M1 RES - Architecture des réseaux 9/10
Architecture support - Point-à-point

Olivier Fourmaux

olivier.fourmaux@lip6.fr

Version 4.c, septembre 2004

UNIVERSITE
PIERRE & MARIE CURIE
LA SCIENCE A PARIS

Plan

Architecture Ethernet

Architecture ATM/MPLS

Architecture point-à-point

- HDLC
- IP sur liaison série
- PPP
- contrôle de la couche liaison (LCP)
- authentification (PAP, CHAP et RADIUS)
- contrôle de la couche réseau (NCP)
- PPP sur SONET
- PPP sur ATM
- PPP sur Ethernet
- tunnel PPP
- VPN

Introduction

Communication **directe** entre deux entités

Fonctions principales en point-à-point :

- **découpage de trame** (*framming*)
- des fonctionnalités similaires à celles de la couche Transport peuvent aussi intervenir (sauf contrôle de **congestion**) :
  - ✓ contrôle d'erreur
  - ✓ contrôle de flux
  - ✓ ordonnancement (numérotation)
  - ✓ anticipation (*sliding window*)
  - ✓ fiabilité (acquittements et retransmissions)

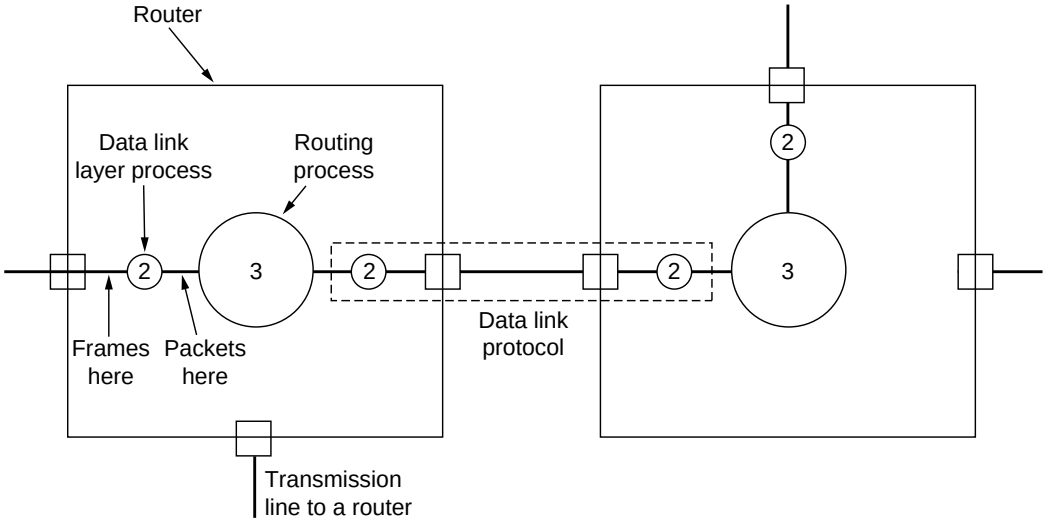
Pour le transport de données :

- pas de résolution d'adresses
- **format d'encapsulation**

Couche liaison point-à-point

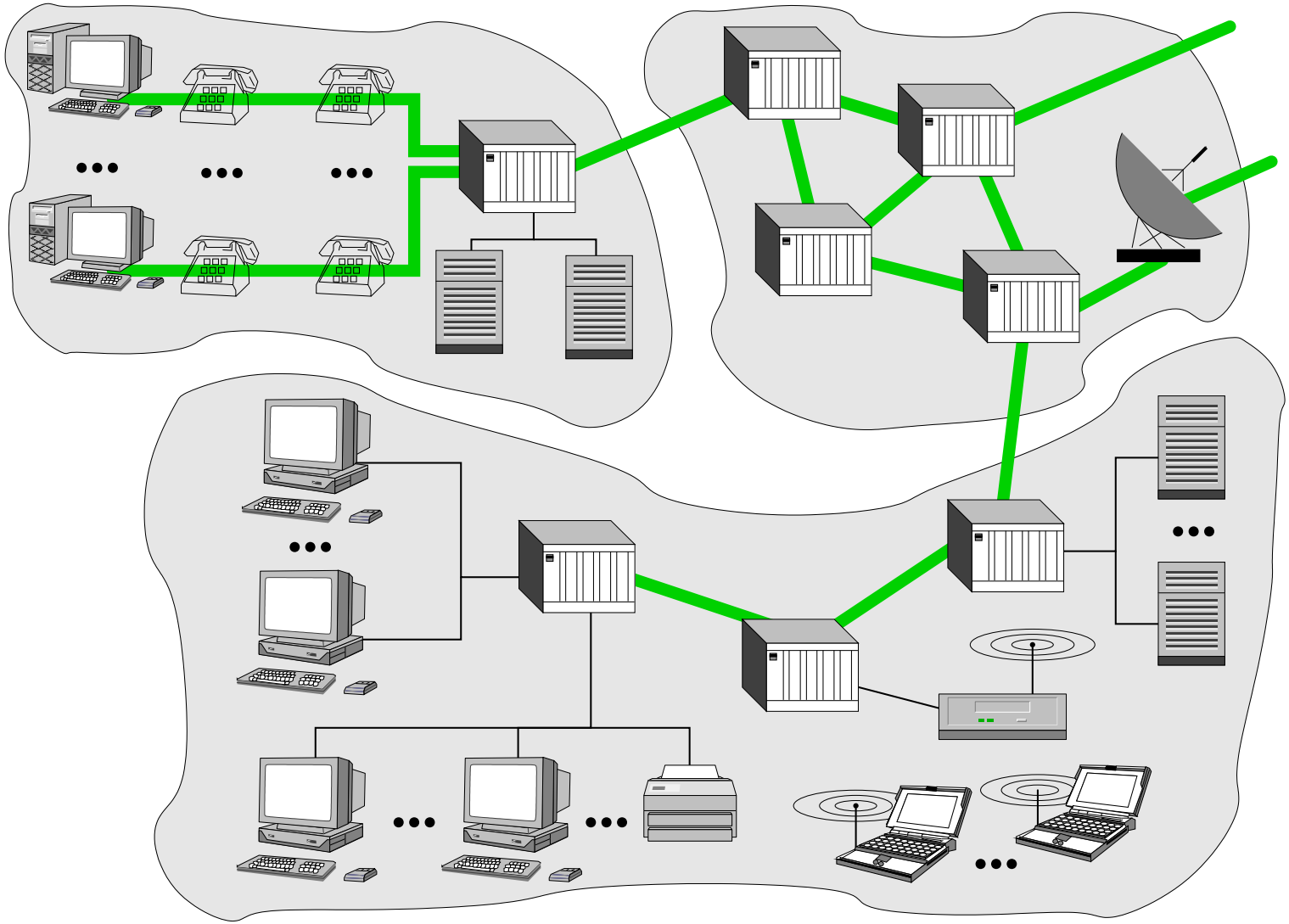
Ce service point-à-point correspond à celui de la **couche liaison** OSI

- Caractéristiques :
  - ✓ technologie d'interface homogène



  - ✓ unités de transmission variées
    - ☞ bits, octets, cellules ...
  - ✓ couches sous-jacentes variées
    - ☞ pas forcément une **couche physique**
    - ☞ avec des éléments actifs (multiplexeurs, modems, répéteurs, ponts, switch, routeur, passerelles applicatives...)

Liaisons point-à-point : Où ?



Plan

Architecture Ethernet

Architecture ATM/MPLS

Architecture point-à-point

- **HDLC**
- IP sur liaison série
- PPP
- contrôle de la couche liaison (LCP)
- authentification (PAP, CHAP et RADIUS)
- contrôle de la couche réseau (NCP)
- PPP sur SONET
- PPP sur ATM
- PPP sur Ethernet
- tunnel PPP
- VPN

HDLC : Famille

La plupart des protocoles de la couche **liaison** pour le point-à-point sont apparentés à HDLC :

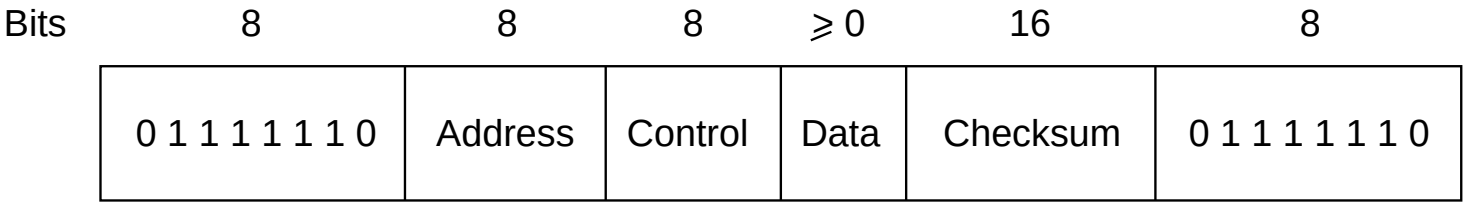
- SDLC (*Synchronous Data Link Control*) d'IBM pour SNA
- ADCCP (*Advance Data Communication Control Procedure*) normalisation de SDLC par l'ANSI
- **HDLC** (*High-level Data Link Control*) normalisation de SDLC par l'ISO
- LAP (*Link Access Procedure*) normalisation d'HDLC par l'ITU
  - ✓ LAP-B pour X25
  - ✓ LAP-D pour *ISDN*
  - ✓ LAP-F pour *Frame Relay*
- **PPP** (*Point-to-Point Protocol*) standard de l'IETF

Ces protocoles s'appuient sur une grande variété de supports **physiques** permettant de transmettre des bits entre deux machines.

