) Pour réaliser ses services,** IKE combine des éléments issus de protocoles différents.
  - **ISAKMP :** Internet Security Association and Key Management Protocol (RFC 2408) => la vision générique.
  - **OAKLEY :** Oakley Key Determination Protocol (RFC 2412) => une réalisation de ISAKMP (autres versions SKIP, Photuris, SKEME).
  - **DOI :** IPSec Domain of Interpretation (RFC 2407) => pour interpréter le contenu des messages ISAKMP.

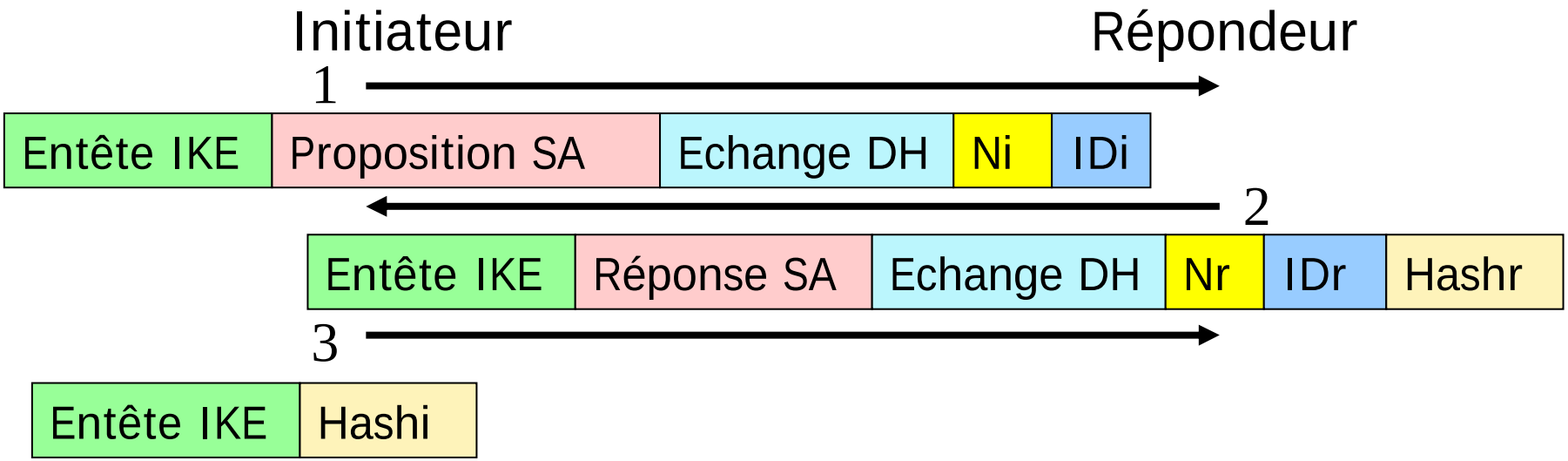
ISAKMP : Internet Security Association and Key Management

- **ISAKMP : un cadre générique pour la négociation et l'échange de clés.**
  - Ce n'est pas un protocole concret c'est une manière de procéder.
- **Deux phases successives.**
- **Phase 1 : Négociation pour la phase 1, Echange de clés et authentification**
  - A) Négociation de l'association de sécurité utilisée pour les propres besoins de l'échange de clé (fonctions cryptographiques et protocoles utilisés par IKE).
  - B) Echange de clé secrète (le plus souvent par le protocole de Diffie-Hellman mais aussi d'autres possibilités).
  - C) Authentification mutuelle des deux entités.
- **Phase 2 : Négociation des associations de sécurité** (SAs) utilisées dans les échanges sécurisés IP ultérieurs.

Protocole ISAKMP/OAKLEY : Mode clés pré partagées

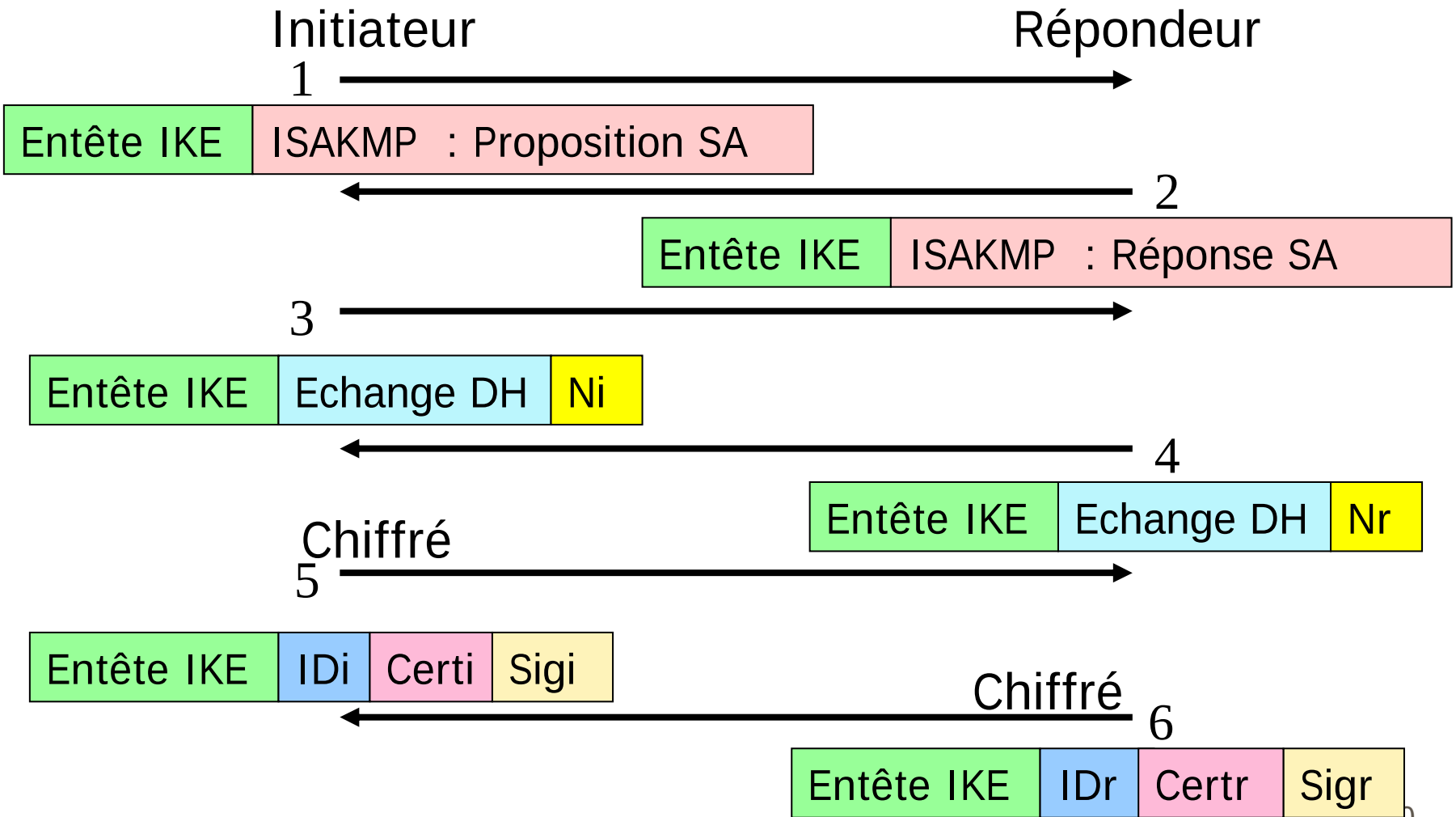


Protocole ISAKMP/OAKLEY : clés pré partagées Mode agressif



- **Mode agressif :** trois messages seulement.
- **Messages non chiffrés :** les identifiants peuvent être lus.
- **Attaques possibles:** La clé pré partagée est hachée (hachages hashi et hashr) avec des données connues => attaque possible à dictionnaire pour déterminer la clé secrète.

