Les protocoles de liaisons point à point

Les protocoles de liaison point à point

- Niveau 2
- paquets IP: ne peuvent être émis directement sur une liaison série
- Délimitation des données: rôle de base des protocoles de liaison
- Plusieurs protocoles définis:
  - BSC (IBM): Binary Synchronous Communication
  - SDLC (IBM): Synchronous Data Link Control
  - LAPB (UIT-T): Link Access Procedure Balanced
  - HDLC (ISO): High level Data Link Control
  - SLIP (IETF): Serial Line Internet Protocol
  - PPP (IETF): Point to Point Protocol
  - PPTP (Microsoft)) Point to Point Tunneling Protocol
  - PPPoE (IETF) PPP over Ethernet
  - PPPoA (IETF) PPP over Atm
  - L2F (CISCO) Layer 2 Forwarding
  - L2TP (IETF) Layer 2 Tunneling Protocol

HDLC

- High level Data Link Control
- Dérivé de SDLC d'IBM
- Normalisé en 1976 par l'ISO
- Synchrone orienté bit
- Mode connecté
- Gestion des erreurs: Détection et correction
- Gestion du contrôle de flux
- Gestion de la fenêtre d'anticipation
- Mono-protocole
- Différentes versions:
    - LAP: Link Access Protocol, fonctionnement sur sollicitation du primaire
    - LAP-B: (B pour Balanced, mode équilibré, primaire – primaire)
    - LAP-D: (D pour canal D, similaire à LAP-B est utilisé dans NUMERIS (RNIS))
    - SDLC est présenté comme un sous-ensemble d'HDLC car moins riche; HDLC est une évolution de SDLC qui ne fonctionne qu'en mode non équilibré

HDLC

- Structure de la trame de données:

Fanion 8 bits 01111110	Adresse 8 bits	Commande 8 bits ou 16 bits	Informations variable	FCS 16 bits	Fanion 8 bits 01111110

- Fanion ou flag:
  - Sur 8 bits
  - Codage: 01111110 , le même pour fanion de début et fin de trame
  - pour délimiter la trame
  - Le fanion de fin de trame peut faire office de fanion de début de trame suivante
  - Pour maintenir la synchronisation entre les trames en cas d'absence de données
  - La transparence est réalisée selon la technique du bit de bourrage (bit stuffing): insertion d'un zéro après 5 bits successifs à 1

HDLC

- Adresse:
  - Contrairement à la structure classique « adresse source/ adresse destination », la trame hdlc ne comporte qu'un seul champ d'adresse
  - Utilisé à l'origine dans une relation maître/esclave, un seul champ adresse était nécessaire, il désignait le terminal auquel on transmettait les données ou le terminal qui transmettait les données
  - Codage:
    - En modulo 8: 00000001 requête
      00000011 réponse

      champ « commande « sur 8 bits
    - En modulo 128 00001000 requête
      00001100 réponse

      champ « commande « sur 16 bits

HDLC

- Commande:
  - Sur 8 bits en modulo 8

Format du cham« commande »	1	2	3	4	5	6	7	8
Trame I: Information	0	N (S)			P/F	N (R)		
Trame S: Supervision	1	0	S	S	P/F	N (R)		
Trame U: Unnumbered	1	1	M	M	P/F	M	M	M

  - N(S) et N(R) sont codés sur 3 bits
  - Les trames sont numérotés de 0 à 7
  - La fenêtre d'anticipation est comprise entre 1 et 8

HDLC

- Commande:
  - Sur 16 bits en modulo 128
  - Mode étendu
  - Dans les réseaux locaux (taux d'erreurs faible) et dans les liaisons satellites (temps de transit important)

Bits →	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Trame I	0	N (S)							P/F	N (R)						
Trame S	1	0	Non utilisé				S	S	P/F	N (R)						
Trame U	1	1	MM	P/F	MMM											

  - N(S) et N(R) sont codés sur 7 bits
  - Les trames sont numérotées de 0 à 127
  - La fenêtre d'anticipation est comprise entre 1 et 128

HDLC

- HDLC distingue 3 types de trames:
  - Les trame d'information dites trames I
  - Les trames de supervision dites trames S
  - Les trames non numérotées dites trames U

