Connexions point à point

Connecting Networks

(Connexion des réseaux)

Cisco | Networking Academy®
Mind Wide Open™

Traduction de la version Anglaise originale effectuée par

Translated from the original English version done by

Jimmy Tremblay

Instructeur au/at Cégep de Chicoutimi

534 Rue Jacques-Cartier Est, Chicoutimi, Québec, Canada

Courriel/Email: jtremb@cegep-chicoutimi.qc.ca

Chapitre 3

3.1 Présentation des connexions série point à point

3.2 Fonctionnement de PPP

3.3 Configuration PPP

3.4 Dépannage de la connectivité WAN

3.5 Résumé

Chapter 3: Objectives

À l'issue de ce chapitre, vous serez en mesure d'effectuer les tâches suivantes :

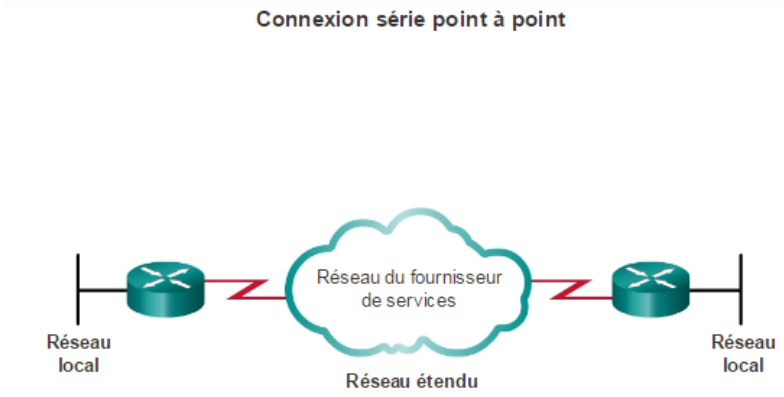
- Expliquer les bases de la communication série point à point sur un WAN.
- Configurer l'encapsulation HDLC sur une liaison série point à point.
- Décrire les avantages du protocole PPP par rapport à HDLC dans un WAN.
- Décrire l'architecture en couches PPP et les fonctions LCP et NCP.
- Expliquer comment une session PPP est établie.
- Configurer l'encapsulation PPP sur une liaison série point à point.
- Configurer les protocoles d'authentification PPP.
- Utiliser les commandes **show** et **debug** pour dépanner le protocole PPP.

3.1 Présentation des connexions série point à point

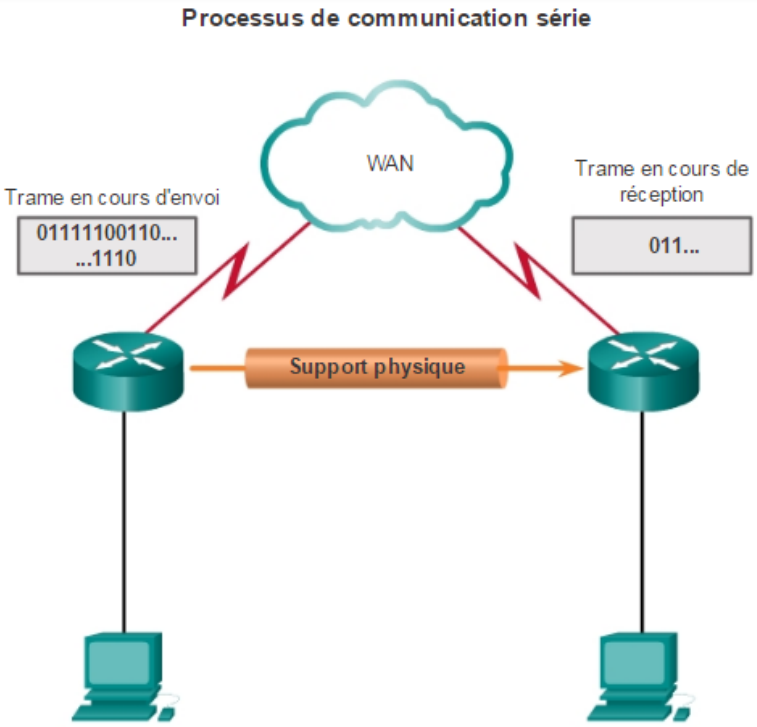
Cisco | Networking Academy®
Mind Wide Open™

Ports série et parallèle

- Les connexions point à point sont utilisées pour connecter des LAN au WAN du fournisseur de services, et pour connecter des segments de LAN dans un réseau d'entreprise.
- Aussi appelée connexion série ou ligne louée.
- La communication sur une connexion série est une méthode de transmission de données dans laquelle les bits sont transférés de façon séquentielle sur un seul canal l'un après l'autre.
- La communication parallèle est différente, car dans ce cas les bits sont transférés simultanément sur plusieurs câbles.