Protocole ISAKMP/OAKLEY : Authentification à clés publiques



Recommandations de sécurité pour le déploiement IPSEC

- **1) Chiffrement en confidentialité**
  - Utiliser plutôt le triple DES que le DES (longueur de clé de 168 bits).
  - Mieux AES (clé 128 bits ou plus jusqu'à 256 bits si les besoins l'exigent).

- **2) IKE en mode clé pré partagée**
  - La clé pré partagée doit faire au moins 128 bits

  22 caractères aléatoires base64 : A..Z, a..z, 0..9, +/

- **3) IKE en mode agressif**
  - Vulnérable - A déconseiller

- **4) IKE en mode principal**
  - Utilisation du mode clé pré partagée pour des tunnels statiques seulement**.**
  - Solution à clé publique RSA souple et sécuritaire pour des tunnels dynamiques**.**
  - Utilisation d'une clé RSA de 2048 bit RSA pour un bon niveau de sécurité.
  - Stockage de la clé privée sur une carte à puce ou une clé USB.

Sécurisation IP

Conclusion

Avantages IPSEC

- **1) Une standardisation assez bonne**
  - => inter opérabilité
- **2) Un ensemble très complet de mécanismes proposés.**
- **3) Des mécanismes de sécurité d'un bon niveau.**
  - **A) Déni de service. B) Rejeu. C) Attaque du milieu.**
  - **D) Secret parfait des clés (PFS Perfect Forward Secrecy)**
  - Des critiques d'experts sur certains mécanismes.
- **4) Peut-être déployé sans impliquer les utilisateurs**
  - de façon sécuritaire.

Inconvénients IPSEC

- **1) Pas d'infrastructure à clés publiques (pour les variantes à clés publiques).**
- **2) Des problèmes de mise au point de certaines versions.**
- **3) Les problèmes avec NAT.**
  - **Solution NAT – T IPSEC (NAT Traversal avec IPSEC) =>** Détecter la présence de NAT et utiliser UDP.

Problèmes rencontrés quand on utilise IPsec avec NAT

- **1) Avec IPSEC NAT ne peut plus modifier les sommes de contrôle TCP (obligatoire) ou UDP (optionnelle).**
  - La somme de contrôle TCP/UDP incorpore l'adresse IP or elle est chiffrée.
- **2) NAT ne peut plus multiplexer différents flots de donnés sur la même adresse IP quand ESP fonctionne.**
  - Avec ESP les numéros de port TCP ou UDP son inaccessibles => un flot est identifié par l'adresse IP et le SPI.
  - Si NAT doit changer l'adresse IP et le port il devrait maintenant changer le SPI et reconvertir IP et SPI à la réception => Changer le SPI est impossible car il entre dans le calcul de l'ICV (le hachage).
- **3) Le champ identification dans IKE n'est pas modifiable par NAT (il est chiffré).**
  - Comme il s'agit en général d'une adresse IP, certaines implantations stoppent l'échange pour incohérence.

- **=> Principaux changements proposés par NAT T pour permettre à NAT de fonctionner avec IPSEC:**
  - Ajout d'une encapsulation UDP en ESP => NAT ne voit plus qu'un segment UDP.
  - Modification des formats des messages en IKE.

Bibliographie

- Kent, S., and R. Atkinson, "IP Security Architecture", RFC 2401, November 1998.
- Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.
- Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.
- [MSST97] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.
- Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.
- Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.
- Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

VPN de niveau réseau

VPN pair à pair dans le protocole MPLS

“MPLS, Multi Protocol Label Switching”

Concepts généraux

Les réseaux privés virtuels VPN MPLS

COMMUTATION IP : MPLS

Rappel du contexte :
le protocole MPLS

Concepts généraux MPLS: Historique MPLS

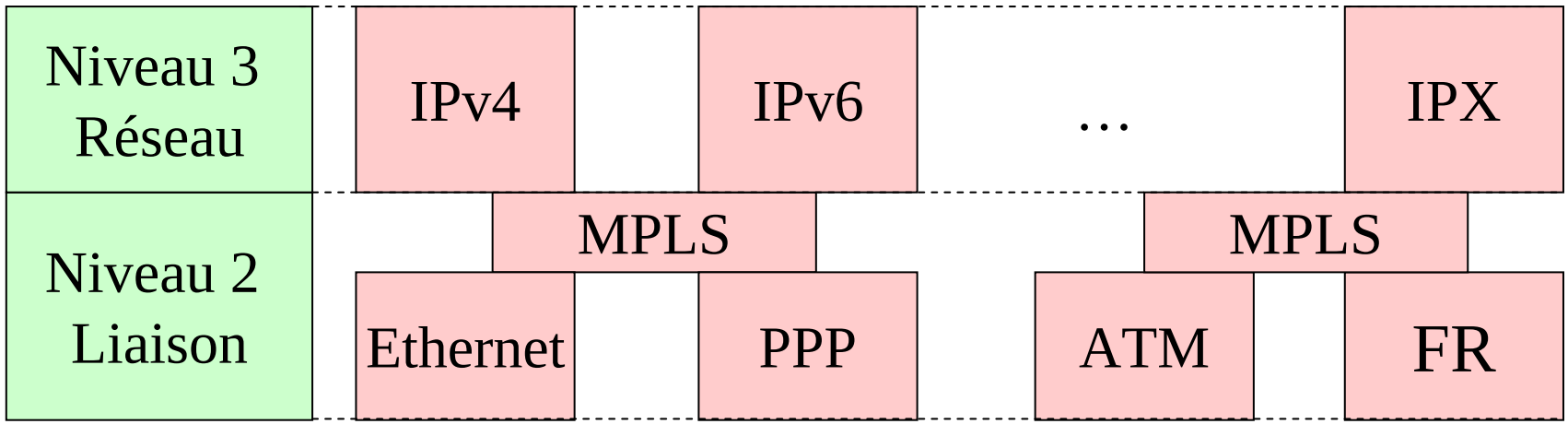
1) Années 1990 adaptation à IP du mode circuit virtuel

- **Ipsilon / Nokia** : IP Switching
- **Cisco** : Tag Switching.
- **IBM** : ARIS Aggregate Route Based IP Switching.
- **Cascade / Ascend / lucent** : IP Navigator

2) Convergence des propositions : groupe de travail IETF créé en 1997 ‘commutation d’étiquettes’ ‘label switching’

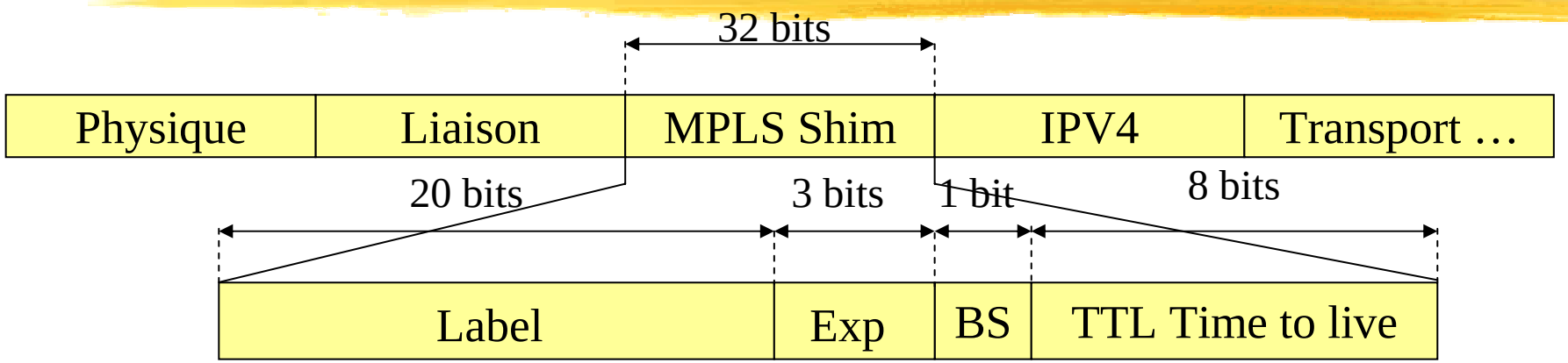
- **RFC 3031** jusqu’à **3038** (janvier 2001).
  - **MPLS Architecture** et suivantes.
- A ce jour une trentaine de RFC (normes) et nombreux ‘drafts’.