- Les trames I : servent à transporter les données provenant de la couche supérieure
  - identifiées par le premier bit du champ commande à 0,
  - transportent les données.
- N(S) : numéro de séquence de la trame envoyée (S: Send)
  - Compteur de séquence Incrémenté de 1 à chaque trame de donnée envoyée
- N(R) : numéro de séquence de la trame reçue (R: Receive)
  - Compteur de séquence incrémenté de 1 à chaque trame de données recue
- P/F: Poll/Final
  - P/F = 0 trame intermédiaire, ce n'est pas la fin de la fenêtre
  - P/F = 1 dernière trame de la fenêtre, j'attend un acquittement

HDLC

- Les trames de supervision:
  - Pour superviser l'échange de données sur la liaison, elles transportent des commandes
  - Identifiées par les 2 premiers bits positionnés à 10 du champ « commande »
  - Les bits SS identifient le type de trame S
  - 3 trames S utilisées par HDLC: RR, REJ et RNR

Bits SS	signification
00	RR: Receive Ready, acquittement positif et prêt à recevoir (contrôle de flux: XON)
01	REJ: REJect, acquittement négatif, retransmission séquentielle de toutes les trames envoyées à partir de l'erreur (reprise sur erreur signalée)
10	RNR: Receive Not Ready, acquittement positif mais non prêt à recevoir (contrôle de flux: XOFF)
11	SREJ: Selective REJect, acquittement négatif, retransmission sélétive, uniquement de la trame indiquée par N(R) Non utilisée par HDLC

HDLC

- Les trames non numérotées dites trames U (Unnumbered):
  - Pour configurer le mode de fonctionnement de la liaison

MMMMM	
	SNRM Set Normal Response Mode mode « maître – esclave »
	SARM Set Asynchronous Response Mode mode « primaire – secondaire » , en half-duplex
11100	SABM Set Asynchronous Balanced Mode mode « primaire – primaire » , full-duplex, mode de base, modulo 8
11110	SABME Set Asynchronous Balanced Mode Extended mode « primaire – primaire », full-duplex, mode étendu, modulo 128
10001	FRMR FRaMe Reject trame invalide
00010	DISC DISConnect l'une des extrémité se déconnecte
11000	DM Disconnect Mode la station est déconnectée
00110	UA Unnumbered Acknowledge acquittement positif des trames U

HDLC

- FCS:
    - Frame Check Sequence
    - Codé sur 16 bits
    - Champ de contrôle d'erreur
    - Calculé sur la base des champs « adresse, commande, informations »
    - Selon l'algorithme du CRC16
    - Reste sur 16 bits, de la division de « adresse, commande, information » par le polynôme générateur: X16 + X12 + X5 + 1
    - Calculé à l'émission et vérifié à la réception