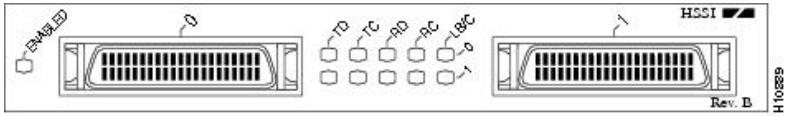


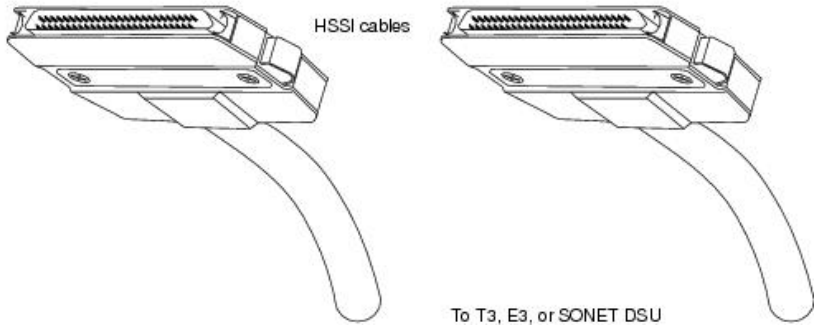
Communication série



- Des données sont encapsulées par le protocole de communications utilisé par le routeur expéditeur.
- La trame encapsulée est envoyée au WAN sur un support physique.
- Il existe plusieurs façons de traverser le WAN, mais le routeur de destination utilise le même protocole de communication pour désencapsuler la trame lorsqu'elle arrive.

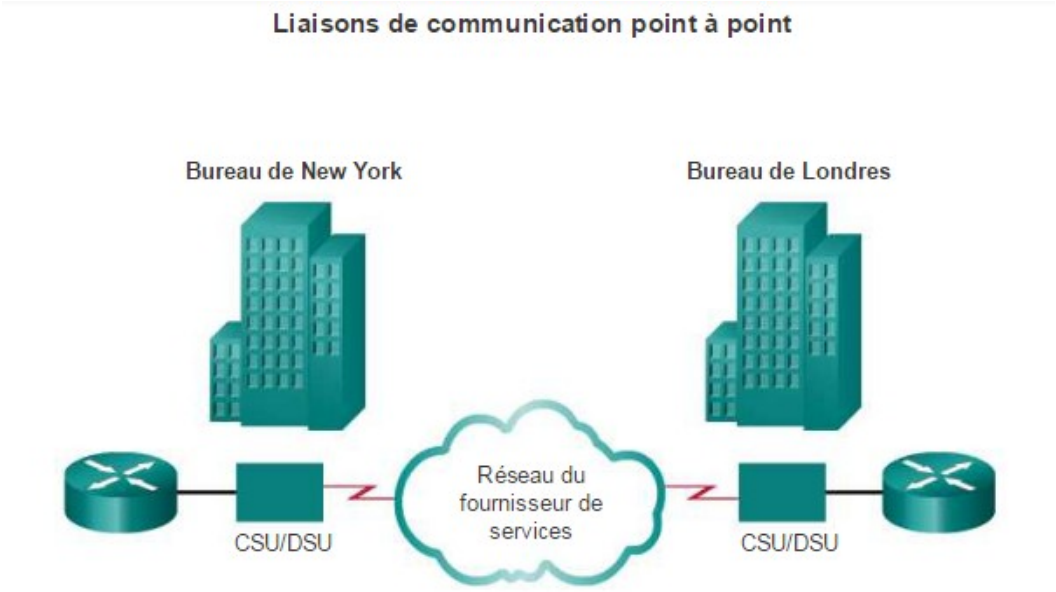
Les normes de communication série importantes affectant les connexions LAN vers WAN sont au nombre de trois : RS-232, V.35, HSSI





