PPP : Point to point Protocol

Christophe Deleuze
Grenoble INP/ESISAR

NE424 – 2023/2024

Plan

Plan

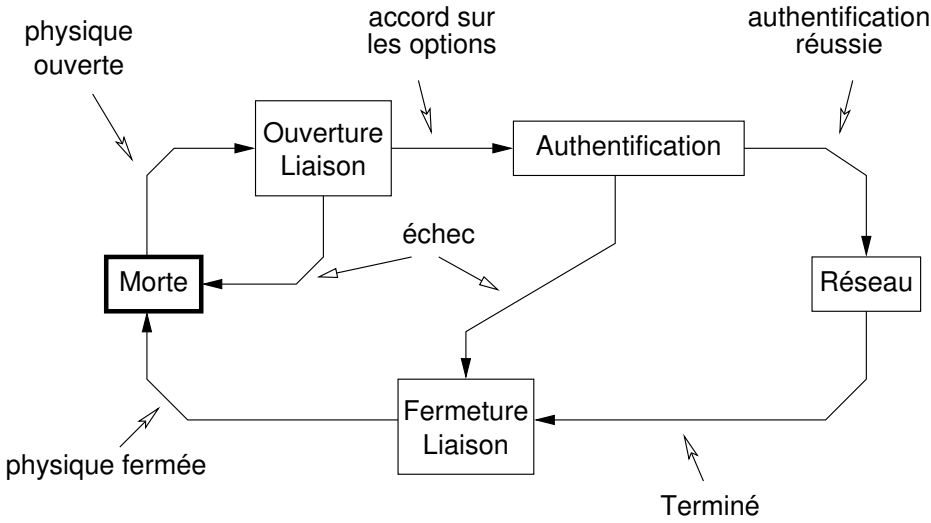
PPP : Point to Point Protocol

- Protocole de couche liaison pour liens point à point
- ex. connexion internet par ligne téléphonique (puis ADSL)
  - entre PC (ou box) et NAS
- défini dans les RFC 1661,2,3 (1994)
- premières versions dès 1989

fournit :

1. format de trame pour encapsulation
2. établissement, test et configuration de la liaison : *Link control protocol* (LCP)
3. configuration pour la couche réseau : famille de *network control protocol* (NCP)

Phases de PPP



Encapsulation

Format de la trame

Octets	1	1	1	2 (1)	Variable	Variable	2	1
Fanion 01111110	Adresse 11111111	Contrôle 00000011	Protocole	Données	Bourrage	FCS	Fanion 01111110	

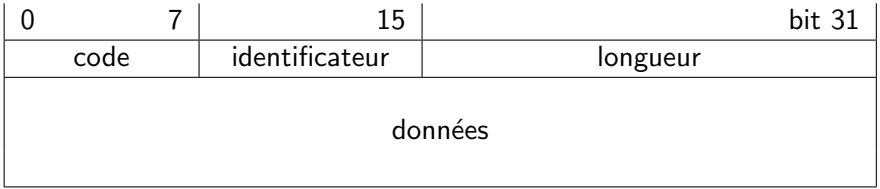
Protocole :

- **LCP**: protocole de contrôle de la couche liaison
  - négociation des paramètres de la liaison (taille des trames...)
- **PAP**, **CHAP** et **EAP**: protocoles d'authentification
- un **NCP**: protocole de contrôle de la couche réseau
  - négociation des paramètres du (d'un) protocole transporté (adressage...) → *dépend de chaque couche réseau supportée*
- **IP**, AppleTalk, IPX, IPv6...

Protocole	Description
0x0001	Protocole de bourrage
0x0021	IP
0x0029	AppleTalk
0x002B	IPX
0x002D	TCP/IP Compression d'entête de Van Jacobson
0x002F	TCP/IP Compression VJ non compressé
0x0057	IPv6
0x8021	IPCP: configuration d'IP
0x8029	ATCP: configuration d'AppleTalk
0x802B	IPXCP: configuration d'IPX
0x8057	IPv6CP: configuration d'IPv6
0xC021	LCP: *Link Control Protocol*
0xC023	PAP: *Password Authentification Protocol*
0xC025	LQR: *Link Quality Report*
0xC223	CHAP: *Challenge Handshake Authentification Protocol*

Plan

Link control protocol – LCP



- `code`: indique le type de message LCP
- `identificateur`: association requêtes/réponses
- `longueur`: taille totale du message avec l'entête LCP
  - permet de supprimer de potentiels octets de bourrage
- `données`: paramètres de la négociation