HDLC : Structure

Découpage au niveau bit

- délimitation par un fanion (*flag*) de valeur binaire : `0111 1110`
- protection par *bit stuffing* (insertion d'un `0` après `11111`)



picture from TANENBAUM A. S. *Computer Networks 3rd edition*

3 types de trames (`control`) :

- **Information** : transmission de données avec *sliding window* (7 trames non acquittées max)
- **Supervisory** : contrôle de flux, ACK non *piggyback*, NACK, demande de retransmission selective...
- **Unumbered** : pour le contrôle interne à la couche liaison

Plan

Architecture Ethernet

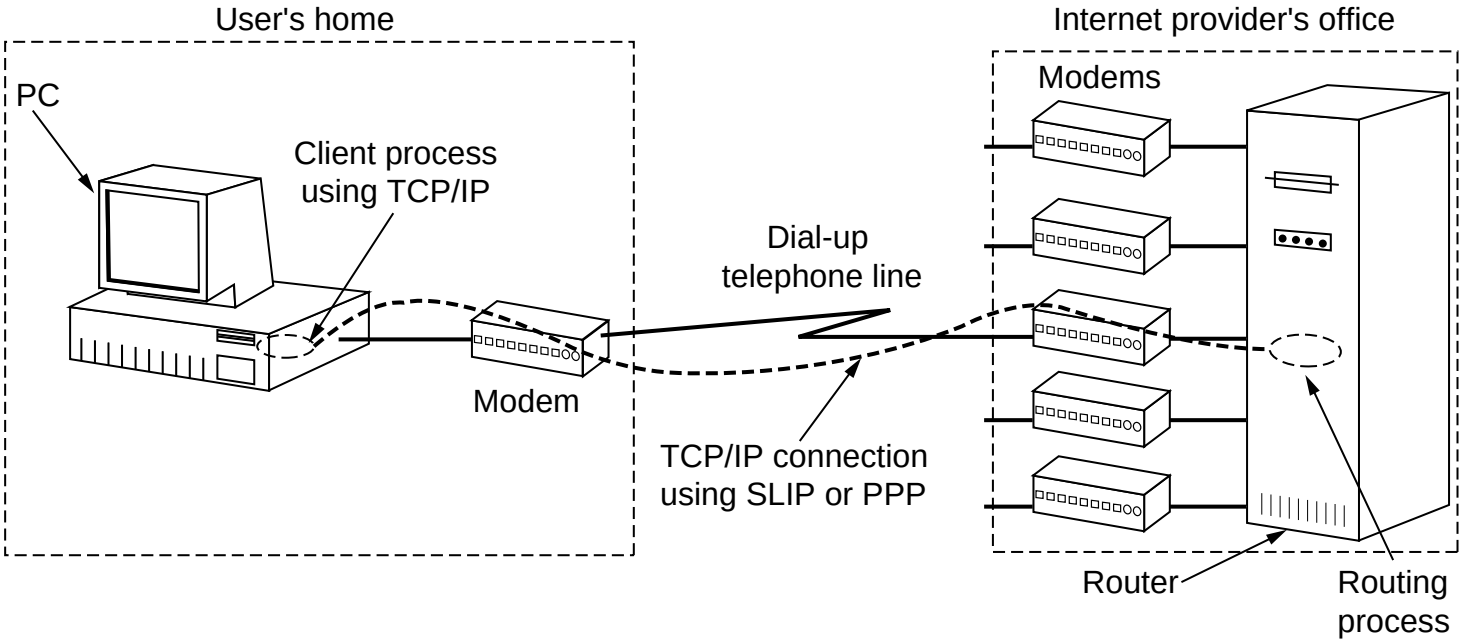
Architecture ATM/MPLS

Architecture point-à-point

- HDLC
- **IP sur liaison série**
- PPP
- contrôle de la couche liaison (LCP)
- authentification (PAP, CHAP et RADIUS)
- contrôle de la couche réseau (NCP)
- PPP sur SONET
- PPP sur ATM
- PPP sur Ethernet
- tunnel PPP
- VPN

IP sur ligne série

picture from TANENBAUM A. S. *Computer Networks 3rd edition*



- SLIP (*Serial Line Internet Protocol*)
  - ✓ orienté caractère, découpage grâce au caractère `0xC0`
  - ✓ rudimentaire : aucun contrôle, aucune négociation
- **PPP** ...

Plan

Architecture Ethernet

Architecture ATM/MPLS

Architecture point-à-point

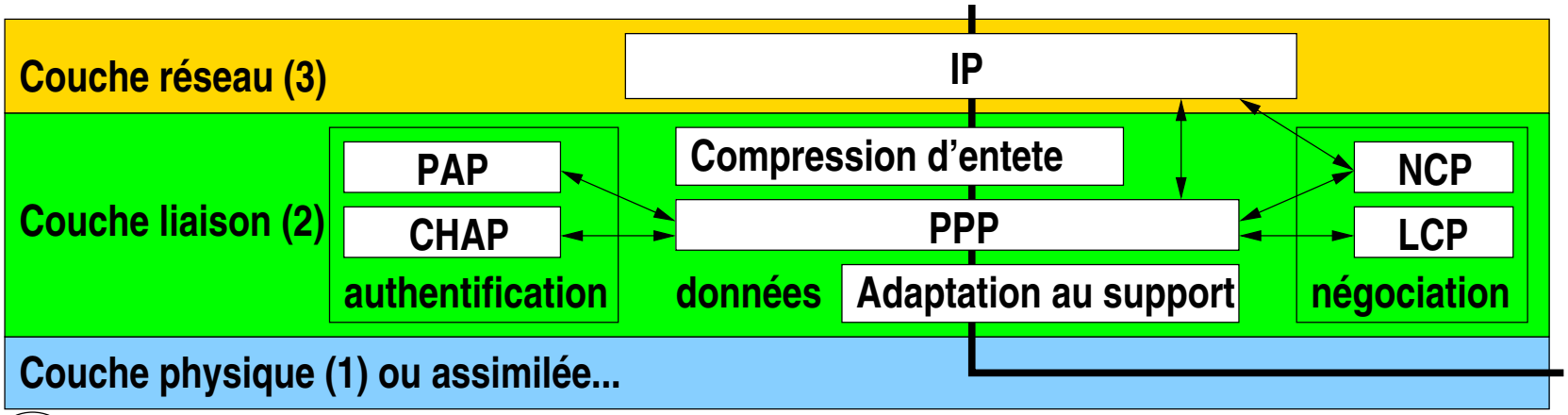
- HDLC
- IP sur liaison série
- **PPP**
- contrôle de la couche liaison (LCP)
- authentification (PAP, CHAP et RADIUS)
- contrôle de la couche réseau (NCP)
- PPP sur SONET
- PPP sur ATM
- PPP sur Ethernet
- tunnel PPP
- VPN

PPP : Introduction

Point-to-Point Protocol (RFC 1661)

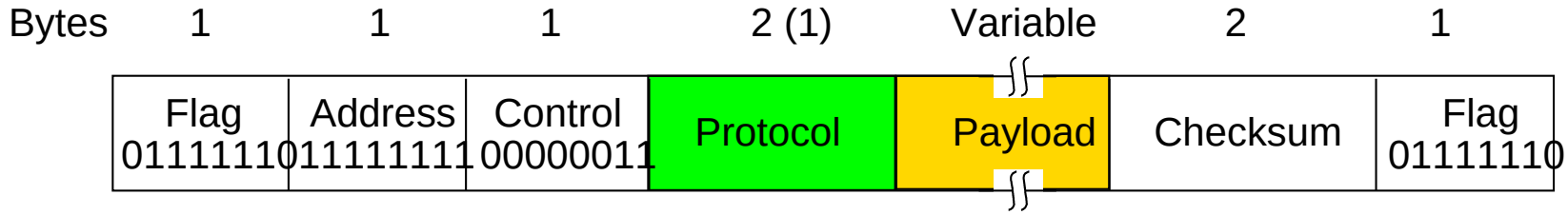
Protocole générique ➠ nombreuses fonctionnalités :

- multiprotocolaire
  - ✓ transporte d'autres niveaux 3 que IP
  - ✓ s'appuie sur d'autres technologies que les lignes séries
- négociation
  - ✓ adaptation au support
    - ☞ détection et correction d'erreur
    - ☞ compression d'entête pour les liaisons à faible débit
  - ✓ configuration automatique du client



PPP : Encapsulation

Format de la trame PPP :



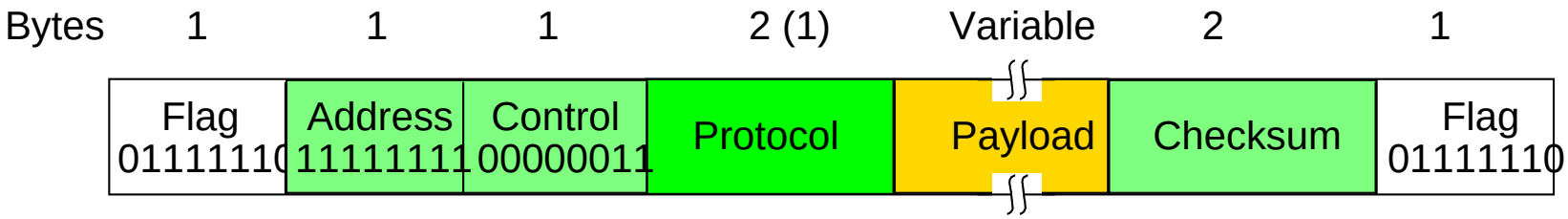
Encapsulation simple : ajout de **2 octets** (compressible à 1 octet)

- `Protocol` : indique le type d'information transportée
  - ✓ **LCP** : protocole de contrôle de la couche liaison
    - ☞ négociation des paramètres de la couche support (compression, taille des trames...)
  - ✓ **PAP** et **CHAP** : protocoles d'authentification
  - ✓ **NCP** : protocole de contrôle de la couche réseau
    - ☞ négociation des paramètres du protocole transporté (adressage...) ➠ *dépend de chaque couche réseau supportée*
  - ✓ **IP**, AppleTalk, IPX, IPv6...
- `Payload` : contient les données de la trame
  - ✓ MRU (*Maximum Receive Unit*) négociable (par défaut : 1500 o)
  - ✓ **bourrage** si la technologie support le nécessite