SLIP

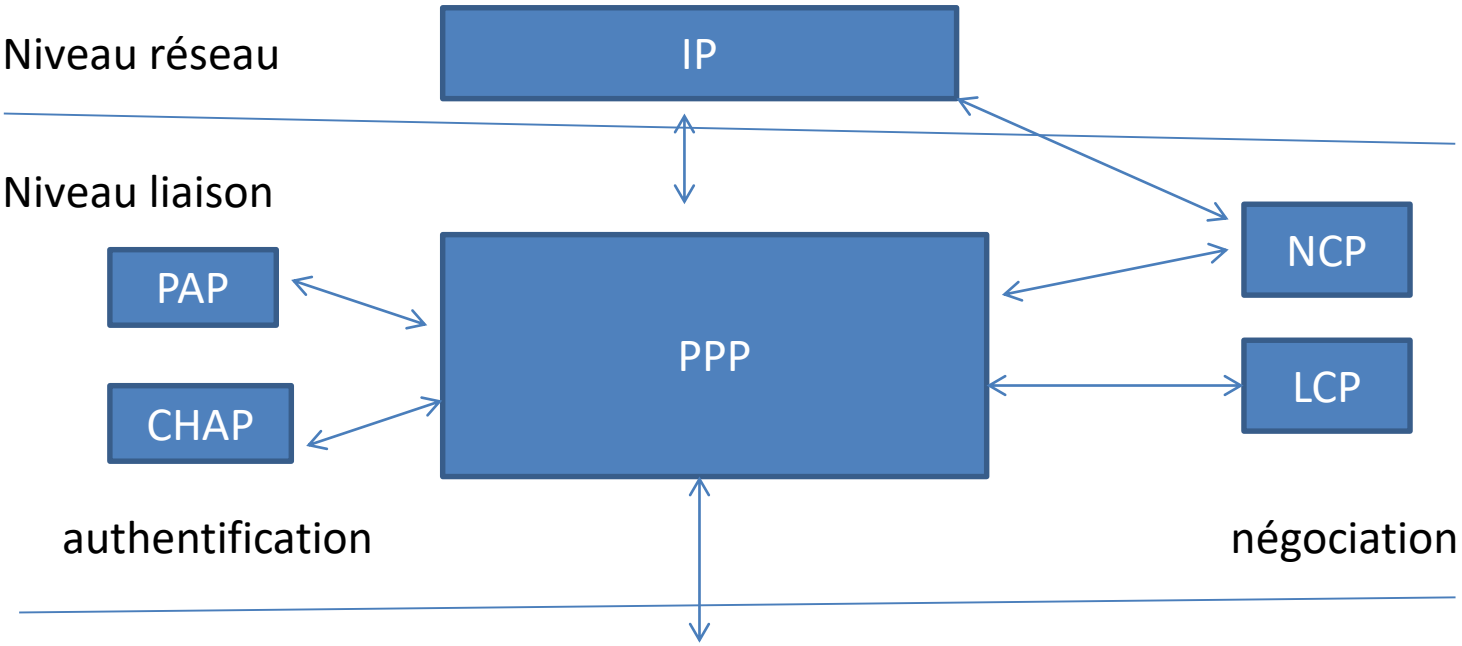
- Obsolète
- RFC 1055
- Asynchrone orienté bloc
- Simple
- Uniquement la délimitation des trames (flag de début et de fin)
- Transparence des données: caractère de transparence (ESC)
- Mono-protocole, pas de multiplexage
- Pas de mécanisme de contrôle ni de sequencement
- Connexion temporaire (dial-up)
- Chaque extrémité doit connaître l’adresse de l’autre

PPP

- RFC 1548
- Inspiré de HDLC
- Liaison d'accès au réseau Internet ou liaison entre 2 routeurs
- Sur une liaison synchrone ou asynchrone
- Par défaut, mode sans connexion, donc trames non numérotées; Possible de négocier l'utilisation de trames numérotées.
- Multi-protocole
- Détection et correction d'erreurs
- Mécanisme d'anticipation
- Comporte un ensemble de protocoles:
    - PPP: ppp proprement dit pour le transport des données (trame ppp)
    - LCP: Link Control Protocol pour la négociation des paramètres de liaison
    - PAP: PPP Authentification Protocol ou
    - CHAP: Challenge Handshake Authentification Protocol
    - NCP: Network Control Protocol pour obtenir les paramètres de niveau réseau

PPP

- Niveau réseau
- Niveau liaison
- Niveau physique



- L'ensemble des protocoles de PPP

PPP

- Ensemble de sous-protocoles qui autorisent la négociation des paramètres et la sécurisation des échanges
- Composé de 3 entités:

- 1: LCP:
  - Établissement de la liaison LCP
  - Lors de l'initialisation d'un transfert, chaque extrémité de la connexion entreprend une procédure de négociation des paramètres de l'échange par l'intermédiaire du protocole LCP (MRU: Maximum Receive Unit, PAP ou CHAP,)

- 2: PAP ou CHAP:
  - L'entité appelée doit pouvoir identifier et authentifier l'appelant avant d'accepter une connexion