Types de messages LCP

Code	Nom	Description
1	`Configure-Request`	modif. aux valeurs par défaut
2	`Configure-Ack`	récepteur accepte toutes les modif.
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 de test de l'état de la liaison
10	`Echo-Reply`	réponse de test de l'état de la liaison
11	`Discard-Request`	supprimés en silence par le récepteur

LCP : données

Style TLV :

1 octet	1 octet	Longueur – 2 octets
Type	**Longueur**	**Valeur**

Type	Nom	Description
1	MRU	Taille maximale des trames reçues
2	ACCM	table des caractères à transcoder
3	authentification	protocole d'authentification choisi
4	qualité	protocole de surveillance de la qualité
5	*Magic Number*	négociation de cette valeur
7	compression `protocol`	champ `protocol` sur 1 octet
8	compression `address` et `control`	suppression de ces champs
...		

`http://www.iana.org/assignments/ppp-numbers/ppp-numbers.xhtml`

Exercice !

```
ff 03 c0 21 01 01 00 14 02 06 00 00 00
00 05 06 64 e5 39 d8 07 02 08 02 7f 41
```

Exercice !

```
ff 03 c0 21 01 01 00 14 02 06 00 00 00
00 05 06 64 e5 39 d8 07 02 08 02 7f 41
```

protocole=C021 →LCP

Exercice !

```
ff 03 c0 21 01 01 00 14 02 06 00 00 00
00 05 06 64 e5 39 d8 07 02 08 02 7f 41
```

protocole=C021 →LCP
Conf-Request id=1 len=0x0014 (20)

Sondage : combien d'options dans ce message ?

a) 2
b) 3
c) 4
d) 5

Exercice !

```
ff 03 c0 21 01 01 00 14 02 06 00 00 00
00 05 06 64 e5 39 d8 07 02 08 02 7f 41
```

protocole=C021 →LCP
Conf-Request id=1 len=0x0014 (20)
ACCM (val = 00 00 00 00)

Exercice !

```
ff 03 c0 21 01 01 00 14 02 06 00 00 00
00 05 06 64 e5 39 d8 07 02 08 02 7f 41
```

protocole=C021 →LCP
Conf-Request id=1 len=0x0014 (20)
ACCM (val = 00 00 00 00)
magic number (val = 64 e5 39 d8)

Exercice !

```
ff 03 c0 21 01 01 00 14 02 06 00 00 00
00 05 06 64 e5 39 d8 07 02 08 02 7f 41
```

protocole=C021 →LCP
Conf-Request id=1 len=0x0014 (20)
ACCM (val = 00 00 00 00)
magic number (val = 64 e5 39 d8)
protocol field compression

Exercice !

```
ff 03 c0 21 01 01 00 14 02 06 00 00 00
00 05 06 64 e5 39 d8 07 02 08 02 7f 41
```

protocole=C021 →LCP
Conf-Request id=1 len=0x0014 (20)
ACCM (val = 00 00 00 00)
magic number (val = 64 e5 39 d8)
protocol field compression
addr/ctrl field compression

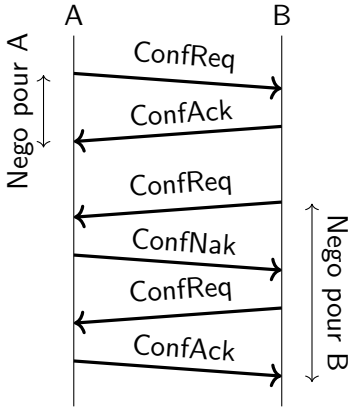
Exercice !

```
ff 03 c0 21 01 01 00 14 02 06 00 00 00
00 05 06 64 e5 39 d8 07 02 08 02 7f 41
```

protocole=C021 →LCP
Conf-Request id=1 len=0x0014 (20)
ACCM (val = 00 00 00 00)
magic number (val = 64 e5 39 d8)
protocol field compression
addr/ctrl field compression

Négociation LCP

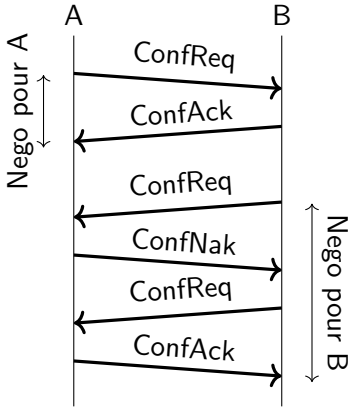
- paramètres unidirectionnels
- tous ont des valeurs par défaut
- négociation des valeurs en réception