PPP : Protocoles encapsulés

Valeur	Description
0x0001	Protocole de bourrage
0x0021	IP
0x0029	AppelTalk
0x002B	IPX
0x002D	TCP/IP Compression d'entête de Van Jacobson
0x002F	TCP/IP Compression inefficace
0x0057	IPv6
0x0281	MPLS
0x8021	IPCP : configuration d'IP
0x8029	ATCP : configuration d'AppelTalk
0x802B	IPXCP : configuration d'IPX
0x8057	IPV6CP : configuration d'IPv6
0x8281	Configuration de MPLS
0xC021	LCP : *Link Control Protocol*
0xC023	PAP : *Password Authentification Protocol*
0xC025	LQR : *Link Quality Report*
0xC223	CHAP : *Challenge Handshake Authentification Protocol*

PPP : Format de la trame



Similaire à une trame **HDLC** pour les flux d'octets :

- un **fanion** (`flag`) de valeur binaire : `0111 1110` (`0x7E`)
- `address` (1 octet) : `1111 1111` (`0xFF`, diffusion)
  - ✓ il n'y a qu'un destinataire (point-à-point)
- `control` (1 octet) :
  - ✓ **liaison fiable** ➠ pas de contrôle : `0000 0011` (`0x03`, trame UI, voir le RFC 1662)
    - ☞ optimisation : suppression des champs `Address` et `Control`
  - ✓ **liaison peu fiable** ➠ contrôle du séquencement (voir HDLC, trames UA et SABME, voir le RFC 1663)
- `Protocol` et `Payload` : encapsulation PPP
- `Checksum` (2 octets) : CRC 16 bits
- encore un **fanion** de valeur binaire : `0111 1110`

PPP : Transparence du fanion

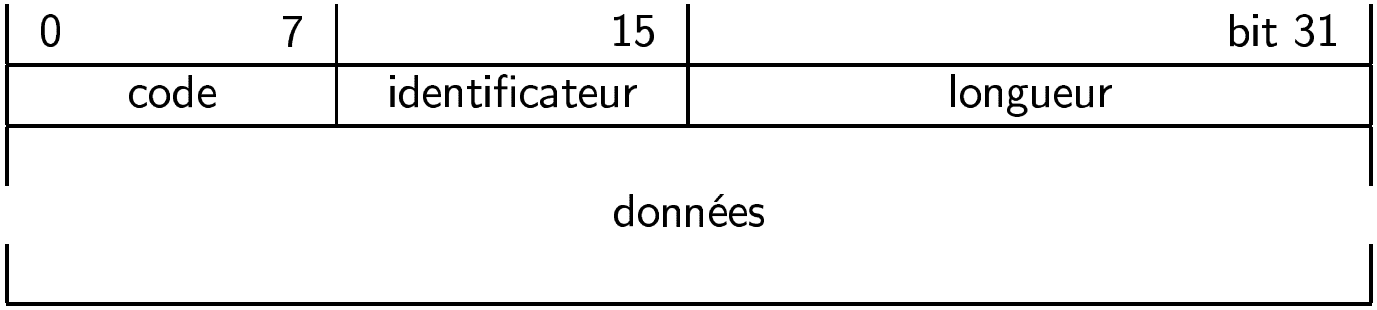
Deux types de liaison point-à-point :

- **synchrone** (bits : le fanion est la séquence `0111 1110`)
  - ✓ 1 bit à 0 est rajouté tout les 5 bits à 1
    - ☞ `01111110111110` ➠ `011111`**`0`**`101111`**`0`**`0`
- **asynchrone** (octets, le fanion à la valeur `0x7E`)
  - ✓ fanion protégé par échappement (octet de valeur `0x7D`) :
    - ☞ `0x7E` ➠ `0x7D 0x5E`
    - ☞ `0x7D` ➠ `0x7D 0x5D`
  - ✓ valeurs d'octets actives pour la gestion de la connexion asynchrone (correspond aux codes ASCII < 32), même principe de protection :
    - ☞ `0x11` (XON : reprise du transfert) ➠ `0x7D 0x31`
    - ☞ `0x13` (XOFF : arrêt du transfert) ➠ `0x7D 0x33`

➠ La bande passante disponible est **variable** !

PPP : Négociation

Structure de la trame de négociation typique de PPP :



- `code` : indique le type de négociation
- `identificateur` : mise en correspondance entre les requêtes et les réponses
- `longueur` : taille totale de la trame avec l'entête LCP
  ✓ permet de supprimer de potentiels octets de bourrage
- `données` : paramètres de la négociation

Les négociations débutent lors de l'initiation de la connexion

PPP : Trames de négociation

Valeur	Code	Description	LCP	NCP
1	`Configure-Request`	modif. aux valeurs par défaut	✔	✔
2	`Configure-Ack`	récepteur accepte toutes les mofif.	✔	✔
3	`Configure-Nak`	valeurs refusées, en proposer d'autres	✔	✔
4	`Configure-Reject`	valeurs non négociables	✔	✔
5	`Terminate-Request`	un des equipements veut terminer	✔	✔
6	`Terminate-Ack`	confirmation de la terminaison	✔	✔
7	`Code-Reject`	code inconnu	✔	✔
8	`Protocol-Reject`	protocole inconnu	✔	
9	`Echo-Request`	demande test l'état de la liaison	✔	
10	`Echo-Reply`	réponse de test de l'état de la liaison	✔	
11	`Discard-Request`	supprimées en silence par le récepteur	✔	

Plan

Architecture Ethernet

Architecture ATM/MPLS

Architecture point-à-point

- HDLC
- IP sur liaison série
- PPP
- **contrôle de la couche liaison (LCP)**
- authentification (PAP, CHAP et RADIUS)
- contrôle de la couche réseau (NCP)
- PPP sur SONET
- PPP sur ATM
- PPP sur Ethernet
- tunnel PPP
- VPN

LCP

Link Control Protocol

Supervision de l'état de la liaison

- champ `protocol` de la trame PPP : `0xC021`
- négociation initiale à l'ouverture de la connexion
- définition d'options de type TLV
  - ✓ voir RFC 1570 et **RFC 1661**
  - ✓ format :

1 octet	1 octet	(Longueur - 2) octets
Type	**Longueur**	**Valeur**

LCP : Types d'options

Valeur	Code	Taille	Description
1	MRU	4	Taille maximale des trames reçues
2	ACCM	6	table des caractères à transcoder
3	authentification	4	type du protocole d'authentification choisi
4	qualité	6	type du protocole de gestion de la QoS
5	*Magic Number*	6	négociation de cette valeur
7	compression `protocol`	2	champ de contrôle sur 1 octet
8	compression `address` et `control`	2	suppression de ces champs
10	bourrage auto-descriptif	3	paramètre d'un bourrage qui peut être automatiquement supprimé par le récepteur
13	rappel automatique	3+	...

Plan

Architecture Ethernet

Architecture ATM/MPLS

Architecture point-à-point

- HDLC
- IP sur liaison série
- PPP
- contrôle de la couche liaison (LCP)
- **authentification (PAP, CHAP et RADIUS)**
- contrôle de la couche réseau (NCP)
- PPP sur SONET
- PPP sur ATM
- PPP sur Ethernet
- tunnel PPP
- VPN

PAP

Password Authentification Protocol (RFC 1334)

Une fois la connexion établie et les paramètres LCP négociés

➠ vérification de l'identité

- champ `protocol` de la trame PPP : `0xC023`
- transmission en clair de **l'identifiant** et du **mot de passe**
- 4 types de trames de négociation (`Configure-Request`, `Configure-Ack`, `Configure-Nak` ou `Configure-Reject`)
- format identique à LCP, valeur du champ `code` :
  - ✓ 1 : **demande d'authentifiaction**

format :

1 o.	(LgId) octets	1 o.	(LgMP) octets
LgId	**Identificateur**	**LgMP**	**Mot_de_passe**

  - ✓ 2 : **acquittement positif**

format :

1 o.	(LgId) octets
LgId	**Message_pour_le_client**

  - ✓ 3 : **acquittement négatif** (retransmission nécéssaire)

format :

1 o.	(LgId) octets
LgId	**Message_pour_le_client**

CHAP

CHallenge Authentification Protocol (RFC 1334)

Après la négociation LCP et pendant la communication

➠ vérification de l'identité (suite)

- champ `protocol` de la trame PPP : `0xC223`
- les 2 extrémités possèdent une **clé** identique et secrète
- 4 types de trames de négociation (`Configure-Request`, `Configure-Ack`, `Configure-Nak` ou `Configure-Reject`)
- format identique à LCP, valeur du champ `code` :
  - ✓ 1 : **challenge** (envoi d'une séquence binaire)

    format :

1 o.	(LgCh) octets
LgCh	**séquence_binaire**

  - ✓ 2 : **réponse** (retour de la séquence cryptée avec la **clé** ➠ sceau)

    format :

1 o.	(LgCC) octets
LgCC	**séquence_binaire_cryptée**

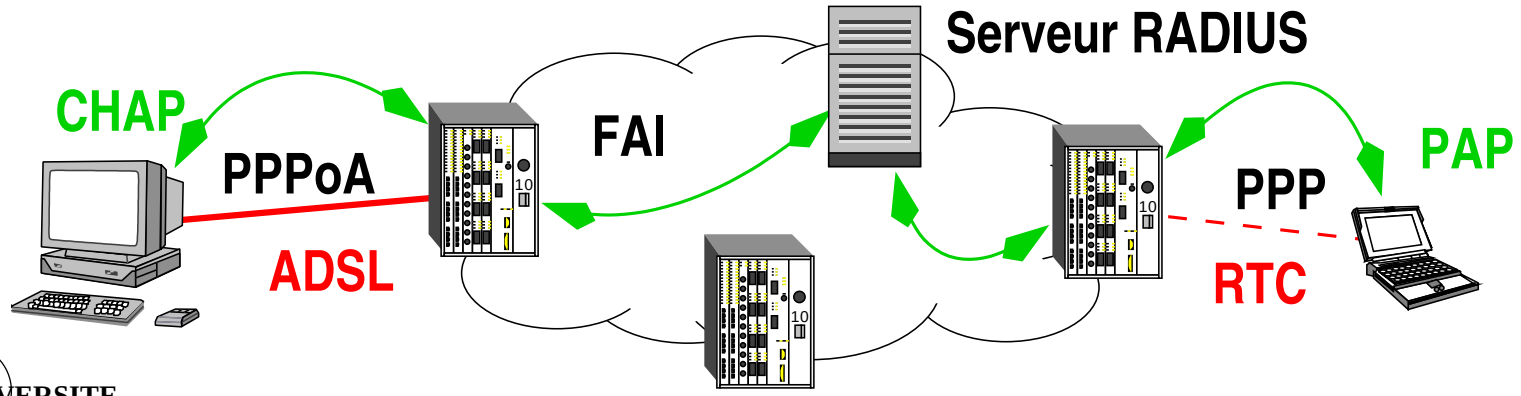
  - ✓ 3 : **succès** : la séquence cryptée reçue et celle calculée localement sont identiques
  - ✓ 4 : **échec** (retransmission nécéssaire)