Concepts généraux MPLS: Situation de MPLS dans le modèle de référence



- 1) Situation entre les niveaux 2 et 3.
- 2) Protocole de niveau liaison.
- 3) Applicable à tout protocole de niveau réseau.
- 4) Utilisation de tous les niveaux liaisons existants.
- 5) Fonctionnement sur tous les niveaux physiques.

Concepts généraux MPLS: Entête MPLS (MPLS Shim). Notion de label



- **Label** : nombre **entier identificateur local** de chemin fixe (n'existe pas en IP donc doit être rajouté).
- **MPLS Shim** : une **pile** de labels (sur la figure un seul label).
  - **Label (20 bits):** un identifiant local de chemin (unicité des labels : par interface ou par commutateur).
  - **Exp (3 bits)** : Zone expérimentale (au départ COS Classe de service).
  - **BS ('Bottom of Stack') (1 bit)** : Dernier label d'une pile de labels (valeur 1) sinon 0 pour tous les autres éléments.
  - **TTL ('Time To Live') (8 bits)** : Durée de vie dans le réseau MPLS (décrémenté à chaque saut comme en IP).

Concepts généraux MPLS: Router sur les bords , Commuter au centre

- **1) Création préalable des labels** : notion de distribution des labels (création des tables).
- **2) Ajout de label à un datagramme IP** par le commutateur entrée 'ingress' : **opération 'push'.**
- **3) Commutation** dans les commutateurs de cœur de réseau par consultation des tables : **opération 'swap'.**
- **4) Retrait de label en sortie**: **opération 'pop'.**

'Route at edge , Switch in core'

- **Z** La terminologie reste floue: les commutateurs MPLS sont souvent appelés routeurs.

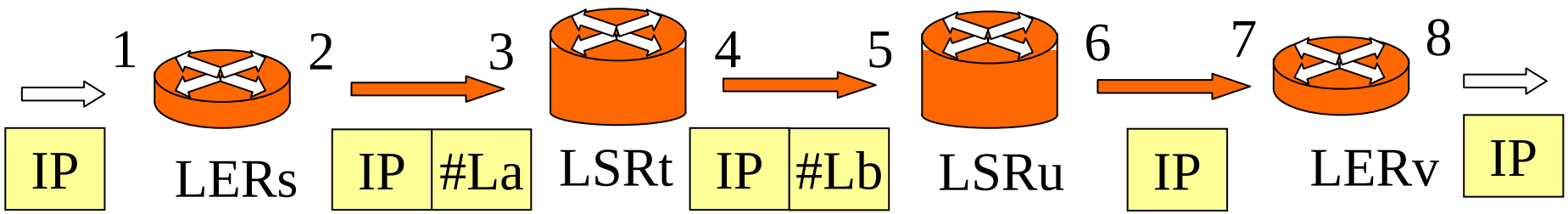
Concepts généraux MPLS: Exemple simple de fonctionnement

Tables de commutation (LIB Label Information Base)

1	IP	2	#La
..	…	..	…

3	#La	4	#Lb
..	…	..	…

5	#Lb	6	IP
..	…	..	…



Assignation d'un label Push #La

Evolution des labels Swap # LA # Lb

Retrait de label Pop #Lb

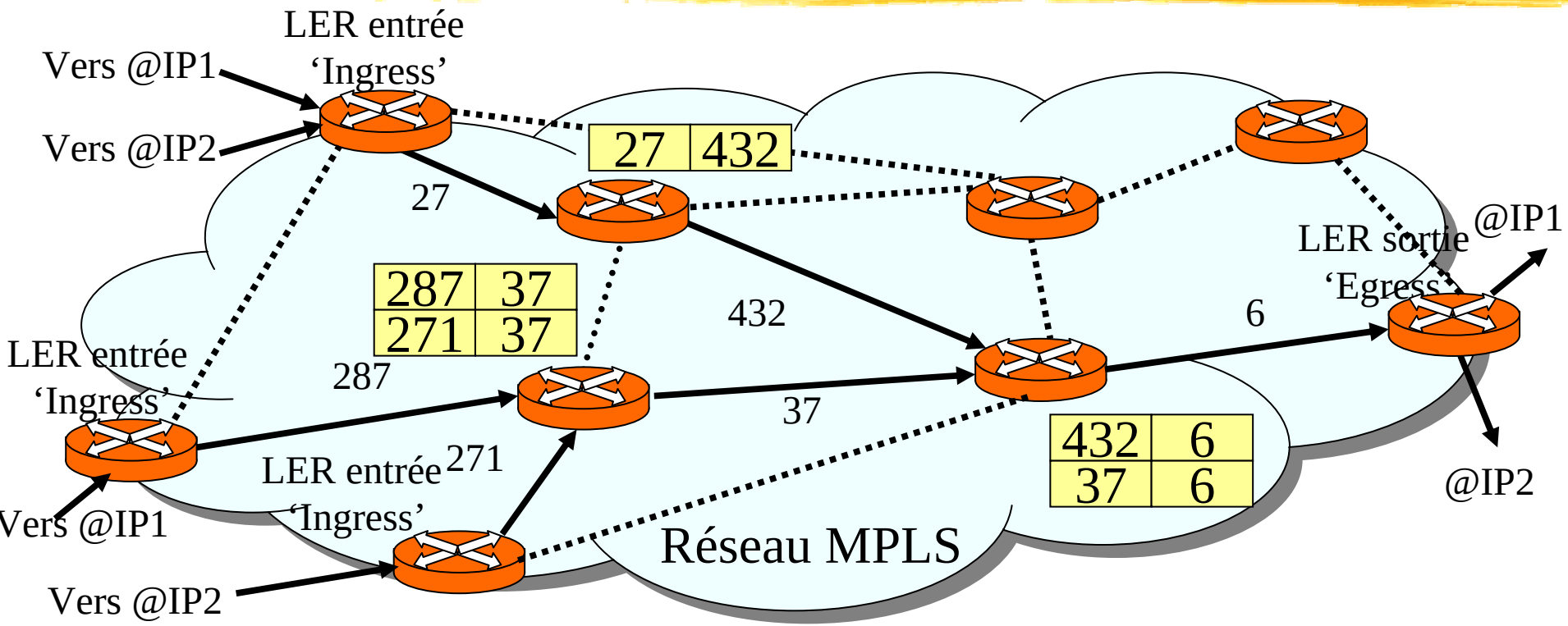
Z Retrait du label par l'avant dernier ('penultimate pop').

Concepts MPLS : Classes de trafic FEC Forwarding Equivalence Class

- **FEC** : **un ensemble** de datagrammes IP subissant **le même traitement MPLS.**
  - Même imposition de label au départ.
  - Même prochain saut , même file d'attente ...