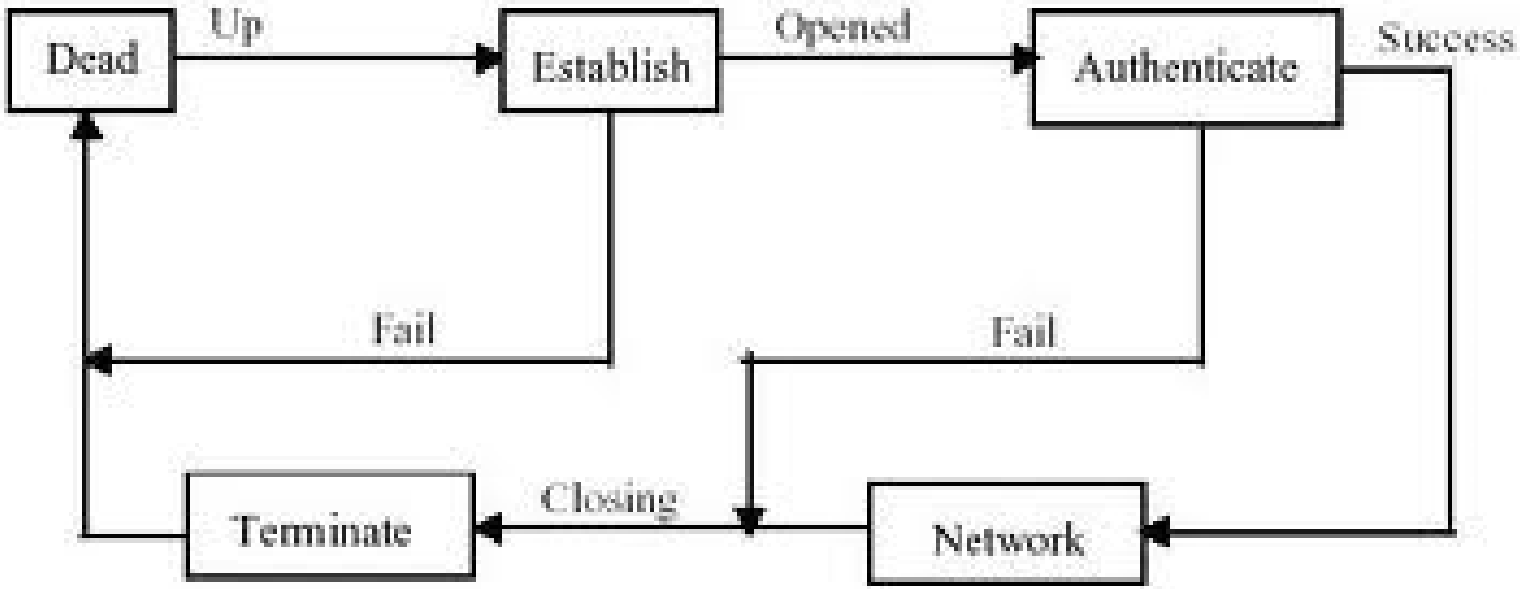
- 3: NCP:
  - Pour définir les paramètres de niveau réseau (affectation des adresses IP, compression d'entête, ..)
  - PPP pouvant être interrogé par divers protocoles de niveau 3
  - NCP est constitué d'un ensemble de protocoles spécifiques à chaque protocole de niveau 3
    - sur IP l'implémentation NCP se nome IPCP: IP control Protocol)
    - Sur IPX , c'est IPXCP: IPX Control Protocol
    - Sur AppleTalk, c'est ATCP: Apple Talk Control Protocol

PPP

- Une session PPP, de l'ouverture à la fermeture, se déroule comme suit:
- 1- Lors de la connexion, un paquet LCP est envoyé
- 2- en cas de demande d'authentification de la part du serveur, un paquet correspondant à un protocole d'authentification peut être envoyé (PAP ou CHAP ou KERBEROS)
- 3- une fois la connexion établie, PPP envoie des informations de configuration grâce au protocole NCP
- 4- les datagrammes à envoyer sont transmis sous forme de trame PPP
- 5- à la déconnexion, un paquet LCP est envoyée pour fin session

PPP

- Automate:



PPP

- Structure de la trame:

FANION 8 bits	ADRESSE 8 bits	COMMANDE 8 bits	PROTOCOLE 8 ou 16 bits	DONNEES variable	FCS 8 ou 16 bits	FANION 8 bits

- Fanion:
  - indicateur de début ou de fin de trame
  - Valeur: 01111110
- Adresse:
  - Pas d'adresse car liaison point à point
  - Valeur: 11111111
- Commande:
  - Valeur standard: 00000011 indique trame d'information non numérotée, P/F positionné à 0.
  - Possible d'utilisé un mode numéroté pour plus de fiabilité
- Protocole:
  - Indique quel protocole transmet les données
  - Longueur sur 1 octet négociée lors de la connexion
  - Multi-protocole
  - Exemples de valeurs du champ « Protocole »:
    - Ox 0021: IP Ox002D: TCP/IP Ox800F: IPV6
    - OxC021: LCP OxC023: PAP OxC223: CHAP