RADIUS (1)

Remote Authentication Dial-In User Service (RFC 2865)

Centralisation des informations concernant un utilisateur

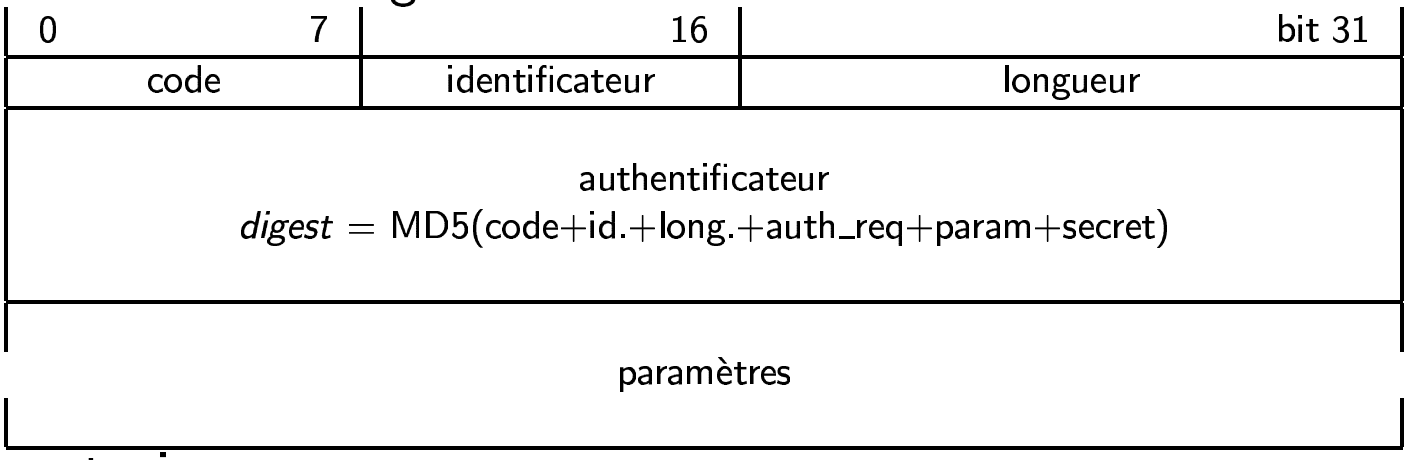
- fonctions AAA : *Authentication*, *Authorization*, and *Accounting*
  - ✓ vérification de l'identité
  - ✓ connaitre les droits et configuration d'accès
  - ✓ suivre les actions de l'utilisateur
- modèle client/serveur
  - ✓ le client peut se connecter aux différents points d'accès d'un FAI
    - ☞ client : point d'accès au FAI (extrémité PPP, ou autre protocole)
    - ☞ serveur : supporte une base de données utilisateurs du FAI



RADIUS (2)

Service sans connexion (**UDP port 1812**)

- fiabilité gérée au niveau applicatif
- format du message :



Echange typique :

- message `Access-Request` du client d'accès
  - ✓ nom de l'utilisateur, mot de passe crypté
  - ✓ adresse IP du point d'accès, port UDP
  - ✓ type de session (PPP, rlogin, telnet...)
- réponse `Access-Accept` du serveur RADIUS
  - ✓ liste d'attributs à utiliser pour la session (adresse, serveurs...)
- réponse `Access-Reject` du serveur RADIUS
  - ✓ si l'utilisateur n'est pas dans la base ou n'a pas accès au service

Plan

Architecture Ethernet

Architecture ATM/MPLS

Architecture point-à-point

- HDLC
- IP sur liaison série
- PPP
- contrôle de la couche liaison (LCP)
- authentification (PAP, CHAP et RADIUS)
- **contrôle de la couche réseau (NCP)**
- PPP sur SONET
- PPP sur ATM
- PPP sur Ethernet
- tunnel PPP
- VPN

NCP

Network Control Protocol

Après la configuration de la liaison (LCP) et une authentification optionnelle (PAP ou CHAP), **configuration des protocoles de couche 3**

- un NCP par protocole transporté :
  - ✓ IPCP pour la configuration IPv4 (RFC 1332)
  - ✓ IPV6CP pour la configuration IPv6 (RFC 2472)
  - ✓ ATCP pour la configuration AppleTalk (RFC 1378)
  - ✓ IPXCP pour la configuration IPX (RFC 1552)
  - ✓ OSINLCP pour la configuration des protocoles de l'OSI (RFC 1377)
  - ✓ ...

IPCP

Internet Protocol Control Protocol

- champ `protocol` de la trame PPP : `0x8021`
- 4 types de trames de négociation (`Configure-Request`, `Configure-Ack`, `Configure-Nak` ou `Configure-Reject`)
- format identique à LCP, valeur du champ `code` :
  - ✓ 2 : **compression d'entête**
    - ☞ 2 octets pour le type de compression (`0x002d` pour **Van Jacobson** ; `0x0061` pour **étendu**, RFC 2507 ; `0x0003` pour **ROHC**, *RObust Header Compression*, RFC 3241)
    - ☞ 1 octet pour le nombre max de connexions compressées
    - ☞ 1 octet pour indiquer la présence du numéro de connexion
  - ✓ 3 : **adresse IP** du client sur 4 octets
  - ✓ 4 : **adresse IP permanente** (*home address*)
  - ✓ 129 : adresse IP du **serveur DNS primaire**
  - ✓ 130 : adresse IP du **serveur NBNS primaire**
  - ✓ 131 : adresse IP du **serveur DNS secondaire**
  - ✓ 132 : adresse IP du **serveur NBNS secondaire**

Compression d'entête TCP/IP

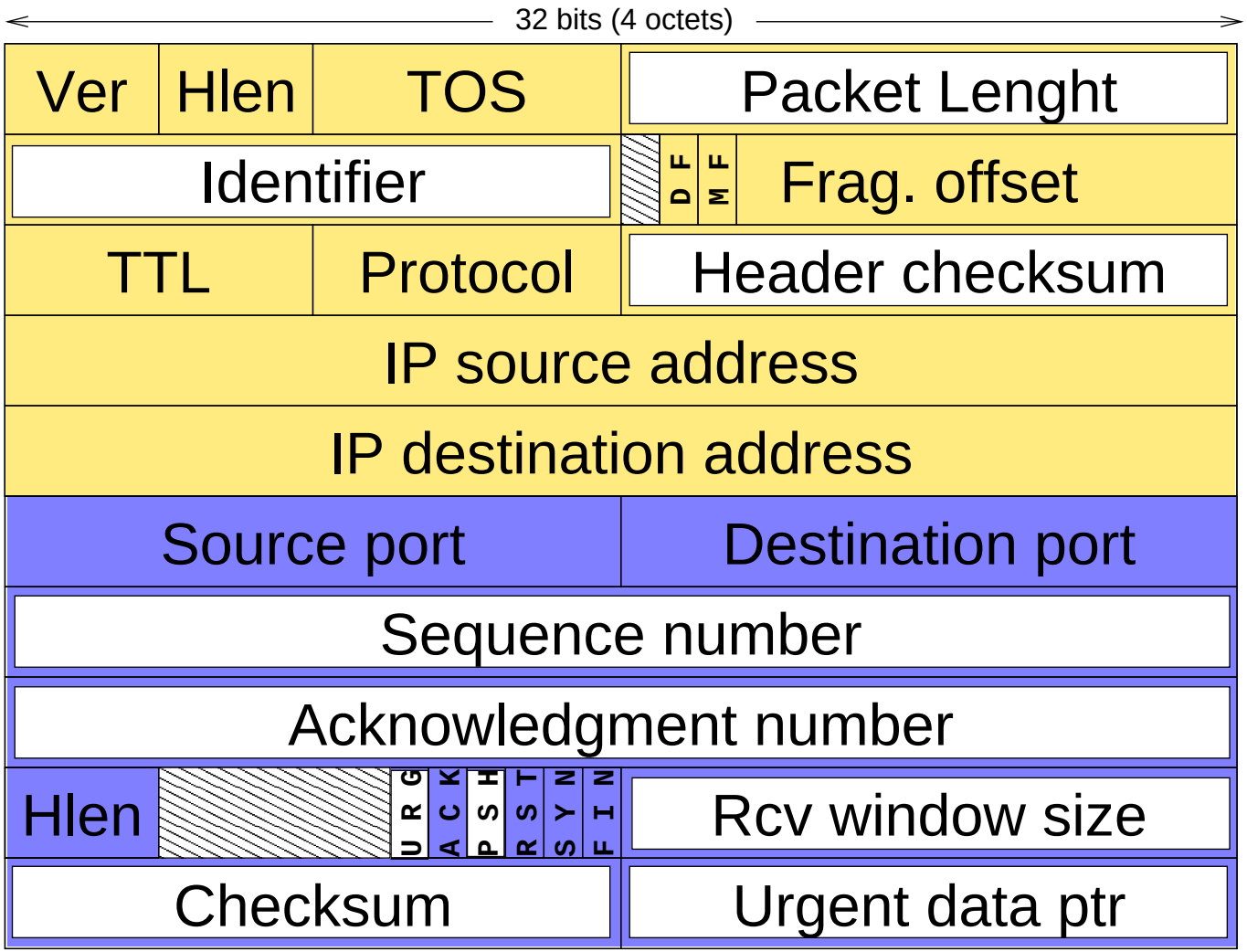
PPP doit être efficace sur les liaisons à bas débit