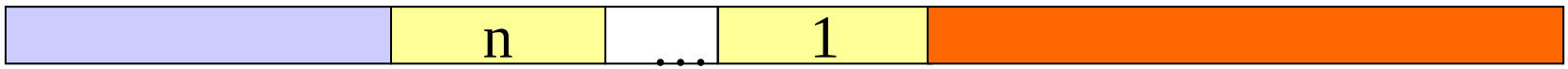
- **FEC : trois catégories principales**.
  - **FEC Préfixe** : même préfixe IP (réseau IP dest)
  - **FEC Routeur** : même routeur IP destination,
  - **FEC Flux** : FEC associée à une application c'est-à-dire adresses IP et numéros de port source et destination.
  - **Autres principes de définition** de FEC possibles : sur définition de COS (class of service entête IPv4 ou V6) où sur requête de QOS.

Concepts généraux MPLS : Arbre associé à une FEC



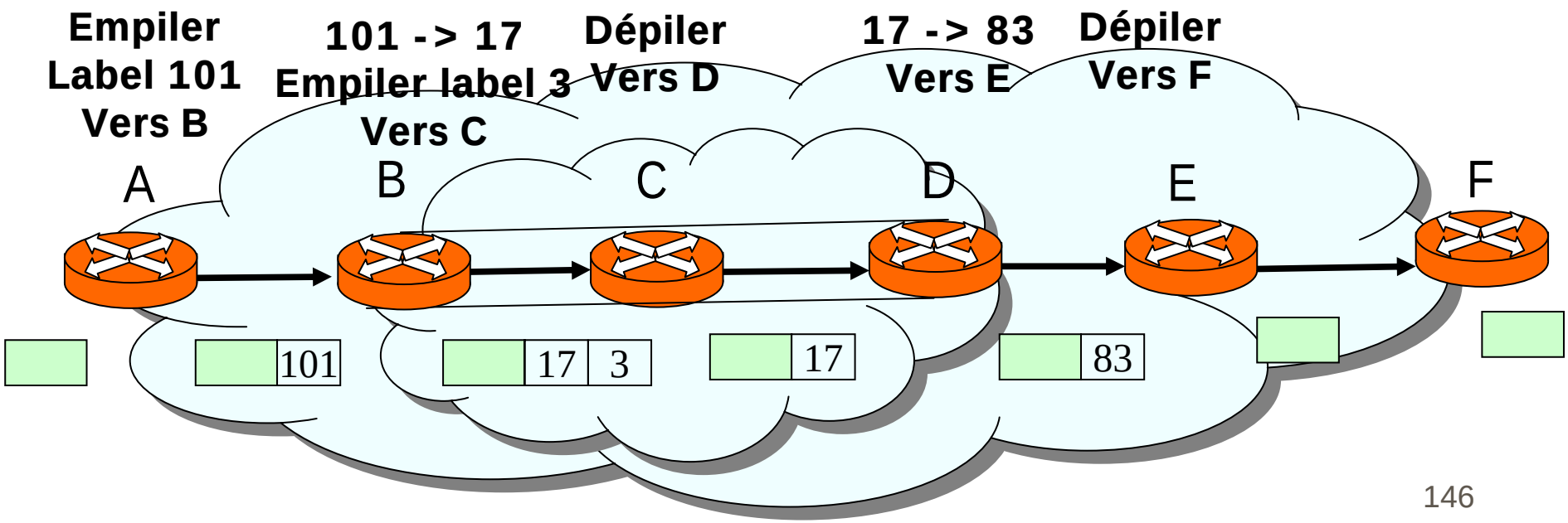
- **FEC : un arbre** d'un ensemble de commutateurs **d'entrée** vers un commutateur de sortie.
- **Notion de fusion des labels** sur les sommets de l'arbre.

Concepts généraux MPLS : hiérarchie de réseaux MPLS (piles de labels)



Entêtes niveau 1,2 : PPP | Entêtes MPLS 1,n Shim | Paquet réseau : IP

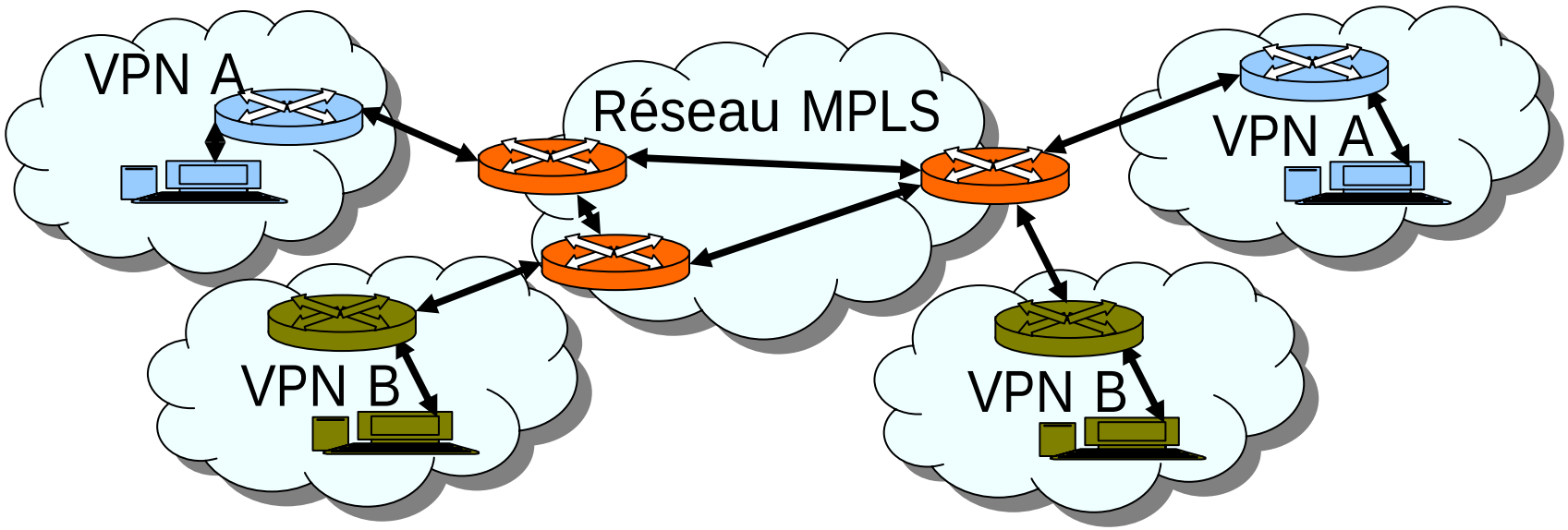
- **Empilement d'entêtes MPLS** : 'shim' (labels et TTLs) =>
- **Une hiérarchie de réseaux MPLS:** exemple avec 2 réseaux.