- REQ : propose modifs aux valeurs par défaut

Négociation LCP

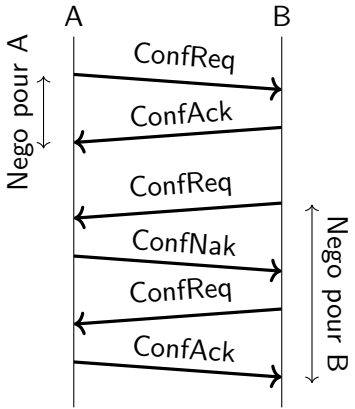
- paramètres unidirectionnels
- tous ont des valeurs par défaut
- négociation des valeurs en réception



- REQ : propose modifs aux valeurs par défaut
- ACK : accepte la proposition

Négociation LCP

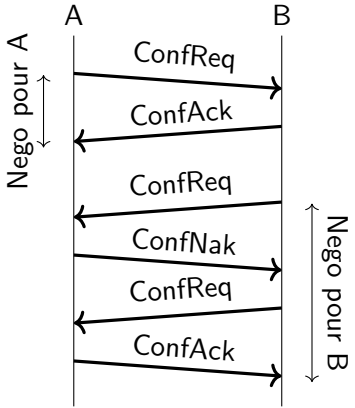
- paramètres unidirectionnels
- tous ont des valeurs par défaut
- négociation des valeurs en réception



- REQ : propose modifs aux valeurs par défaut
- ACK : accepte la proposition
- NAK : renvoie les options non acceptées avec valeurs acceptables + options voulues non demandées

Négociation LCP

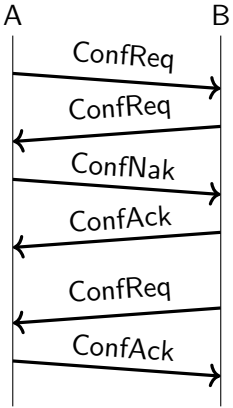
- paramètres unidirectionnels
- tous ont des valeurs par défaut
- négociation des valeurs en réception



- REQ : propose modifs aux valeurs par défaut
- ACK : accepte la proposition
- NAK : renvoie les options non acceptées avec valeurs acceptables + options voulues non demandées
- REJ : options non reconnues ou non négociables

Négociation LCP

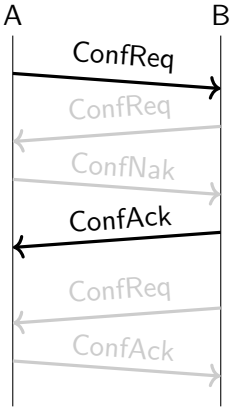
- paramètres unidirectionnels
- tous ont des valeurs par défaut
- négociation des valeurs en réception



en général, négociations entremêlées

Négociation LCP

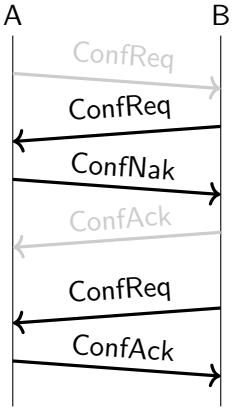
- paramètres unidirectionnels
- tous ont des valeurs par défaut
- négociation des valeurs en réception



en général, négociations entremêlées

Négociation LCP

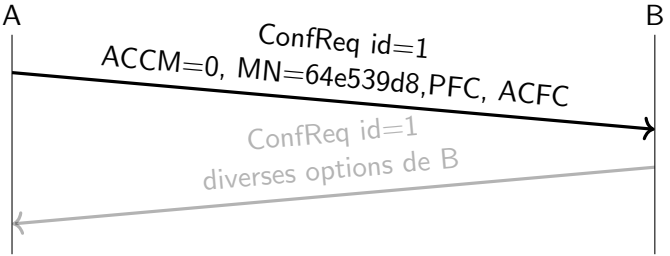
- paramètres unidirectionnels
- tous ont des valeurs par défaut
- négociation des valeurs en réception



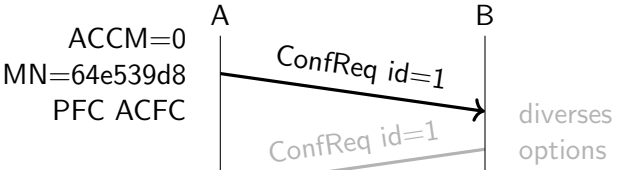
en général, négociations entremêlées

Faites des diagrammes complets !