- connexion TCP/IP interactive (`telnet`...)
  - ✓ algorithme de Nagle
  - ✓ taille importante des entêtes
  - ✓ exemple :

```
trame 1 (A->B)
0000   00 07 e9 0c 90 62 00 20   ed 87 fd e6 08 00 45 00
0010   00 28 b5 8e 40 00 40 06   0d bf 84 e3 3d 7a cb 10
0020   ea 14 81 cf 00 50 52 40   18 64 52 65 10 0d 50 10
0030   2d a0 bb 7b 00 00

trame 2 (A->B)
0000   00 07 e9 0c 90 62 00 20   ed 87 fd e6 08 00 45 00
0010   00 28 b5 8f 40 00 40 06   0d be 84 e3 3d 7a cb 10
0020   ea 14 81 cf 00 50 52 40   18 64 52 65 15 c1 50 10
0030   39 08 aa 5f 00 00
```

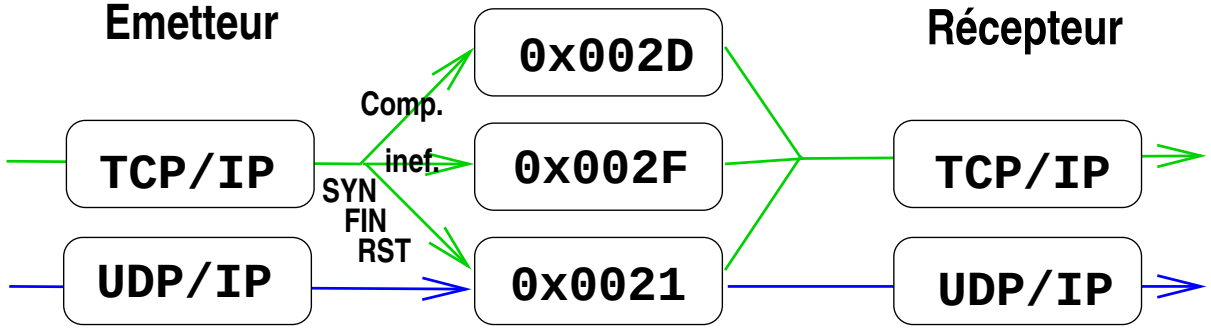
Différence entre deux segments



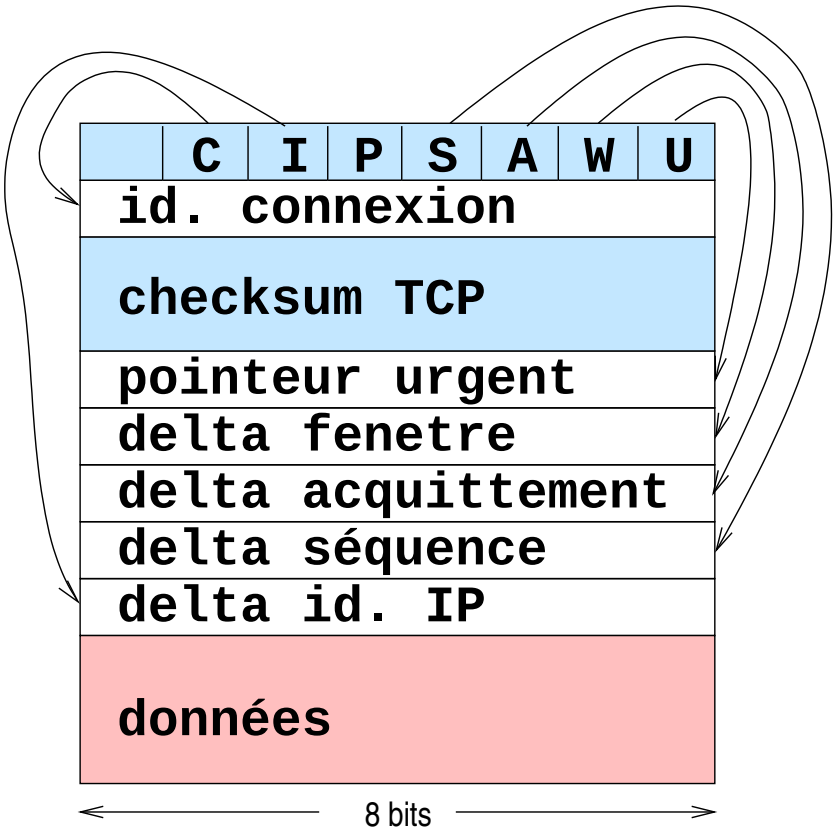
Algorithme de Van Jacobson

Algorithme de compression des entêtes TCP/IP (RFC 1144)

- émission des entêtes classiques pour SYN, RST et FIN (champ `protocol` à `0x0021`)
- puis compression :
  - ✓ envoi complet avec l'**identificateur** de connexion (`0x002F`) :
    - ☞ pour la synchronisation (premier paquet complet)
    - ☞ pour les valeurs négatives d'acquitement ou de séquence (erreur)
  - ✓ **différentiel** entre deux entêtes (`0x002D`) :
    - ☞ identificateur de connexion
    - ☞ maintient d'un **contexte** à chaque extrémitée
    - ☞ seuls les champs modifiés sont transmis
    - ☞ la différence est généralement codée sur un octet



Entête IP compressé

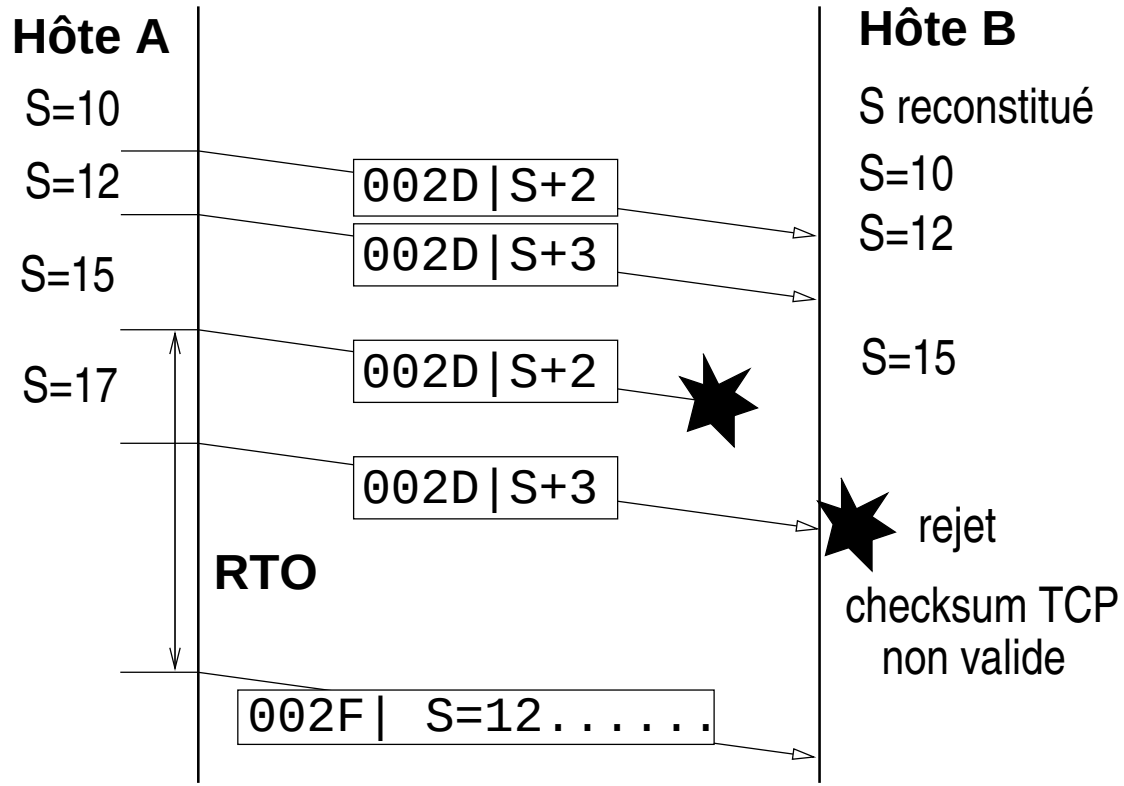


Seul le premier octet et `cheksum TCP` sont obligatoires (3 octets mini)

- la présence des champs est indiquée dans le premier octet
- les delta sont codés sur 1 à 2 o.
  - ✓ 1 octet :`0x01` à `0xFF`
  - ✓ 3 o. : `0x000100` à `0x00FFFF`
- bit `C` : présence `id. connex.`
  - ✓ non émis si idem précédent
- `checksum TCP` : recopie
- bit `U` : recopie
- bit `W` : `delta fenetre`
  - ✓ négatif en complément à 2
- bits `S`/`A` : `delta seq.`/`acq.`
  - ✓ pas de négatifs
- bit `I` : `delta id. IP`
  - ✓ absent $= +1$
- bit `P` : recopie bit `PUSH` TCP

Détection d'erreur

Validation de la reconstitution avec la correspondance du `checksum TCP` :



Plan

Architecture Ethernet

Architecture ATM/MPLS

Architecture point-à-point

- HDLC
- IP sur liaison série
- PPP
- contrôle de la couche liaison (LCP)
- authentification (PAP, CHAP et RADIUS)
- contrôle de la couche réseau (NCP)
- **PPP sur SONET**
- PPP sur ATM
- PPP sur Ethernet
- tunnel PPP
- VPN