COMMUTATION IP : MPLS

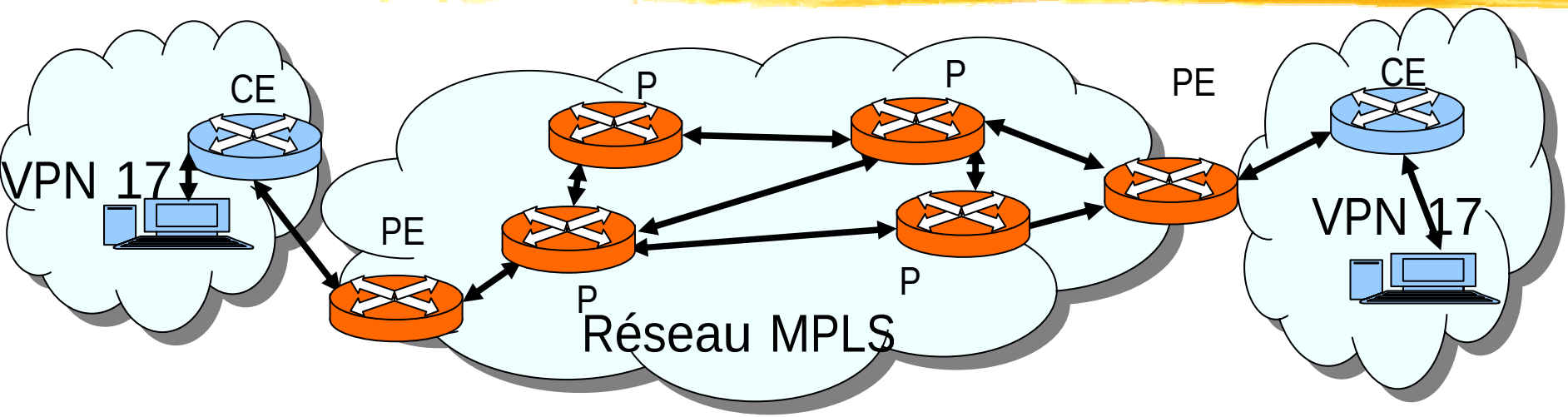
Les réseaux privés virtuels MPLS
VPN Virtual Private Networks

VPN MPLS : Introduction



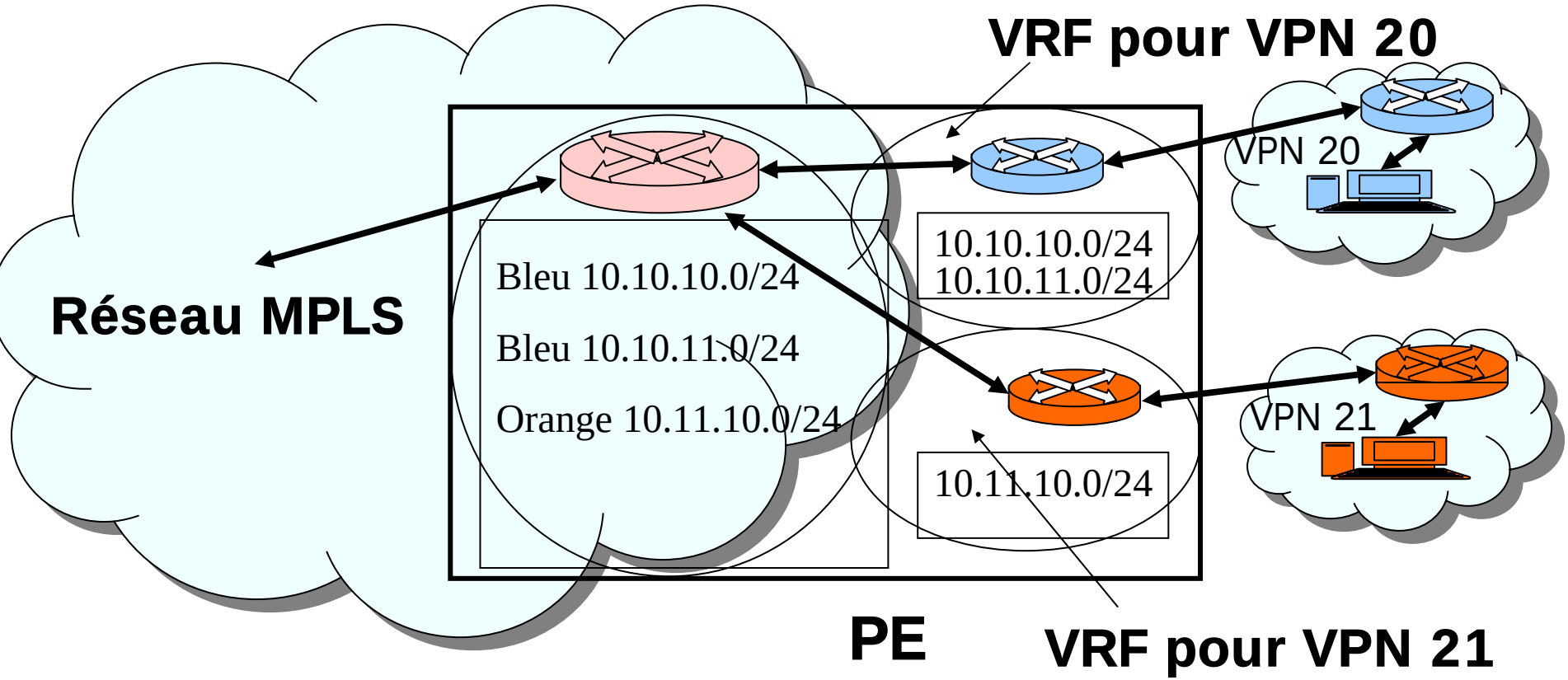
- **VPN en MPLS :** une approche de contrôle d'accès avec l'objectif d'assurer le caractère contrôlé des échanges pour un ensemble d'hôtes d'un réseau Internet utilisant un cœur de réseau MPLS.
  - Exemple type : les datagrammes des utilisateurs A ne doivent pas être acheminés vers des routeurs des utilisateurs B et réciproquement.
  - Typiquement un service pour FAI mais utilisable aussi dans une entreprise.
- **VPN :** un service MPLS qui valorise beaucoup l'intérêt de déployer MPLS.

VPN MPLS : Notions de base
CE , PE, P



- **CE (‘Customer Edge’) :** Un routeur usager dont une interface est reliée au domaine MPLS.
- **PE (‘Provider Edge’) :** Un commutateur de frontière de réseau MPLS.
  - Une ou plusieurs interfaces sont reliées au domaine client.
- **P (‘Provider’) :** Un commutateur MPLS interne de réseau prestataire.
  - Toutes ses interfaces sont connectées dans le réseau MPLS.
- **P, PE, CE :** Des commutateurs ou routeurs réels (physiques).

Notion de routeur virtuel : VRF ‘VPN Routing Forwarding’



- **VPN :** Empilement d’un label supplémentaire spécifique VPN.

Routeur virtuel VRF : Précisions

- **Fonction routeur :** agissant pour le compte d'un seul VPN.
- **Routeur virtuel :**
  - Fonctionnant uniquement dans un routeur réel d'entrée (un PE).
  - Autant de VRF par PE que de VPN déclarés.
- **Outils d'un VRF :**
  - Une table de routage propre au VRF.
  - La table de routage globale du PE et sa table de commutation (de transmission dans le domaine MPLS)
  - L'exportation/L'importation des routes vers la table globale des routes du PE (avec des règles qui contrôlent l'importation/l'exportation des routes).
  - Une ou plusieurs interfaces physiques reliées au domaine client : une interface n'est utilisable que dans un seul VRF (protection).
  - Des protocoles de routage qui alimentent les routes dans le VRF.