Indiquez sur vos diagrammes les infos nécessaires à la compréhension de la négociation.
Dans le cas de l'exercice précédent :



ou bien :



Plan

PAP

Password Authentification Protocol (RFC 1334)

- transmission en clair de **l'identifiant** et du **mot de passe**
- 3 types de msgs de négociation (`Authenticate-Request`, `Authenticate-Ack`, `Authenticate-Nak`).
- format identique à LCP, valeur du champ code :
  - 1: **demande d'authentification**

    format :

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

  - 2: **acquittement positif**

    format :

1 o.	LgId octets
LgMsg	**Message_pour_le_client**

  - 3: **acquittement négatif** (échec)

    format :

1 o.	LgId octets
LgMsg	**Message_pour_le_client**

CHAP

Challenge Handshake Auth. Protocol (RFC 1994)

- les 2 extrémités possèdent un **secret** partagé
- 4 types de messages de négociation (`Challenge`, `Response`, `Success` ou `Failure`)
- format identique à LCP, valeur du champ `code` :
  - 1: **défi** (envoi d'une séquence binaire)

format:

1 o.	Lg octets	
Lg	**séquence_binaire**	nom de l'émetteur

  - 2: **réponse** (hash crypto de `id+secret+séquence`)

format:

1 o.	Lg octets	
Lg	**hash calculé**	nom de l'émetteur

  - 3: **succès** : les hashs reçu et calculé localement sont identiques
  - 4: **échec**

Plan

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 de couche réseau :
  - IPCP pour la configuration IPv4 (RFC 1332)
  - IPv6CP pour la configuration IPv6 (RFC ~~2472~~ 5072)
  - ATCP pour la configuration AppleTalk (RFC 1378)
  - IPXCP pour la configuration IPX (RFC 1552)
  - ...

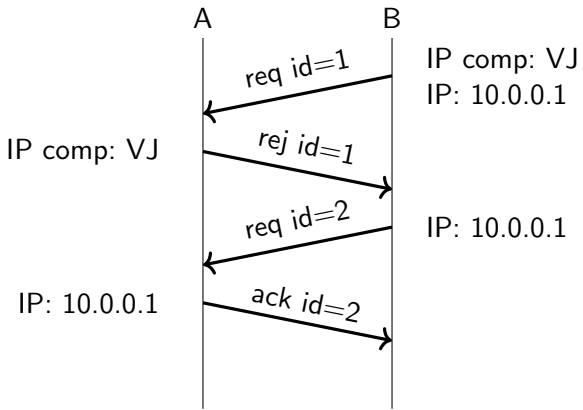
IPCP

Internet Protocol Control Protocol

- 4 types de paquets de négociation (`Configure-Request`, `Configure-Ack`, `Configure-Nak` ou `Configure-Reject`)
- format identique à LCP, options [1] :
  - 2 : **compression d'entête**
    - le type de compression (**Van Jacobson**; **étendu**; **ROHC**, *RObust Header Compression*)
    - nombre max de connexions compressées
  - 3 : **adresse IP** sur 4 octets
  - 129 : adresse IP du **serveur DNS primaire**
  - 131: adresse IP du **serveur DNS secondaire**
  - ...

1. `http://www.iana.org/assignments/ppp-numbers/ppp-numbers.xhtml`

Un exemple de demi-négociation IPCP



Plan

AAA : authentication, authorization, accounting

- authentification : vérifier une identité
- autorisation : déterminer si une entité peut accéder à une ressource/service
- comptabilité : collecte des infos d'utilisation de la ressource (facturation, audit, *capacity planning*)

RADIUS

Remote Authentication Dial In User Service [RFC2865]

protocole entre :

- NAS (*network access server* = point d'accès = extrémité PPP)
- serveur AAA

Centralise les fonctions d'AAA

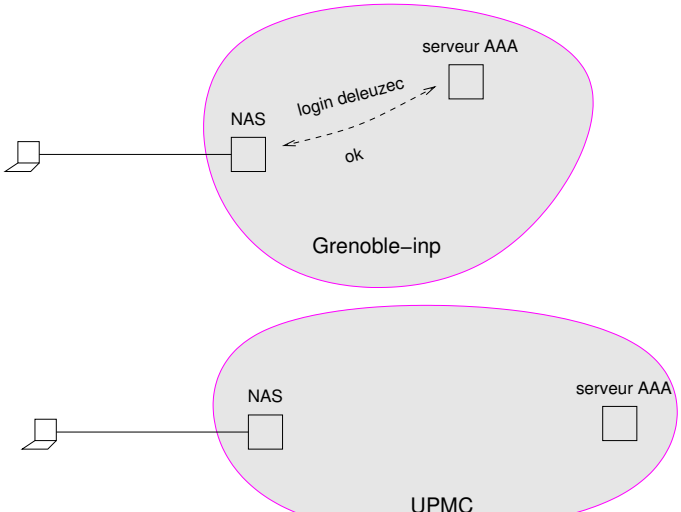
Messages RADIUS

protocole de couche application, au dessus d'UDP (port 1812)
fiabilité par retransmissions au niveau application

- message Access-Request du client d'accès - nom de l'utilisateur, mot de passe chiffré - 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 - l'utilisateur n'est pas dans la base ou n'a pas accès au service
- quelques autres...