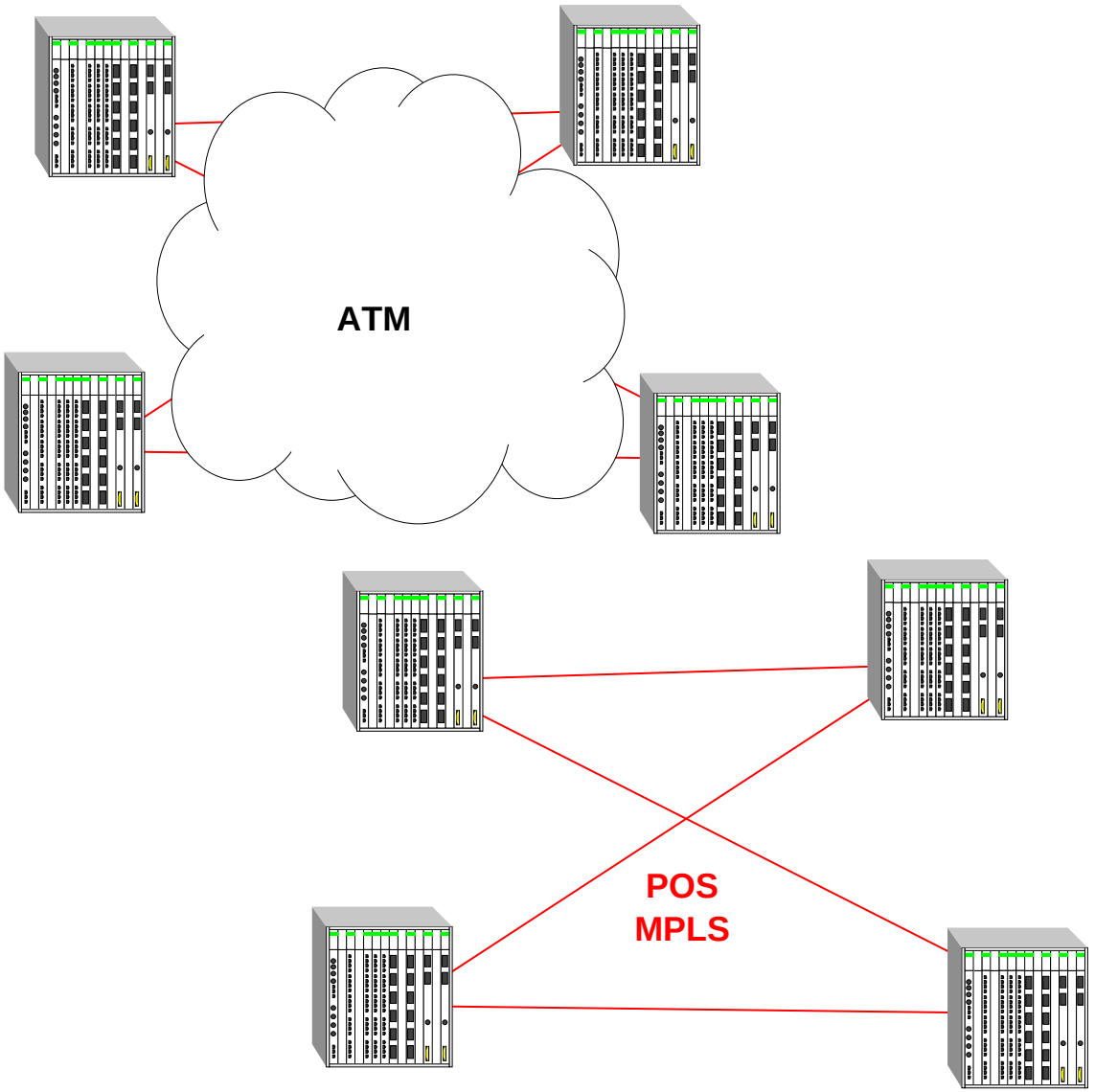
POS (1)

Packet Over SONET

PPP Over SONET/SDH (RFC 2615)

- PPP initialement pour les liaisons RTC à faible débit
- mais aussi adapté aux **liaisons à haut débit** du monde télécom
  - ✓ hiérarchies des multiplexes SONET/SDH
    - ☞ OC-3c/STM-1 (155 Mbps)
    - ☞ OC-12c/STM-4c (622 Mbps)
    - ☞ OC-48c/STM-16c (2.5 Gbps)
    - ☞ OC-192c/STM-64c (10 Gbps)
  - ✓ PPP sur liaisons synchrones basées sur des octets
    - ☞ $\sim$ connexions série orientée octet
- but : se rapprocher de la fibre
  - ✓ POS simplifie l'approche IP/ATM/SONET
    - ☞ MPLS/POS plus souple (*Traffic Eng.*)

POS (2)



Plan

Architecture Ethernet

Architecture ATM/MPLS

Architecture point-à-point

- HDLC
- IP sur liaison série
- PPP
- contrôle de la couche liaison (LCP)
- authentification (PAP, CHAP et RADIUS)
- contrôle de la couche réseau (NCP)
- PPP sur SONET
- **PPP sur ATM**
- PPP sur Ethernet
- tunnel PPP
- VPN

PPPoA

PPP Over ATM

PPP Over AAL5 (RFC 2364)

- Utilisation des connexions ATM **AAL 5**
  - ✓ plus de *framing* HDLC
  - ✓ adaptation au trames CPCS PDU AAL 5
    - ☞ *padding* (multiples de 48 octets)
- deux encapsulation RFC 1483 :
  - ✓ *VC-multiplexed PPP*
    - ☞ les extrémités savent qu'elles transportent du PPP
  - ✓ *LLC encapsulated PPP*

PPPoA : Encpsulations

VCMUX

Protocol Identifier (8 or 16 bits)	
... PPP information field ...	PPP payload
PAD (0 - 47 octets)	
CPCS-UU (1 octet) CPI (1 octet) Length (2 octets) CRC (4 octets)	CPCS-PDU Trailer

SNAP/LLC

Destination SAP (0xFE) Source SAP (0xFE) Frame Type = UI (0x03)	LLC header
NLPID = PPP (0xCF)	
Protocol Identifier (8 or 16 bits)	
... PPP information field ...	PPP payload
PAD (0 - 47 octets)	
CPCS-UU (1 octet) CPI (1 octet) Length (2 octets) CRC (4 octets)	CPCS-PDU Trailer

PPPoA : Critiques

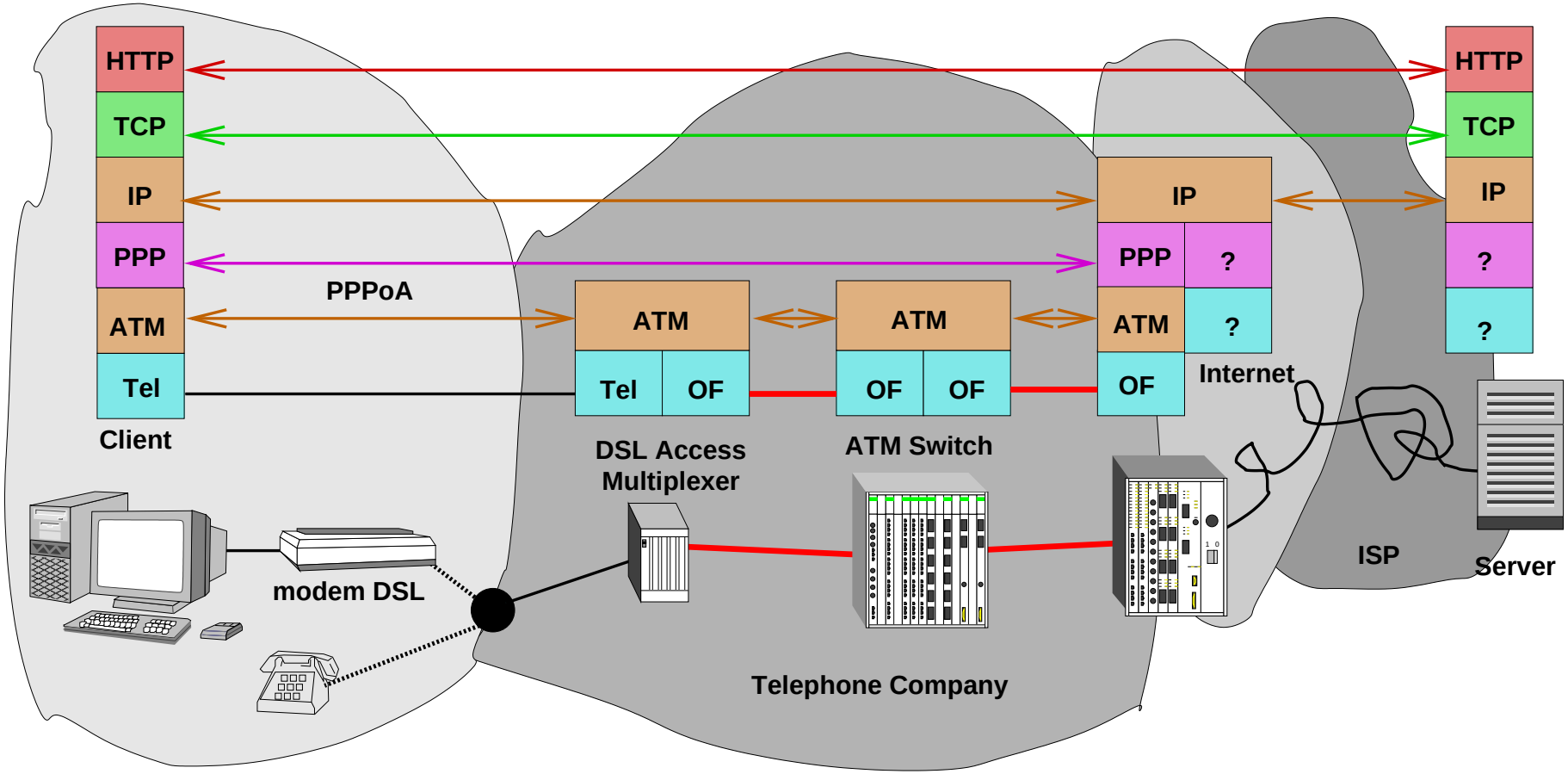
Avantages

- dissocie le fournisseur d'accès ADSL/ATM du FAI
- **authentification** par session (PAP et CHAP)
- surveillance des utilisateurs (**RADIUS**)
  - ✓ facturation des utilisateurs à la session
  - ✓ sur-réservation et déconnexions temporisées
- attribution d'**une adresse IP** au client
  - ✓ possibilité d'en gérer plus avec NPAT
- **sécurisation** de l'accès sans gestion au niveau ATM
  - ✓ signalisation ATM trop complexe : utilisation de PVC
  - ✓ VPN géré par des tunnels (voir L2TP)
- **adaptable** aux évolutions du réseau
  - ✓ gestion souple au niveau IP
    - ☞ déploiement de routeurs d'agrégation (terminaison PPP)