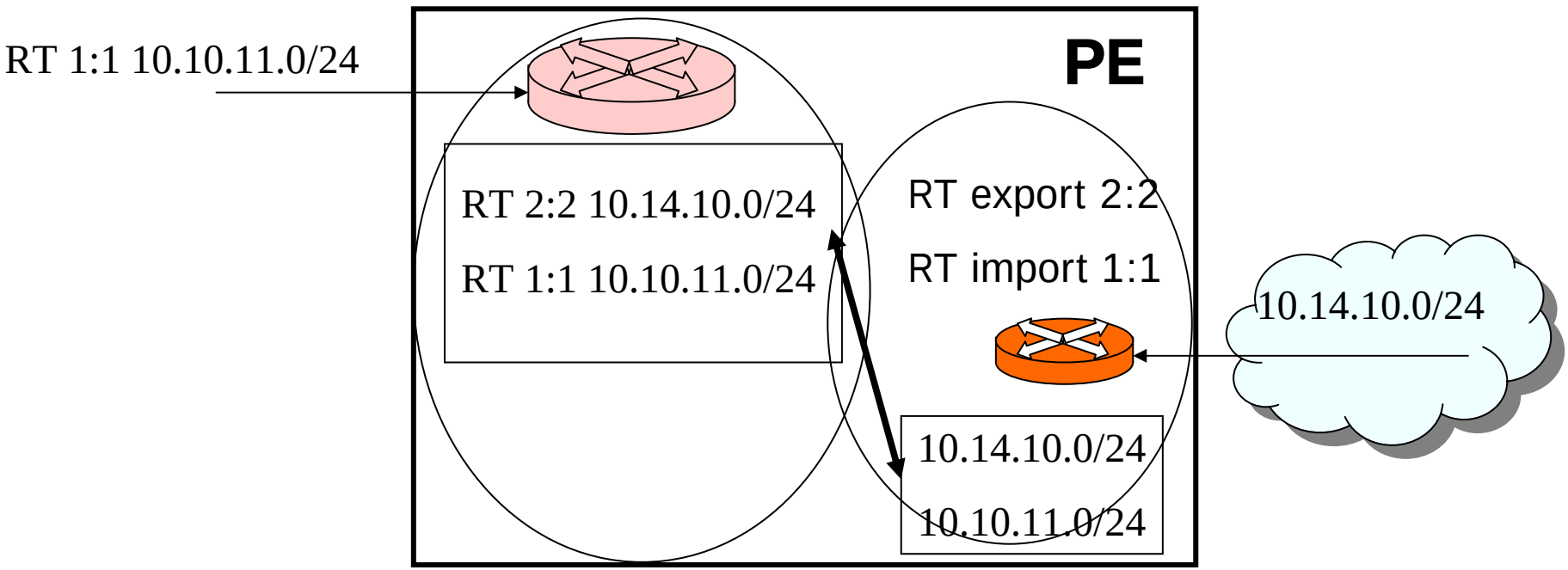
Protection des routes dans les VPN MPLS

- **Solution standard pour gérer la protection :**
  - Définir des sujets (les routeurs), des objets (les routes).
  - Définir de droits des sujets sur les objets : emprunter une route.
  - Créer une architecture à base de capacités : par exemple une solution à base de liste de capacités gérée dans les sujets (les routeurs).
  - Définir une stratégie de propagation des droits (de transfert des capacités ainsi créées). Les capacités devraient être signées.
- **Solution retenue en MPLS :**
  - Ce qui n'est pas connu ne peut être utilisé et donc est interdit.
  - On ne transmet les routes d'un routeur à l'autre que sous certaines conditions de telle sorte qu'une politique de contrôle d'accès soit réalisée.

Routeur VRF : Notion de route cible RT Route Target

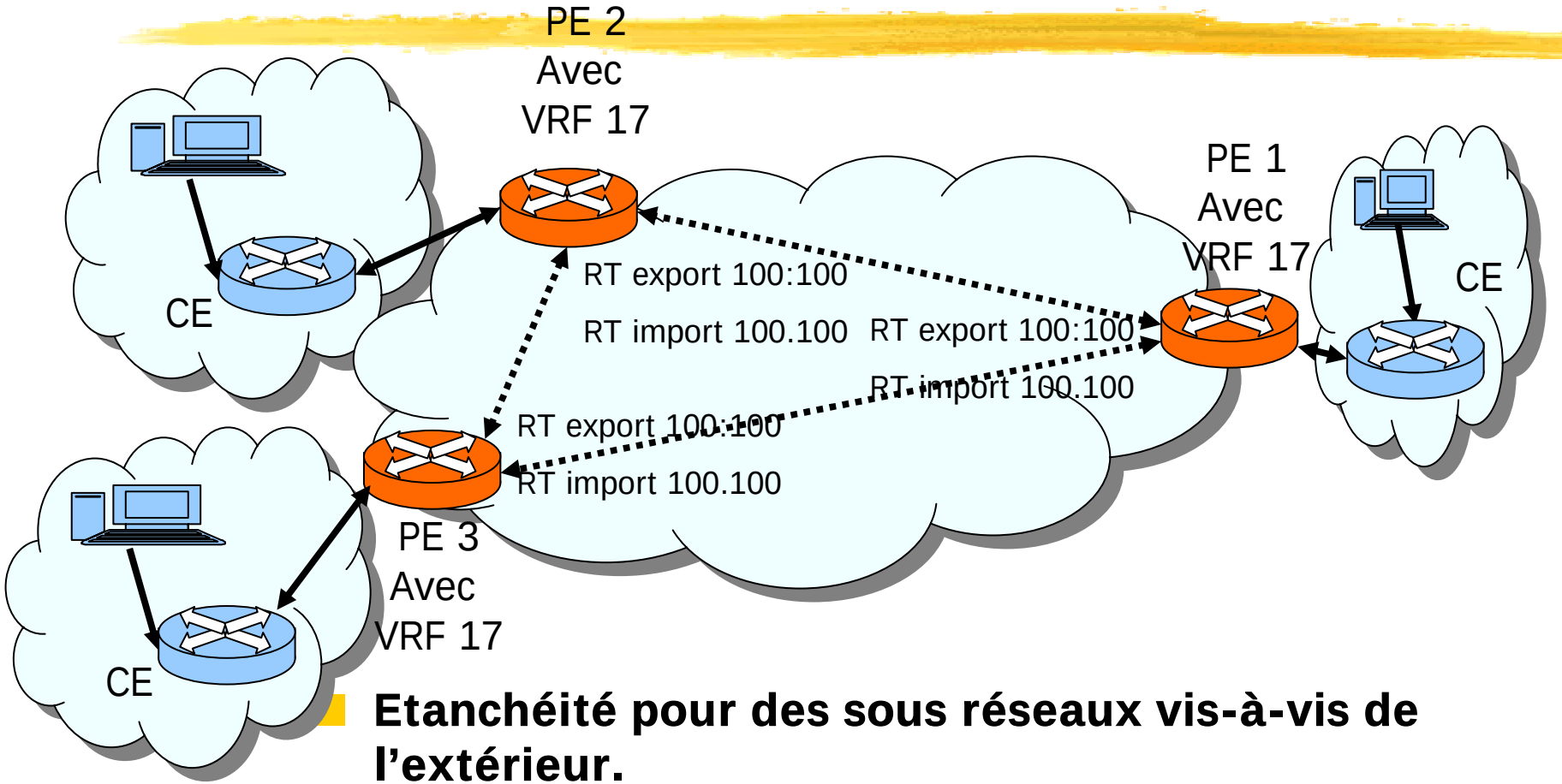
- **Notion d'exportation de routes :**
  - Une route figurant dans la table d'un routeur virtuel VRF peut être exportée vers la table globale d'un routeur PE.
  - On peut atteindre le réseau appartenant à un VPN (la destination de la route) desservi par le PE en venant du domaine MPLS.
  - **En protection** : export = offrir un droit d'utiliser une route.
- **Notion d'importation de route :**
  - Une route figurant dans la table globale du PE peut être importée dans la table de routage d'un VRF.
  - Alors les hôtes connectés au VPN local pourront atteindre des réseaux distants connectés au réseau MPLS (appartenant au même VPN).
  - **En protection** : import = installer une capacité dans une liste.
- **Notion de route cible 'route target' RT**
  - Etiquette qui permet de nommer les routes à importer ou à exporter.