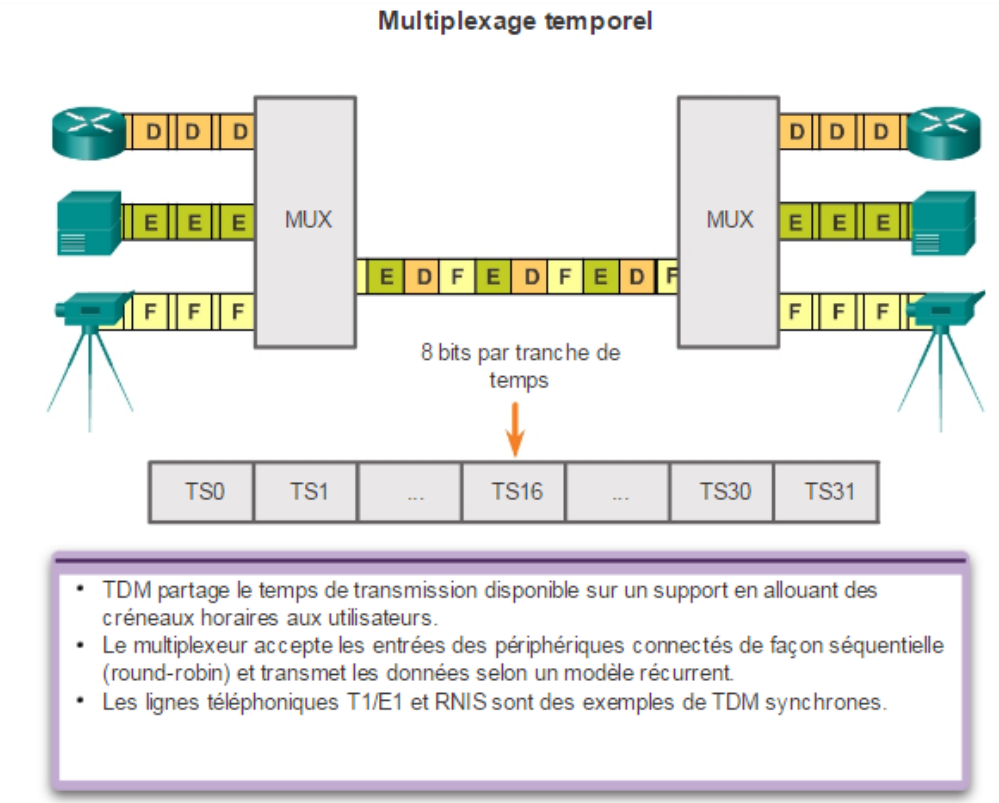
Liaisons de communication point à point

- La liaison point à point peut connecter deux sites géographiquement distants.
- L'opérateur alloue des ressources spécifiques pour une ligne louée par le client (ligne louée).
- Les liaisons point à point sont en général plus coûteuses que les services partagés.



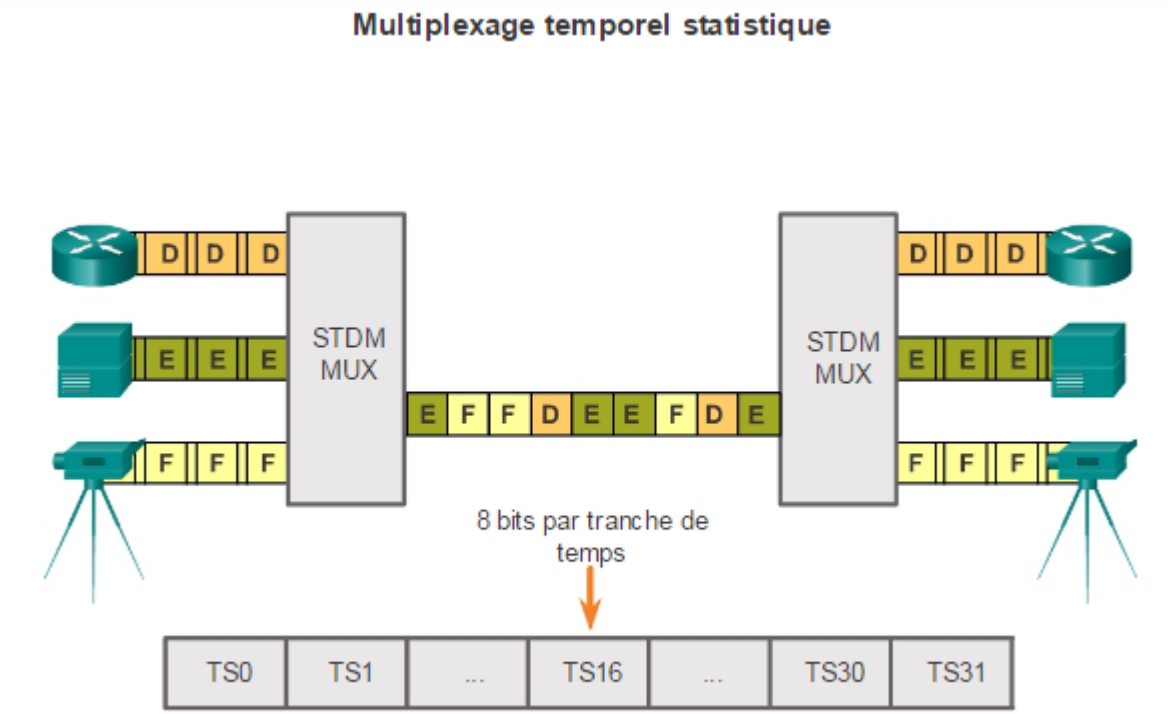
Multiplexage temporel

Le multiplexage est un système dans lequel plusieurs signaux logiques partagent un seul canal physique. TDM (Time-division multiplexing) et STDM (Statistical time-division multiplexing) sont deux types courants de multiplexage.