Inconvénients

- une connexion par PVC
- complexité globale de la solution (maitrise IP, PPP, AAA, ATM...)
- NPAT limite les applications

PPPoA sur ADSL



Plan

Architecture Ethernet

Architecture ATM/MPLS

Architecture point-à-point

- HDLC
- IP sur liaison série
- PPP
- contrôle de la couche liaison (LCP)
- authentification (PAP, CHAP et RADIUS)
- contrôle de la couche réseau (NCP)
- PPP sur SONET
- PPP sur ATM
- **PPP sur Ethernet**
- tunnel PPP
- VPN

PPPoE (1)

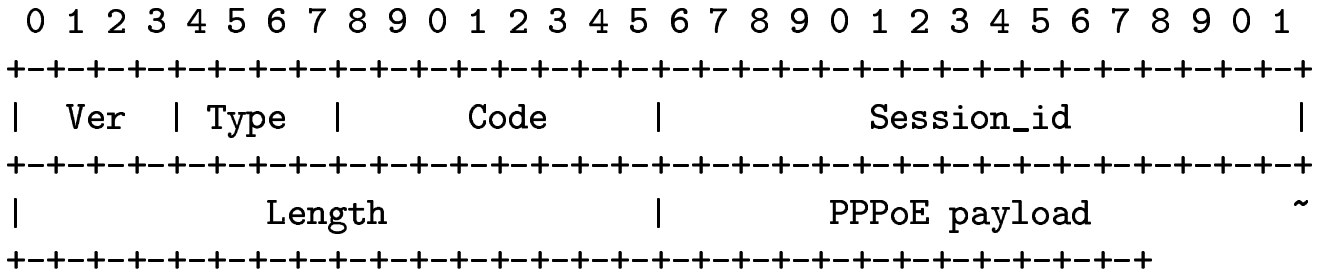
PPP Over Ethernet (RFC 2516)

Quel est l'intérêt de faire du point-à-point sur un support partagé ?

- Ethernet dispose d'autoconfiguration : ARP, de DHCP...
- ... mais pas de prise en charge à distance, ni de AAA

Mise en place d'une connexion point-à-point :

- valeurs `Ethertype`
  - ✓ `0x8863` pour les **trames de découverte**
  - ✓ `0x8864` pour les **trames de données**
- format du `payload` de ces trames Ethernet

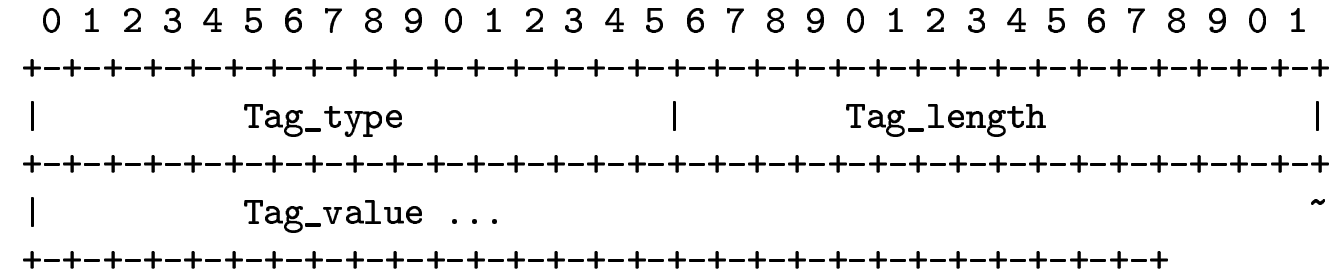


  - ✓ `Ver` et `Type` = `0x01`
  - ✓ `Code` = 00 (données) et ... (découverte)
  - ✓ `Session_id` = identification d'un flux (avec l'@ MAC)
  - ✓ `Length` = taille des données (élimination du bourrage)

PPPoE (2)

Messages de découverte

- encapsulé dans des trames PPPoE (`Ethertype` = `0x8863`)
  - ✓ champ `Code` :
    - ☞ 0x09 : PADI (*PPPoE Active Discovery Initiation*) ➠ diffusion
    - ☞ 0x07 : PADO (*PPPoE Active Discovery Offer*) ➠ proposition (avec `Session_id`)
    - ☞ 0x19 : PADR (*PPPoE Active Discovery Request*) ➠ selection
    - ☞ 0x65 : PADS (*PPPoE Active Discovery Session-confirmation*)
    - ☞ 0xA7 : PADT (*PPPoE Active Discovery Terminate*)
  - ✓ champ `PPPoE payload` : TLV avec caractères codées en UTF-8



  - ☞ nom du FAI, nom du concentrateur d'accès, identificateur de session, *cookie* de validation, nature d'une erreur...

PPPoE : Critiques

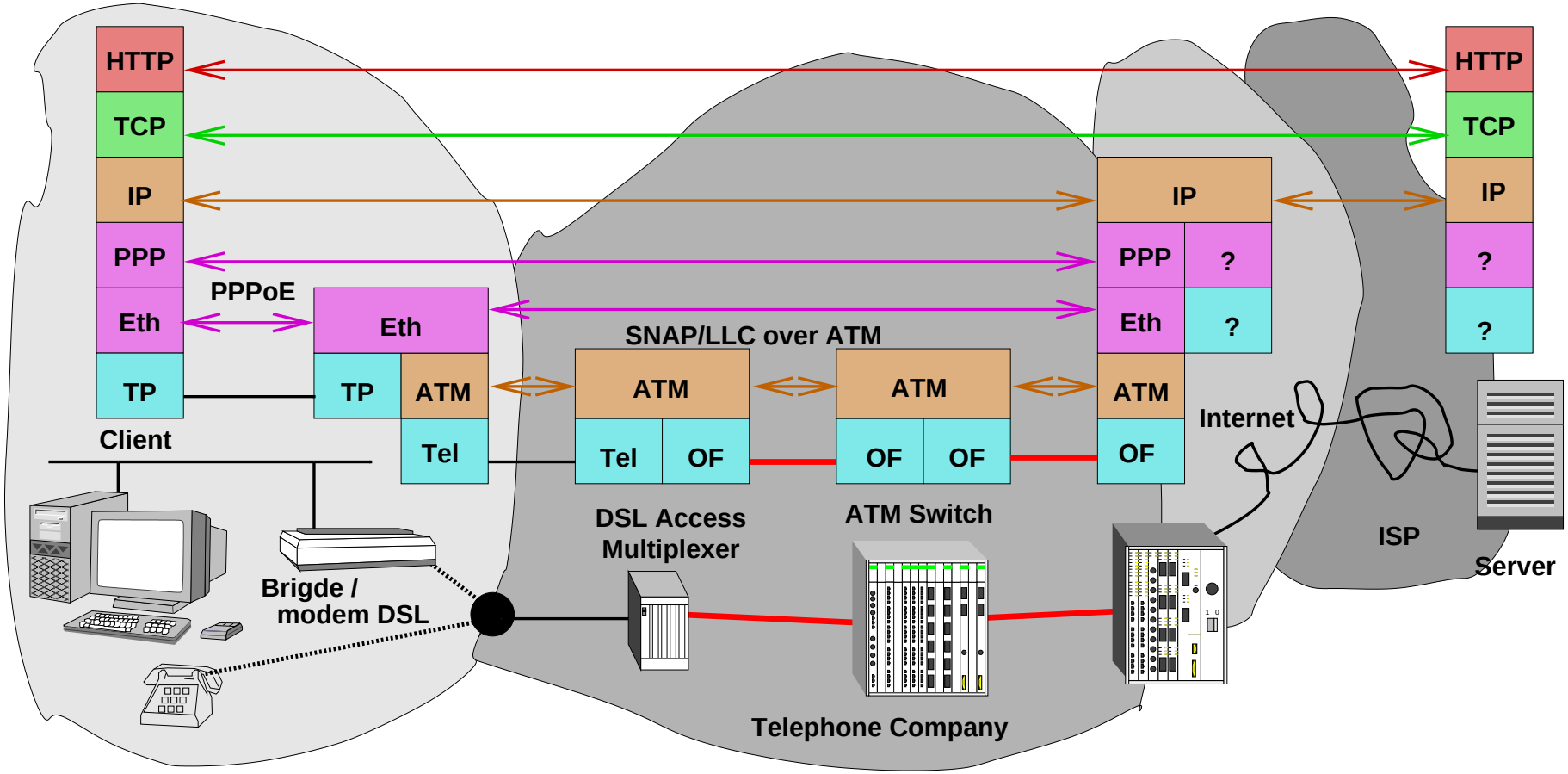
Avantages

- similaires à ceux de PPPoA
- **authentification** par session (PAP et CHAP)
  - ✓ dans un réseau de type LAN
- surveillance des utilisateurs (**RADIUS**)
  - ✓ facturation des utilisateurs à la session
  - ✓ sur-réservation et déconnexions temporisées
- utilisateurs sans accès direct à ATM (**pontage**)
- plusieurs connexions par PVC
- attribution d'**une adresse IP** au client
  - ✓ préserve le modèle point-à-point sur un médium partagé
  - ✓ possibilité de gérer plusieurs adresses avec NPAT

Inconvénients

- technologie LAN, sujet au raffales de **broadcast**
- complexité globale de la solution (maitrise IP, PPP, AAA, ATM, LAN + pontage ...)
- NPAT limite toujours les applications