PPP

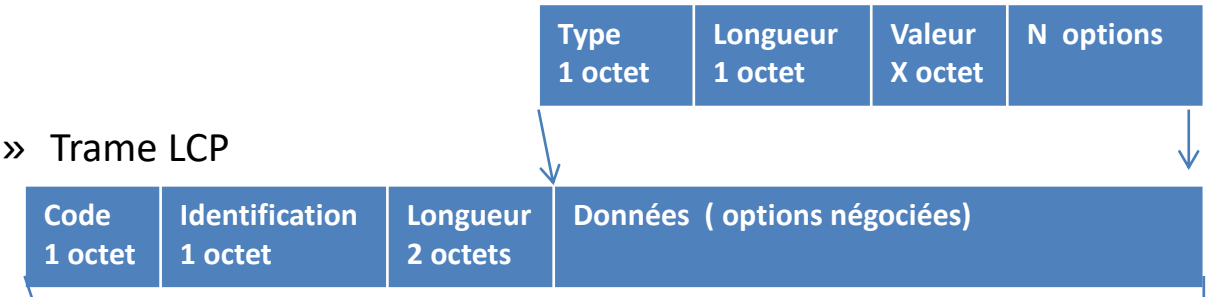
- Transparence des données utiles: (adresse, commande, info, FCS)

- Sur une liaison synchrone:
    - transparence similaire à celle de HDLC
    - Insertion d'un bit à 0 tous les 5 bits à 1, technique de bit stuffing

- Sur une liaison asynchrone:
    - Transparence similaire à celle du protocole SLIP
    - Insertion d'un caractère de transparence devant un fanion présent dans le champ « données »
    - Les caractères dont la transparence doit être assurée sont indiqués à la connexion lors de l'exécution du protocole LCP
    - Table ACCM: Asynchronous Control Character Map
    - Champ « ACCM dans option » de LCP:
        - » 0xFFFFFFFF: mode asynchrone
        - » 0x00000000: mode synchrone

PPP

- **Le protocole LCP**: Link Control Protocol
  - Lors de l'initialisation d'un transfert,
  - procédure de négociation des paramètres de l'échange par l'intermédiaire de LCP
    - Codage d'une option



» Trame LCP

- Trame PPP

PPP

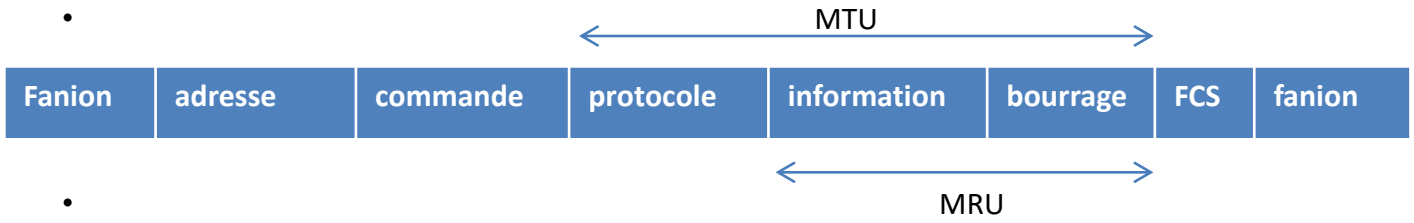
- Quelques options négociées par LCP:

Code option	Fonction	Longueur	Signification
1	MRU	4	Maximum Receipt Unit (par défaut 1500 octets)
2	ACCM	6	Asynchonous Control Character Map
3	Authentification	6	Valeur du champ « protocole » de PPP Soit 0xC023 pour PAP soit 0xC223 pour CHAP
7	compression	2	Codage du champ « Protocole » de PPP sur 1 octet
8	compression	2	Suppression des champ « adresse et commande » de la trame PPP

PPP

- MTU: (Maximum Transfert Unit) définit la capacité d'emport du niveau 2

- MRU: (Maximum Receipt Unit) charge utile vue du niveau réseau
  - Tient compte de la taille du champ « Protocole »
  - Taille maximale du segment admis en réception
  - Valeur par défaut: 1500 octets