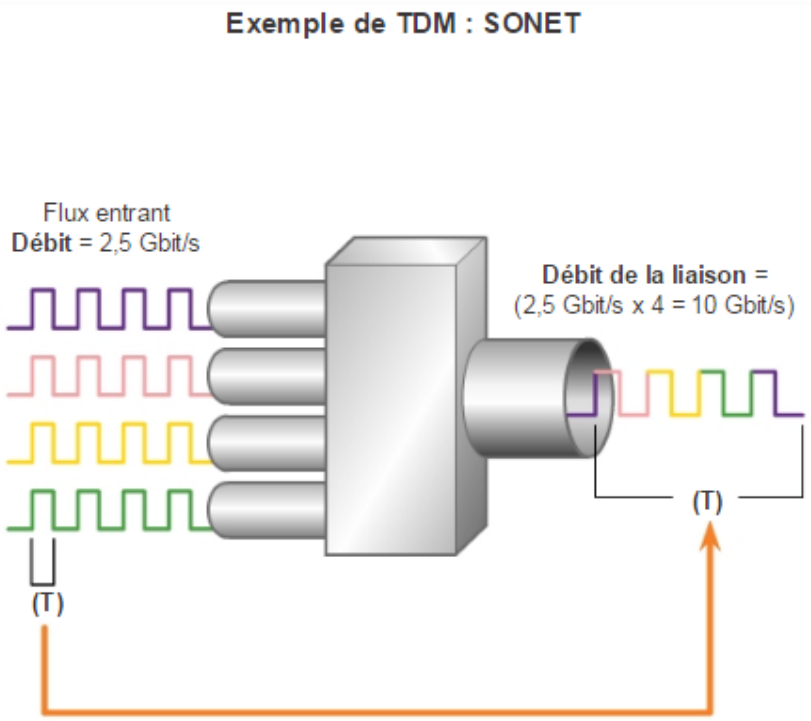
Multiplexage temporel statistique

- Il utilise une longueur de tranche de temps variable permettant à des canaux de convoiter les espaces disponibles.
- le multiplexage temporel statistique ne gaspille pas de temps de ligne à haut débit avec des canaux inactifs.



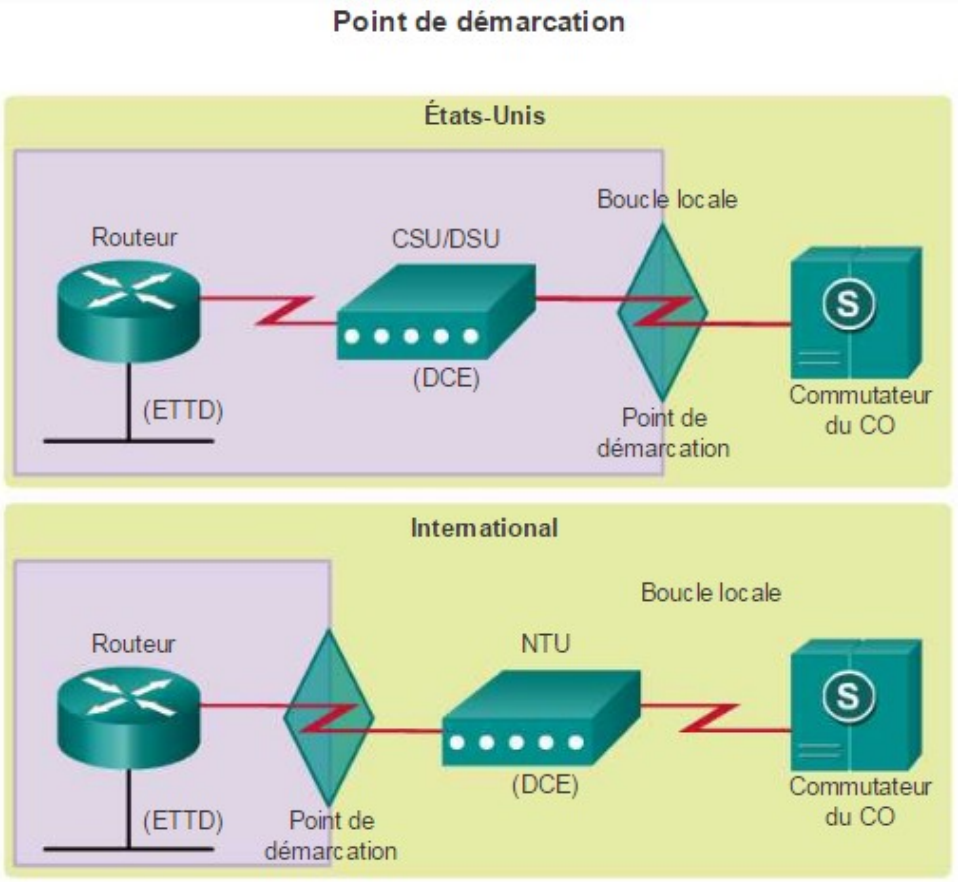
Exemples de TDM

- Le secteur des télécommunications utilise la norme SONET (Synchronous Optical Networking) ou SDH (Synchronous Digital Hierarchy) pour le transport optique de données TDM.
- Le trafic qui arrive au multiplexeur SONET de quatre flux différents à 2,5 Gbit/s repart en un seul flux à la vitesse de 4 x 2,5 Gbit/s, soit 10 Gbit/s.