PPPoE sur ADSL



Plan

Architecture Ethernet

Architecture ATM/MPLS

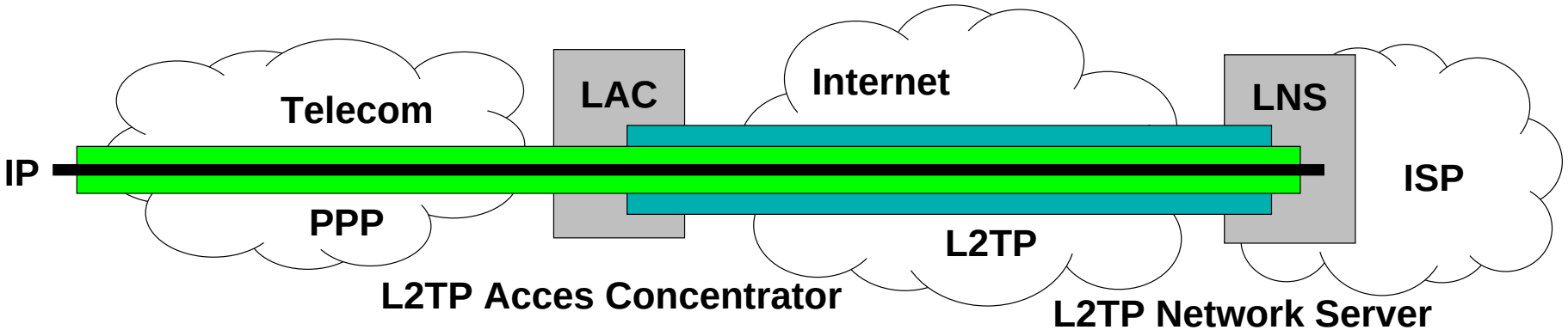
Architecture point-à-point

- HDLC
- IP sur liaison série
- PPP
- contrôle de la couche liaison (LCP)
- authentification (PAP, CHAP et RADIUS)
- contrôle de la couche réseau (NCP)
- PPP sur SONET
- PPP sur ATM
- PPP sur Ethernet
- **tunnel PPP**
- VPN

L2TP (1)

Dans l'accès ADSL,

- le fournisseur d'accès ADSL (FAA) gère la liaison jusqu'à un concentrateur d'accès (CA)
- comment atteindre le fournisseur de service Internet (FAI) ?
  - ✓ CA chez le FAI (au service d'un seul FAI)
  - ✓ le FAA gère la configuration IP (délégation du FAI)
  - ✓ le FAI à un accès à chaque CA (trop lourd)
    - ☞ création d'un tunnel du CA vers le FAI
    - ☞ relayage de PPP à travers le réseau entre le FAA et le FAI

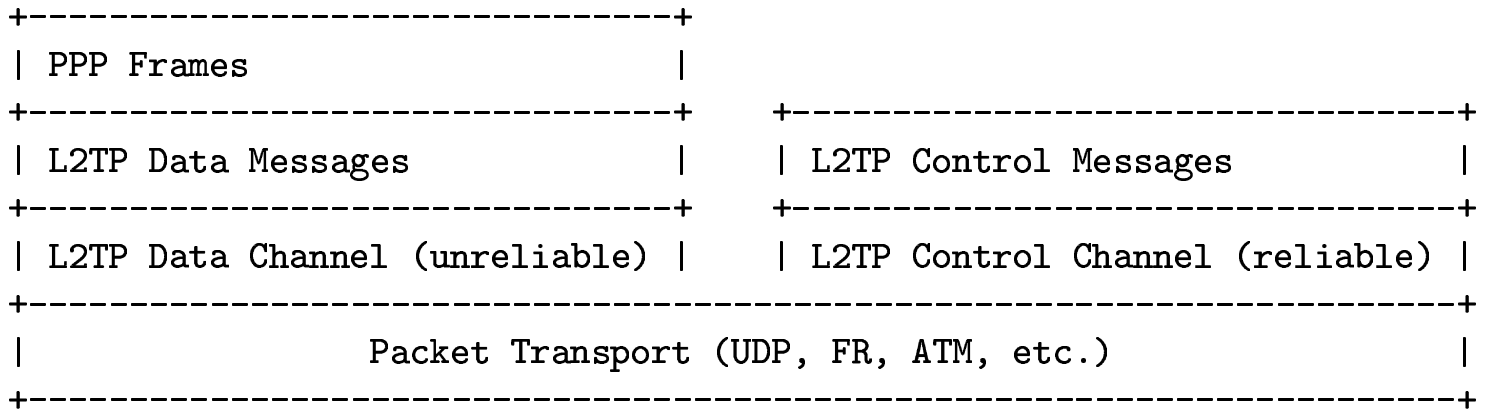


L2TP (2)

Layer 2 Tunneling Protocol (RFC 2661)

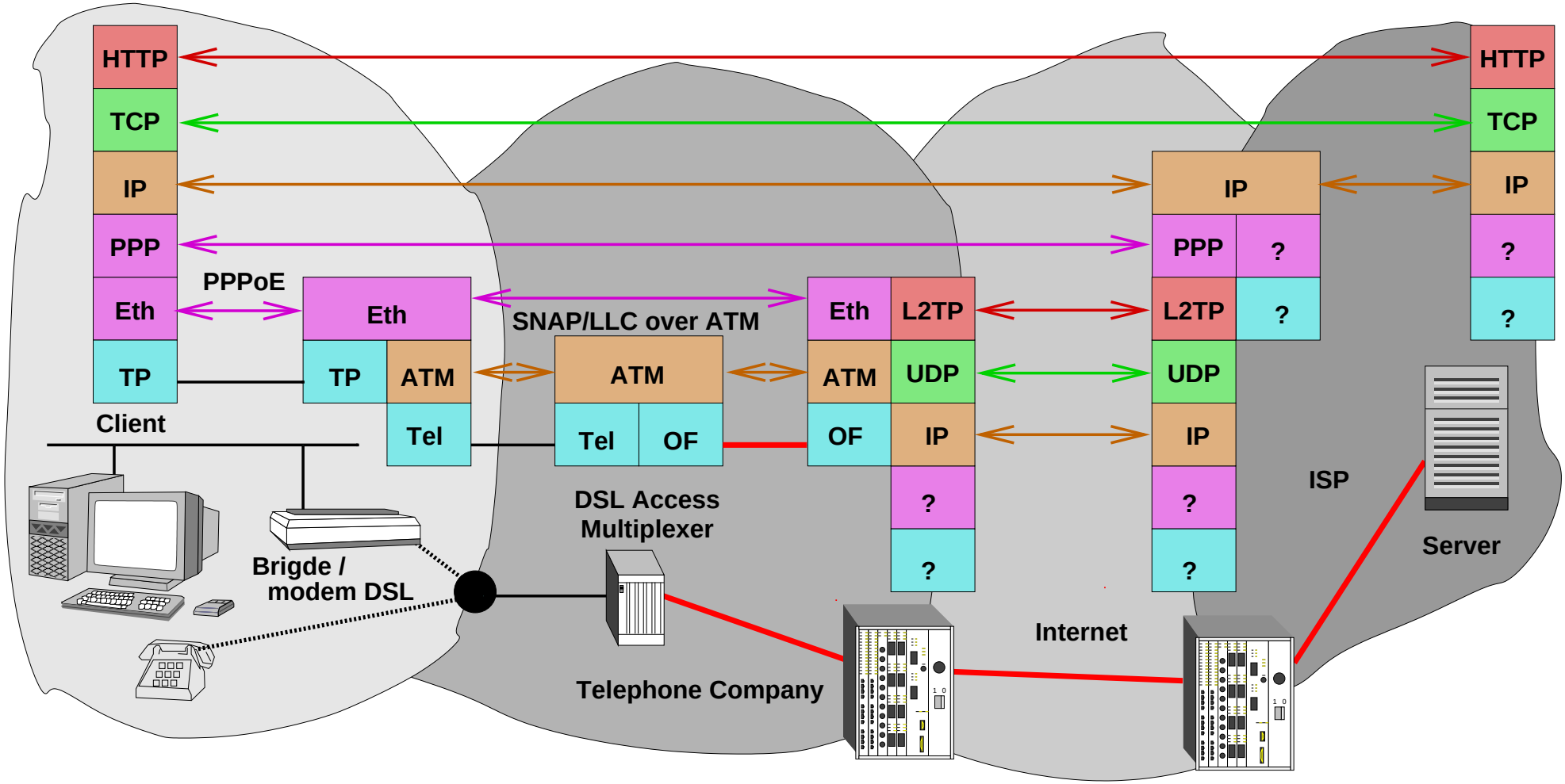
Encapsulation des trames PPP sur :

- réseaux télécom (ATM, FR...)
- Internet (UDP **port 1702**)
  - ✓ architecture L2TP :



  - ☞ `Data Channel` : trames PPP encapsulées dans des messages L2TP non fiable non sécurisé
  - ☞ `Control Channel` : échange de messages de contrôle des tunnels, avec protocole de fiabilité et de contrôle de flux spécifique

ADSL et L2TP


HTTP
TCP
IP
PPP
Eth
TP
PPPoE
Eth
TP
ATM
Tel
Client
SNAP/LLC over ATM
ATM
Tel
OF
Eth
ATM
OF
L2TP
UDP
IP
?
?
DSL Access
Multiplexer
Brigde /
modem DSL
Telephone Company
Internet
IP
PPP
?
L2TP
?
UDP
IP
?
?
ISP
Server
HTTP
TCP
IP
?
?

Plan

Architecture Ethernet

Architecture ATM/MPLS

Architecture point-à-point

- HDLC
- IP sur liaison série
- PPP
- contrôle de la couche liaison (LCP)
- authentification (PAP, CHAP et RADIUS)
- contrôle de la couche réseau (NCP)
- PPP sur SONET
- PPP sur ATM
- PPP sur Ethernet
- tunnel PPP
- **VPN**

VPN

Blabla...

Fin

Document réalisé avec LaTeX.
Généré le 29 novembre 2004.
Classe de document `foils`.
Dessins réalisés avec `xfig`.

Olivier Fourmaux, `olivier.fourmaux@lip6.fr`
`http://www-rp.lip6.fr/~fourmaux`

Ce document est disponible en postscript compressé avec gzip à
`http://www-rp.lip6.fr/~fourmaux/res/res4c9c-.pdf`