PPP

- Code: type de trame

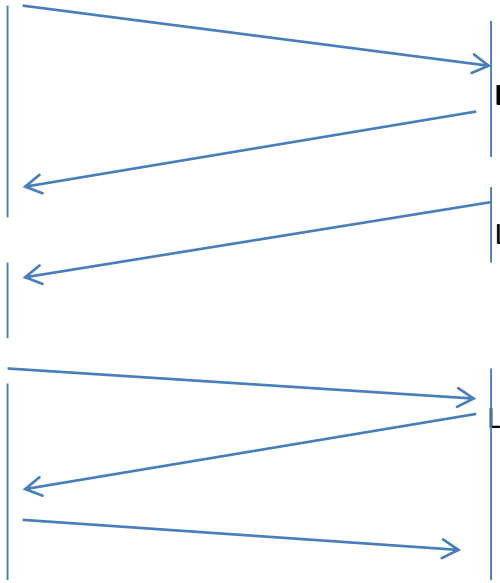
Type de trame	code	utilisation
Configure _request	1	Trame de négociation, le champ de données comprend la liste des options proposées lorsque la valeur proposée est différente de la valeur par défaut.
Configure_ack	2	Trame d'acceptation des options proposées par la trame configure_request
Configure_nack	3	Trame d'acceptation des options négociées mais pas des valeurs indiquées. L'émetteur doit proposer de nouvelles valeurs
Configure_reject	4	Trame de refus des options, le champ données indique les valeurs des options non négociable. L'émetteur reformule une requête de configuration avec les valeurs indiquées dans la trame de rejet
Terminate_request	5	Cette trame met fin à une connexion
Terminate_ack	6	Acquittement d'une fin de connexion
Code_reject	7	Trame utilisée pour indiquer à l'émetteur que le récepteur ignore une option, ceci signifie que les deux extrémités utilisent une version différente de PPP
Protocol_reject	8	Trame de gestion, indiquant que la valeur du champ protocole de la trame PPP est inconnue

- Exemple de trames LCP

PPP

- Phase d'initialisation de PPP

- **LCP Configure_request** (modification à apporter aux valeurs par défaut)



- **LCP configure _ack** (si valeurs acceptées par le récepteur)
- LCP configure_nack (si valeurs non acceptées par le récepteur
- LCP configure_request
- LCP configure_reject (les valeurs ne sont pas négociables)
- LCP configure_request

PPP

- Identification:
  - 1 octet
  - permet d’associer une requête à une réponse

- Longueur:
  - 2 octets
  - permet de distinguer les données utiles d’éventuelles données de bourrage

PPP

- La sécurisation des échanges:
    - Le protocole PPP est utilisé sur des liaison point à point permanentes, mais aussi sur des liens temporaires comme une connexion à Internet via le réseau téléphonique.
    - De ce fait, l'entité appelée doit pouvoir identifier et authentifier l'appelant avant d'accepter une connexion, c'est le rôle de PAP ou CHAP.

- Le protocole PAP: PPP Authentification Protocol
    - Protocole non fiable
    - Échange en clair l'identifiant et le mot de passe de l'appelant une seule fois en début de session
    - L'échange n'a pour objet que de valider la connexion

PPP

- Format de la trame PAP:

Code 1 octet	Identifiant trame 1 octet	Longueur totale 2 octets	Longueur ID 1 octets	Identification Longueur variable	Longueur PWD 1 octets	Password Longueur variable

- Code: 1: authentification_request
  2: authentification_ack
  3: authentification_nack

- Identifiant: permet d'associer une requête à sa réponse
- Les champs suivants contiennent l'identifiant et le mot de passe de l'extrémité qui s'authentifie. Ces champs de longueur variable sont précédés d'une information de longueur.
- En cas d'échec, l'authentification est renouvelée, après n echecs, l'établissement de la liaison est refusé.

PPP

- Le protocole CHAP: Challenge Handshake Authentification Protocol
    - Fiable
    - Mots de passe chiffrés et échangés périodiquement pour s'assurer qu'il n'y à pas eu substitution de correspondant.
    - L'algorithme de chiffrement est précisé lors de la négociation LCP
    - Protocole à 3 temps
    - Après établissement du lien, l'appelé envoie un message de test à l'appelant (challenge)
    - Ce dernier chiffre le contenu du message de test et le renvoie
    - L'expéditeur compare sa réponse avec sa propre valeur (système à clé partagée ou secrète)
    - Si le résultat coïncide, l'authentification est acceptée, dans le cas inverse la liaison est rompue.