Point de démarcation

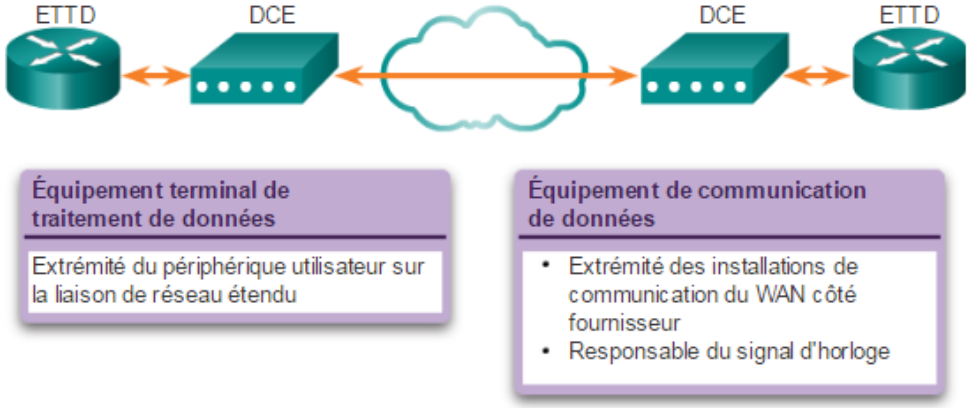
- Le point de démarcation indique l'endroit où votre réseau communique avec un réseau qui est la propriété d'une autre organisation.
- Il s'agit de l'interface entre le CPE (Customer Premises Equipment) et l'équipement du fournisseur de services réseau.
- Ce point de démarcation marque le point du réseau où s'arrête la responsabilité du fournisseur de services



ETTD-DCE

- **ETTD** – L'équipement d'abonné, généralement un routeur, constitue l'ETTD. Il peut s'agir également d'un terminal, d'un ordinateur, d'une imprimante ou d'un télécopieur s'il se connecte directement au réseau du fournisseur de services.
- **DCE** – généralement un modem ou une unité CSU/DSU, est l'équipement servant à convertir les données utilisateur de l'ETTD en une forme compatible avec la liaison de transmission du fournisseur de services de réseau étendu. Le signal est reçu par le DCE distant, qui le décode en une séquence de bits. Le DCE distant signale ensuite cette séquence à l'ETTD distant.