Routeur virtuel VRF : Exemple de route cible RT (‘Route Target’)



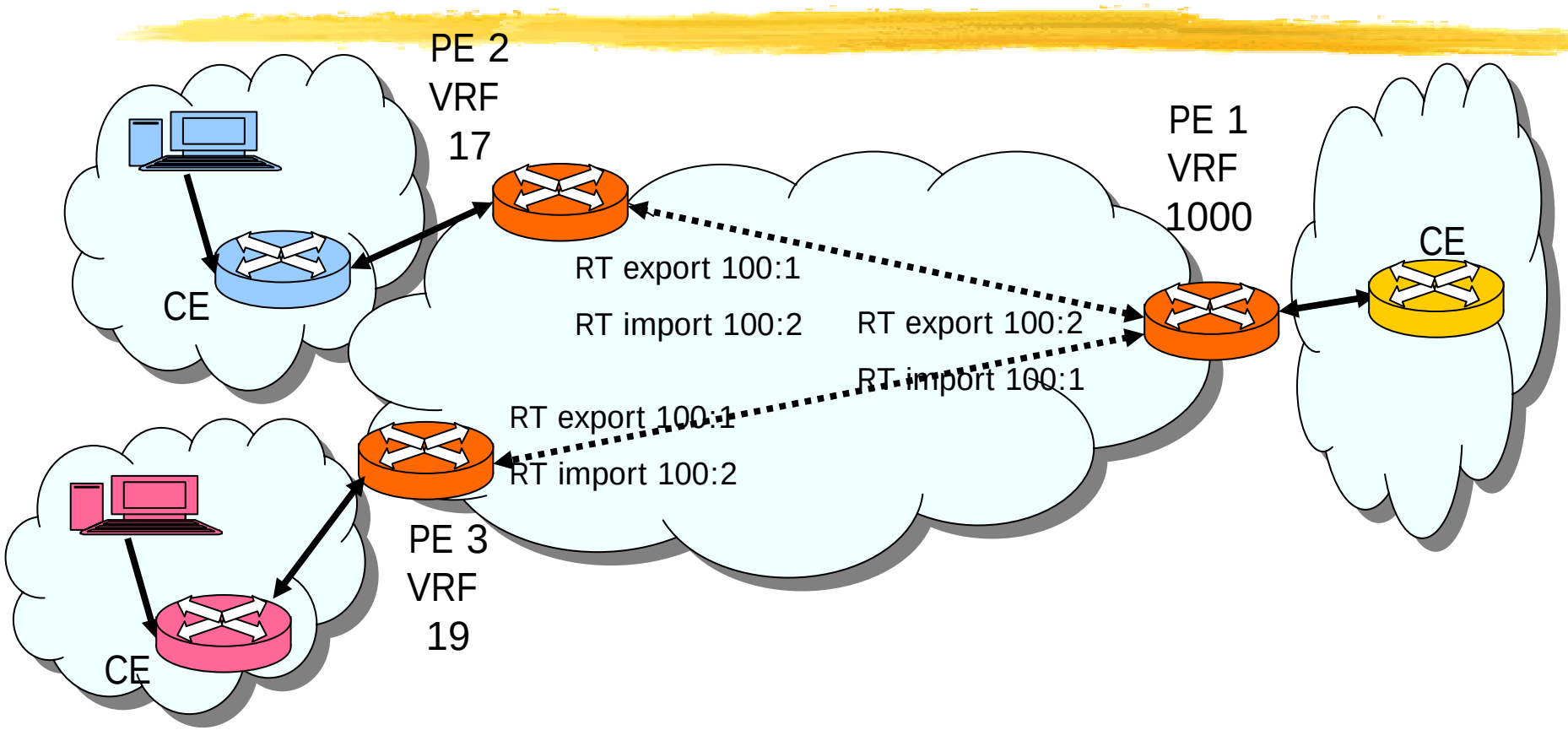
- **RT :** une étiquette sur 64 bits associée à une route dans les tables de routage (forme de RT x:y).
- **Si un RT export est positionné dans un VRF:** toutes les routes provenant des interfaces sont exportées vers la table globale avec le label.
- **Si un RT import est positionné :** toutes les routes avec ce label dans la table globale du PE sont copiées dans la table VRF.

Exemple 1 d'utilisation des RT : une architecture VPN fermée



- **Etanchéité pour des sous réseaux vis-à-vis de l'extérieur.**
- **Tous les VRF ont le même nom 17 et font le même import et le même export (même RT).**
- **La valeur route cible RT n'est pas utilisée ailleurs.**

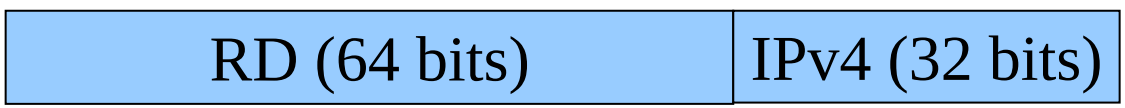
Exemple 2 d'utilisation des RT : architecture avec réseau de sortie



- **Trois VPN différents 17, 19, 1000.**
- **17 et 19 communiquent avec 1000 mais 17 et 19 restent séparés.**
- **Propriété de BGP :** les routes de 17 et 19 apprises par 1000 de MPLS ne sont pas réfléchies vers MPLS (mécanisme anti-bouclage de BGP).

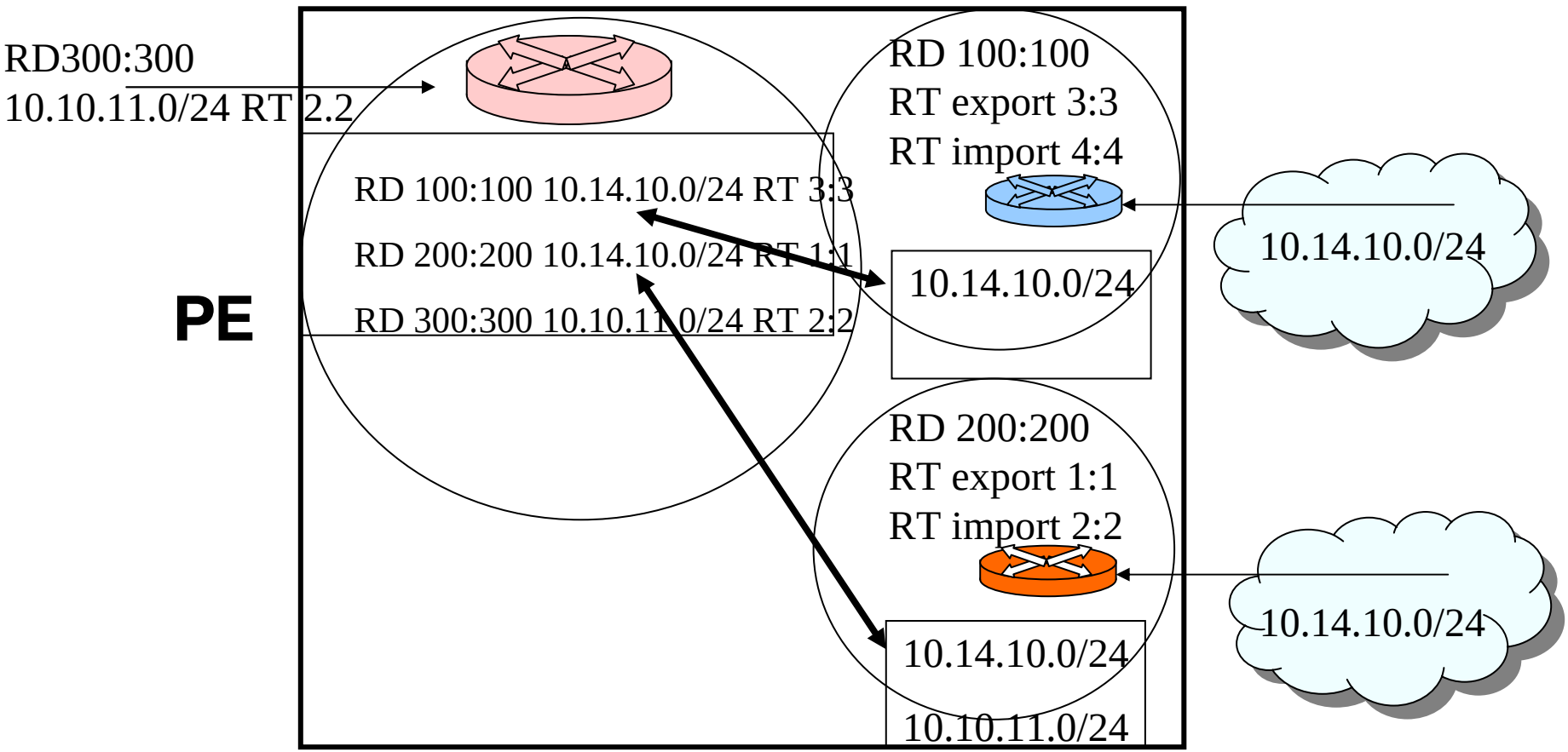
Notion de distingueur de route : RD ‘Route distinguisher’