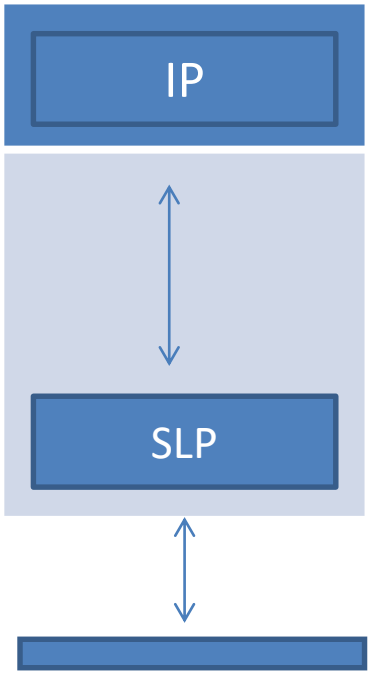
PPP

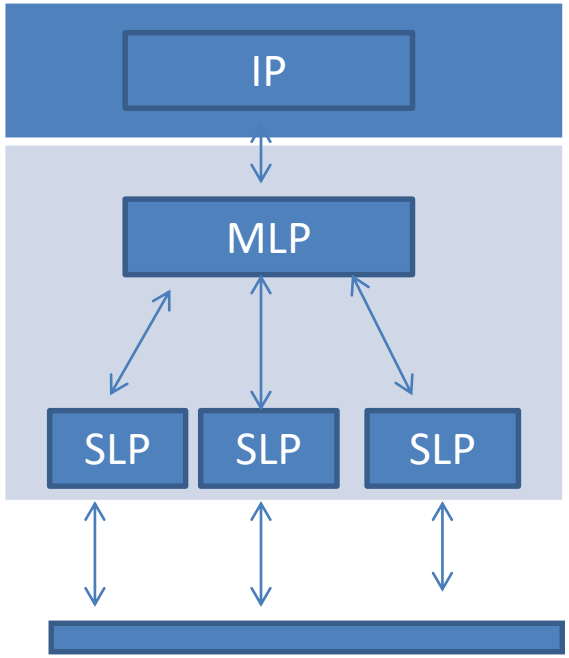
- Le protocole de compression:
    - Les en-têtes IP et TCP occupent une part non négligeable des données émises (40 octets sans les options)
    - Lors de l'envoi de petits paquets il est intéressant de procéder à une réduction de volume des en-têtes
    - Ne transmettre que la différence entre 2 en-têtes successifs (compression Van Jacobson)
- La négociation d'adresse IP de l'équipement terminal:
    - Le lien local peut informer le distant de l'adresse IP qu'il souhaite utiliser.
    - Le distant peut accepter ou refuser en fournissant alors au local une adresse IP valide.
    - Le local peut demander directement une adresse IP à l'hôte distant
    - L'entité qui demande l'attribution d'une adresse IP émet sa requête avec le champ adresse IP égal à zéro

PPP

- MLPPP: Multiple Link PPP
    - L’accès à un réseau distant peut utiliser une ligne unique (SLP: Simple Link Protocol) ou plusieurs lignes à bas débit pour obtenir une liaison haut débit.
    - Le protocole multi-ligne (MLP: Multiple Link Protocol) fragmente le datagramme IP, transmet les différents fragments sur plusieurs lignes et assure le réassemblage.
    - MLPPP peut être utilisé pour répartir la charge sur plusieurs liens, il est transparent pour le protocole de niveau réseau.

PPP





PPP

- Format de la trame MLPPP:

Fanion 8 bits 01111110	Adresse 8 bits 0xFF	Commande 8 bits 0x03	Protocole 8 bits 0x003D	BE00 4 bits Ou 8 bits	Numéro de Séquence 12 ou 24 bits	Segment IP	FCS 8 bits	Fanion 8 bits 01111110

- Protocole MLPPP: 0x003D
- BE00:
  - sur 4 ou 8 bits selon la taille du champ « numéro de séquence » gère la fragmentation.
  - Le bit B (Beginning) est positionné à 1 dans le premier fragment
  - Le bit E (Ending) est positionné à 1 dans le dernier fragment
  - Si un datagramme n'est pas fragmenté, les bits B et E sont tous les deux à 1
- Numéro de séquence: indique la position du fragment dans le datagramme