Connexions de réseau étendu DCE et ETTD série

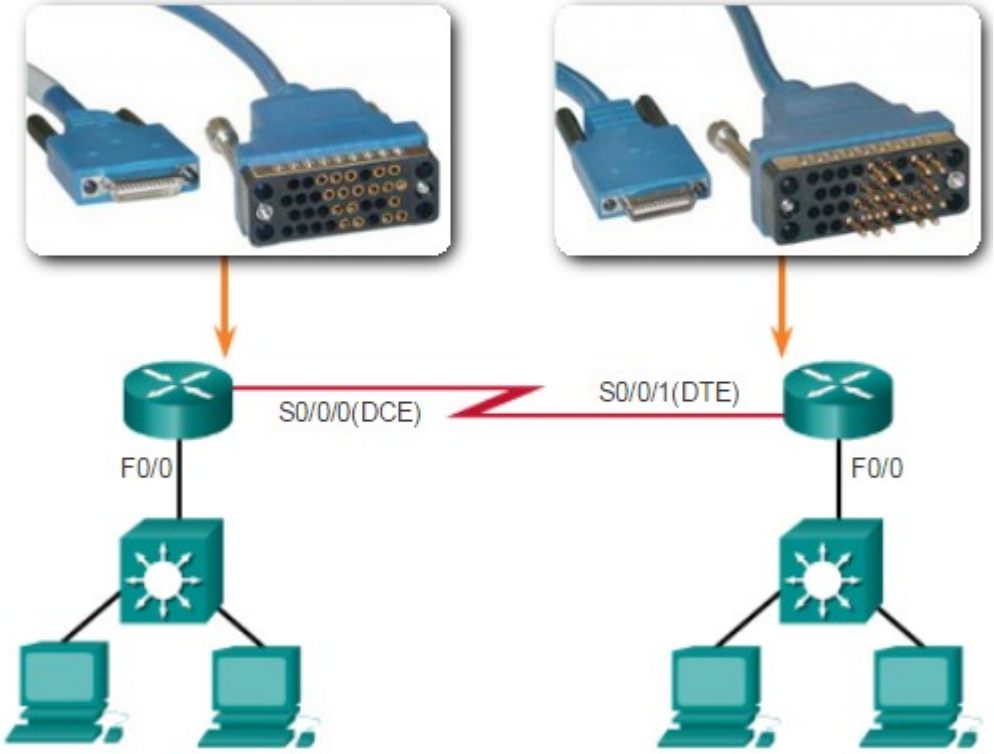


Communications série

Câbles série

Connecteur Smart Serial

Connexion de réseau étendu série dans les TP



Bande passante série

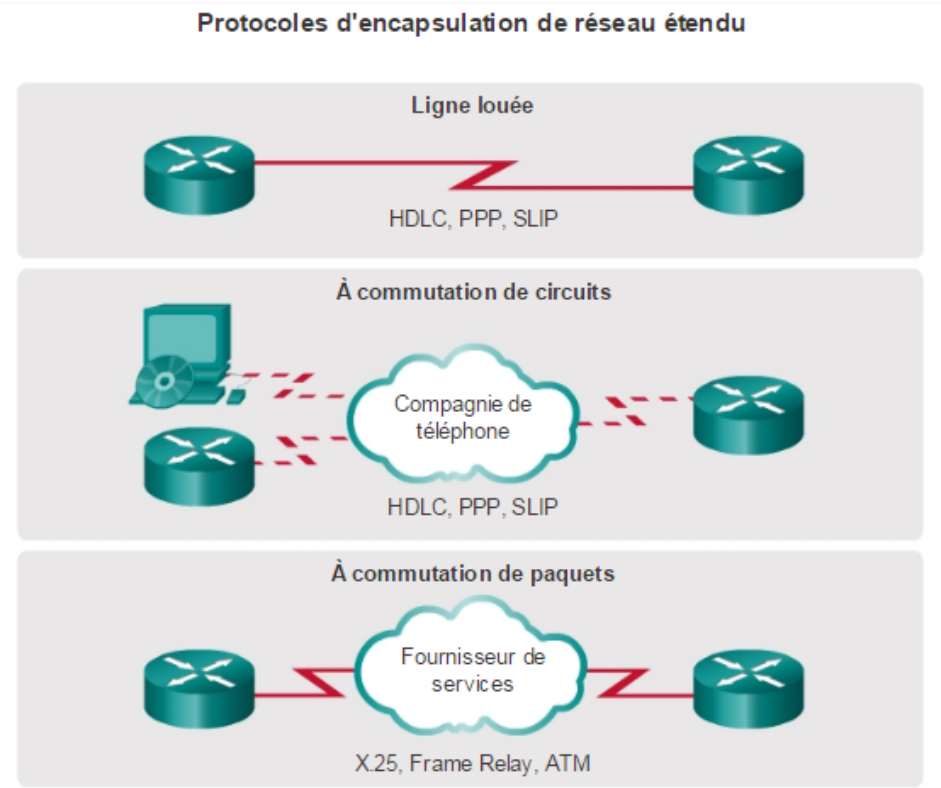
La bande passante se rapporte au débit auquel les données sont transférées sur la liaison de communication.

Débits de transmission

Type de ligne	Débit binaire
56	56 kbit/s
64	64 kbit/s
T1	1,544 Mbit/s
E1	2,048 Mbit/s
J1	1,544 Mbit/s
E3	34,368 Mbit/s
T3	44,736 Mbit/s
OC-1	51,84 Mbit/s
OC-3	155,52 Mbit/s
OC-9	466,56 Mbit/s
OC-12	622,08 Mbit/s
OC-18	933,12 Mbit/s
OC-24	1,244 Gbit/s
OC-36	1,866 Gbit/s
OC-48	2,488 Gbit/s
OC-96	4,976 Gbit/s
OC-192	9,954 Gbit/s
OC-768	39,813 Gbit/s

Protocoles d'encapsulation de réseau étendu

Sur chaque connexion WAN, les données sont encapsulées dans des trames avant de franchir la liaison WAN. Le type d'encapsulation de couche 2 approprié doit être correctement configuré afin que le bon protocole soit appliqué.

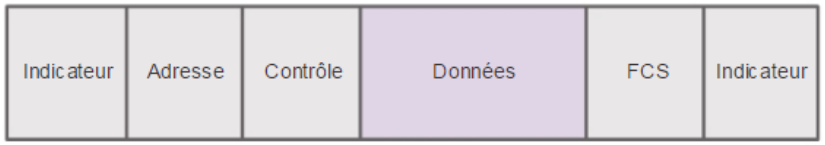


Encapsulation HDLC

- Le protocole HDLC offre à la fois un service orienté connexion et sans connexions.
- HDLC est un protocole de couche liaison de données synchrone développé par l'Organisation internationale de normalisation (ISO).
- Utilise la transmission série synchrone pour assurer une communication dépourvue d'erreurs entre deux points.
- Définit une structure de tramage de couche 2 permettant un contrôle de flux et des erreurs, au moyen de reçus.
- Cisco a développé une extension du protocole HDLC afin de remédier au problème posé par l'incapacité de ce protocole à prendre en charge plusieurs protocoles.(Cisco HLDC également appelé cHDLC).