- **Solution MPLS pour gérer les homonymies dans les réseaux privés :**
  - Deux réseaux privés vont souvent utiliser les mêmes plages d’adresses IP privées (10/8 , 172.16/12, 192.168/16).
  - Besoin de rajouter une extension d’adresse pour distinguer les réseaux homonymes.
- **Notion de route distinguisher RD**
  - Une étiquette sur 64 bits associée aux adresses de destination de route pour distinguer les cas d’homonymie (format d’un RD x:y).
  - D’où un nouveau format de destination de route :



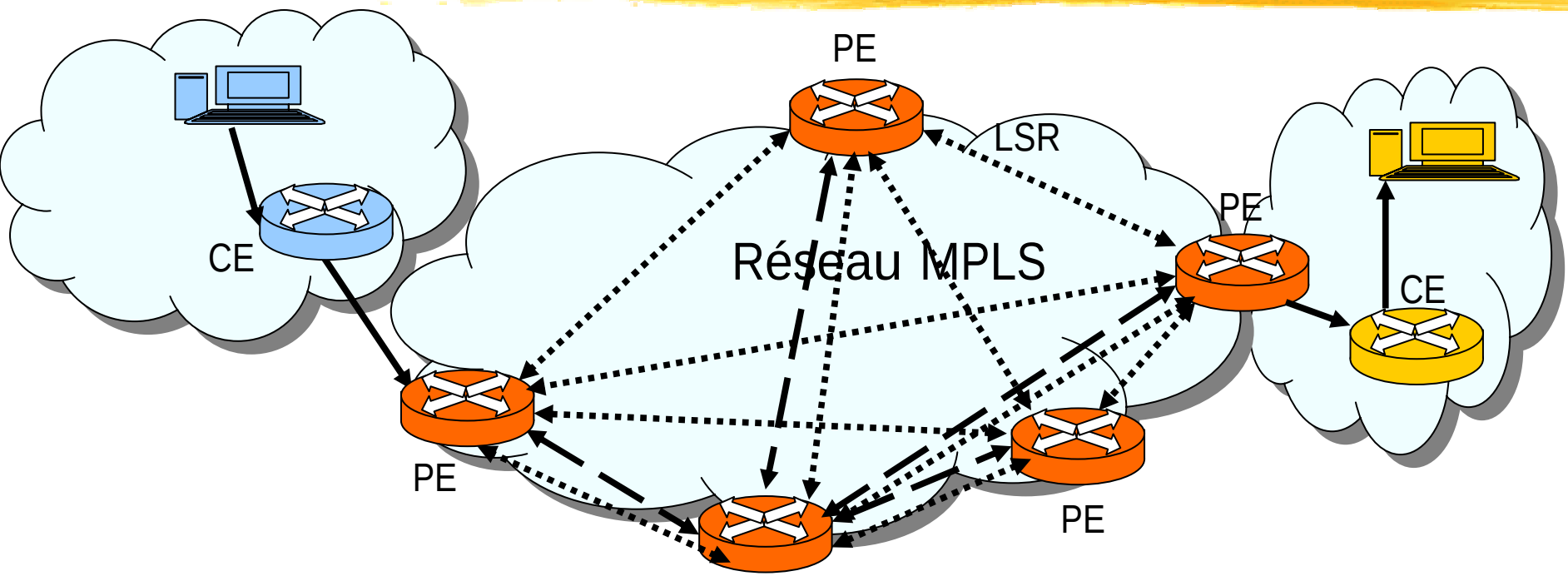
  - Géré par un protocole de routage spécifique : MP-BGP (MPLS Border Gateway Protocol)

Exemple de RD : ‘Route Distinguisher’



- Deux routes de RD différents sont distinguées (comme sur l’exemple).
- Deux routes de RD identiques sont fusionnées.

Topologies pour la mise en place du routage MP-BGP avec VPN



PE réflecteur de routes BGP

- **Pour le routage BGP :** besoin de faire communiquer tous les PE
  - ◄— —► **Solution centralisée (avec un réflecteur de routes).**
  - ◄·····► **Solution de construction d'un graphe complet.**

Conclusion MPLS et VPN MPLS

Au début de MPLS

- MPLS: une amélioration de performances pour IP.
- Succès dans ce domaine mais progression en parallèle des techniques de routage IP.

Actuellement

- Une solution pour le contrôle d'accès via les VPN.
- Une solution pour l'ingénierie de traffic (l'optimisation des ressources réseaux).
- Une version pour la commutation optique : GMPLS

  G 'generalized' : des labels associés à une longueur d'onde en WDM ou DWDM.
- Un protocole devenu complexe à administrer.
- Supporté par les FAI ou les très grands comptes.

Conclusion VPN MPLS

- VPN MPLS: une solution de protection (contrôle d'accès, autorisation) appliquée au routage.
- Généralement appliquée par un FAI. La sécurité repose sur la confiance dans ce FAI.
  - Application stricte par le FAI dans son domaine MPLS de la politique de sécurité demandée.
  - Absence d'erreurs dans la configuation de cette politique (valeur des RT et des RD) surtout si la configuration est manuelle.
- Une approche de VPN MPLS n'est pas à mettre en concurrence avec IPSEC :
  - Objectifs différents.
  - IPSEC offre une approche de confidentialité ou d'intégrité basée sur la cryptographie.
  - Les deux approches peuvent être utilisées simultanément.

Bibliographie VPN

- **Très nombreuses pages Web** sur le sujet.
- Marco Carugi, '**Virtual Private Network services'** Autrans - RHDM'02, Mai 2002.
- Paul Ferguson, Geoff Huston, **'What is a VPN',** The Internet Protocol Journal, Volume 1, 1998.
- Lina AL-CHAAL, **'Une approche dynamique et facilement administrable pour des environnements IPVPN sécurisés'**, Thèse de doctorat INPG, Grenoble, Février 2005.
- Rafael Corvalan, Ernesto Corvalan, Yoann Le Corvic, **'Les VPN'** 2ième édition Dunod 2005.

Biliographie VPN MPLS

- Ulysse Black ‘MPLS and label switching networks’ Prentice Hall 2001
- Très nombreuses pages web de cours sur le sujet MPLS et VPN MPLS : deux exemples
  - http://www.iec.org/online/tutorials/mpls/index.html
  - Cours MPLS A. Le Boudec Ecole Polytechnique de Lausanne

http://ica1www.epfl.ch/cn2/0304/doc/lecture/mpls.pf