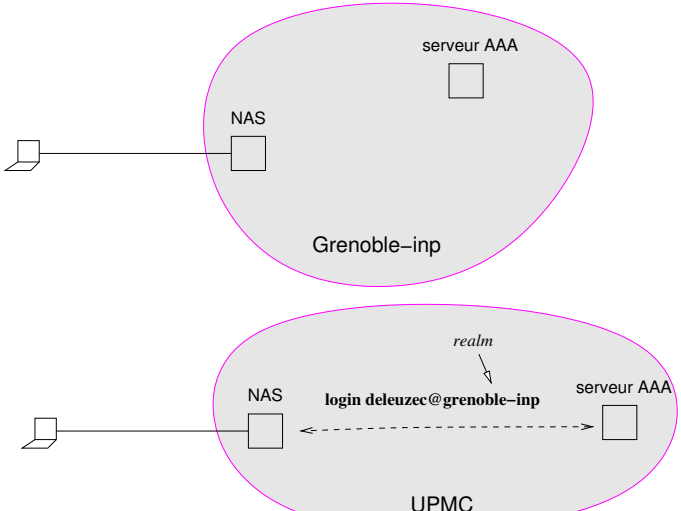
RADIUS : roaming

j'ai un compte à l'INP, je me connecte depuis le réseau de l'INP



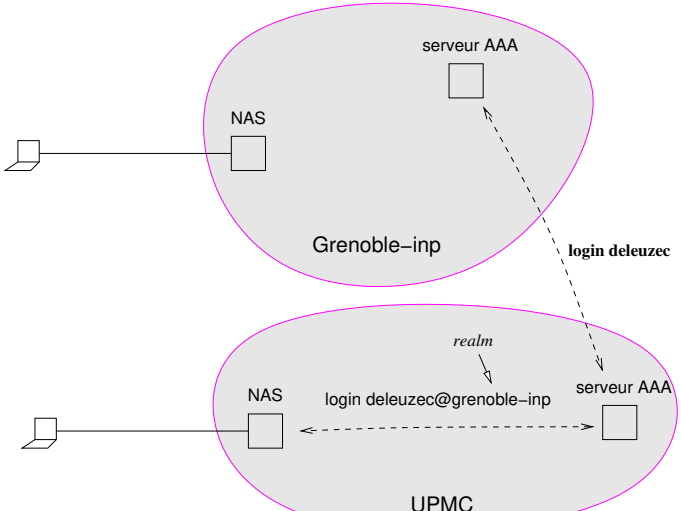
RADIUS : roaming

j'ai un compte à l'INP, je me connecte depuis le réseau de l'UPMC



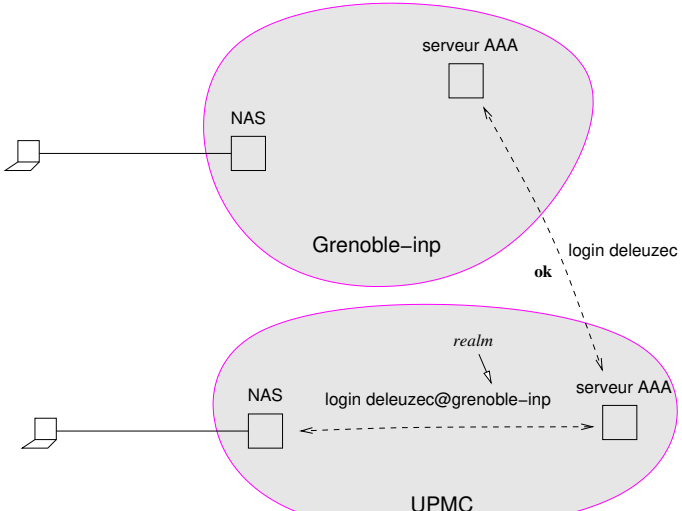
RADIUS : roaming

j'ai un compte à l'INP, je me connecte depuis le réseau de l'UPMC



RADIUS : roaming

j'ai un compte à l'INP, je me connecte depuis le réseau de l'UPMC



RADIUS : roaming

j'ai un compte à l'INP, je me connecte depuis le réseau de l'UPMC