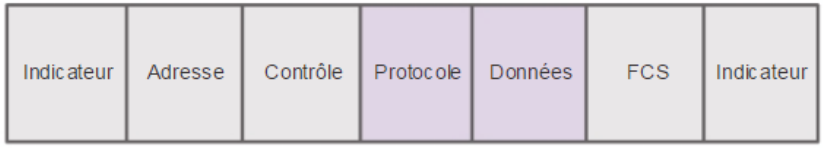
Format de trame Cisco HLDC et standard

HDLC standard



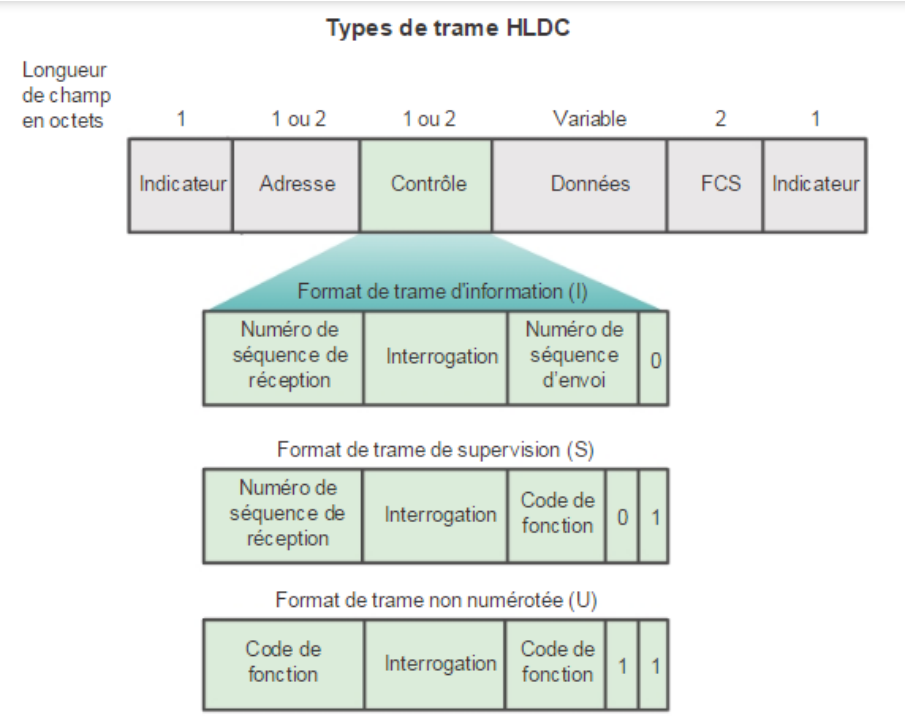
Prend en charge uniquement les environnements de protocole unique.

Cisco HDLC



Utilise un champ de données de protocole pour prendre en charge des environnements multiprotocoles.

Types de trame HLDC



- Le champ d'indicateur déclenche la vérification des erreurs et y met fin. La trame commence toujours par un champ d'indicateur à 8 bits et se termine toujours par ce même indicateur. La séquence de bits est 01111110.

- **Trame d'information (I)** : les trames I transportent les informations de couche supérieure, ainsi que certaines informations de contrôle. Cette trame envoie et reçoit les numéros d'ordre, et le bit d'interrogation final (P/F) est chargé du contrôle de flux et d'erreur.
  - **Trame de supervision (S)** : les trames S fournissent les informations de contrôle. Une trame S peut demander et suspendre la transmission, signaler un état et accuser réception de trames d'information.
    - **Trame non numérotée (U)** : les trames U servent au contrôle, et ne suivent pas de séquence spécifique.

Configuration de l'encapsulation HDLC

- Cisco HDLC est la méthode d'encapsulation par défaut utilisée par les périphériques Cisco sur les liaisons série synchrones.
- Utilisez Cisco HDLC comme protocole point à point sur les lignes louées entre deux périphériques Cisco.
- Si vous connectez des périphériques non-Cisco, utilisez le protocole PPP synchrone.

```
Router(config)# interface s0/0/0
Router(config-if)# encapsulation hdlc
```

- Activer l'encapsulation HDLC
- HDLC est l'encapsulation par défaut sur les interfaces série synchrones

Encapsulation HDLC

Dépannage d'une interface série

```
R1# show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:05, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total
  output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max
total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 1017 bytes, 0 no buffer
     Received 5 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors  0 CRC  0 frame  0 overrun  0 ignored
```

```
R1# show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DCE V.35, clock rate 64000
idb at 0x66855120, driver data structure at 0x6685C93C
wic_info 0x6685CF68
Physical Port 0, SCC Num 0
MPSC Registers:
MMCR_L=0x000304C0, MMCR_H=0x00000000, MPCR=0x00000000
CHR1=0x00FE007E, CHR2=0x00000000, CHR3=0x0000064A,
CHR4=0x00000000
CHR5=0x00000000, CHR6=0x00000000, CHR7=0x00000000,
CHR8=0x00000000
CHR9=0x00000000, CHR10=0x00003008
SDMA Registers:
SDC=0x00002201, SDCM=0x00000080, SGC=0x0000C000
CRDP=0x0DBD2DB0, CTDP=0x0DBD31D0, FTDB=0x0DBD31D0
Main Routing Register=0x0003FE38 BRG Conf
Register=0x0005023F
Rx Clk Routing Register=0x76543818 Tx Clk Routing
Register=0x76543910
GPP Registers:
Conf=0x430002  , Io=0x46C050  , Data=0x7F4BBFAD,
Level=0x80004
Conf0=0x430002  , Io0=0x46C050  , Data0=0x7F4BBFAD,
Level0=0x80004
0 input aborts on receiving flag sequence
```

Dépannage d'une interface série (suite)

Dépannage d'une interface série

Ligne d'état	Condition possible	Problème / Solution
Serial x is up, line protocol is up	Il s'agit de la condition de ligne d'état correcte.	Aucune action n'est requise.
Serial x is down, line protocol is down (DTE mode)	Le routeur ne détecte pas de signal de détection de porteuse (CD), ce qui veut dire que la détection de porteuse n'est pas active. Un problème de fournisseur de services de réseau étendu s'est produit, ce qui veut dire que la ligne est désactivée ou n'est pas connectée au CSU/DSU. Le câblage est défectueux ou incorrect. Un échec matériel s'est produit (CSU/DSU).	1. Contrôlez les voyants sur le CSU/DSU pour voir si la CD est active ou bien insérez une boîte de dérivation sur la ligne pour vérifier le signal CD. 2. Vérifiez que le bon câble et la bonne interface sont utilisés à l'aide de la documentation d'installation du matériel. 3. Insérez une boîte de dérivation et vérifiez toutes les lignes de commande.
		4. Contactez le service de ligne louée ou bien l'opérateur pour vérifier s'il y a un problème. 5. Intervertissez les pièces qui posent problème. 6. Si un routeur défectueux est suspecté, branchez la ligne série sur un autre port. Si la connexion s'établit, l'interface précédemment connectée présente un problème.

Dépannage d'une interface série (suite)

Dépannage d'une interface série

Ligne d'état	Condition possible	Problème / Solution
Serial x is up, line protocol is down (DTE mode)	Un routeur local ou distant n'est pas correctement configuré. Les informations de maintien de connexion ne sont pas envoyées par le routeur distant. Un problème de ligne louée ou de service d'opérateur s'est produit, par exemple du bruit sur la ligne ou bien un commutateur mal configuré ou arrêté.	1. Placez le modem, le CSU ou le DSU en mode de bouclage local et utilisez la commande `show interfaces serial` pour déterminer si le protocole de ligne apparaît. Si oui, le problème vient probablement d'un problème du côté du fournisseur de service WAN ou bien de l'échec d'un routeur distant.
	Le matériel du routeur, local ou distant, a échoué.	4. Activez la commande d'exécution de débogage `serial interface`. 5. Si le protocole de ligne ne s'affiche pas en mode de bouclage local, et si le résultat de la commande d'exécution `debug serial interface` indique que le compteur de maintien de la connexion n'augmente pas, le problème vient probablement du matériel côté routeur. Changez le matériel d'interface du routeur.
		6. Si le protocole de ligne s'affiche et que le compteur de maintien de la connexion augmente, le problème n'est pas au niveau du routeur local. 7. Si un routeur défectueux est suspecté, branchez la ligne série sur un port non utilisé. Si la connexion s'établit, l'interface précédemment connectée présente un problème.
	Un problème de temporisation s'est produit, ce qui signifie que la SCTE (serial clock transmit external) n'est pas définie sur CSU/DSU. La SCTE est conçue pour compenser le décalage de phase dans les longs câbles. Lorsque le périphérique DCE utilise la SCTE au lieu de son horloge interne pour échantillonner des données du DTE, il peut échantillonner ces données sans erreur, même si le câble présente un décalage de phase. Un CSU/DSU local ou distant a échoué.	2. Si le problème semble provenir de l'extrémité distante, répétez l'étape 1 sur le modem distant, l'unité CSU ou l'unité DSU. 3. Vérifiez tout le câblage. Assurez-vous que le câble est connecté à l'interface appropriée, à l'unité CSU/DSU appropriée et au point de terminaison approprié sur le réseau du fournisseur de services de réseau étendu. Utilisez la commande d'exécution `show controllers` pour savoir quel câble est connecté à quelle interface.

Encapsulation HDLC

Dépannage d'une interface série (suite)

Dépannage d'une interface série

Ligne d'état	Condition possible	Problème / Solution
		problème.
Serial x is up, line protocol is down (DCE mode)	La commande de configuration d'interface `clockrate` est manquante. Le périphérique DTE ne prend pas en charge le mode SCTE ou n'est pas configuré pour. Le CSU ou le DSU distant a échoué.	1. Ajoutez la commande de configuration d'interface `clockrate` sur l'interface série. Syntaxe : `clockrate` *`bps`* Description de la syntaxe : *`bps`* - Fréquence d'horloge souhaitée en bits par seconde : 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000 ou 8000000
		2. Si le problème semble provenir de l'extrémité distante, répétez l'étape 1 sur le modem distant, l'unité CSU ou l'unité DSU. 3. Vérifiez que le câble utilisé est le bon. 4. Si le protocole de ligne ne s'affiche toujours pas, il peut s'agir d'un échec du matériel ou bien un problème de câblage. Insérez une boîte de dérivation et observez les lignes de commande. 5. Remplacez les pièces défectueuses si nécessaire.

Dépannage d'une interface série (suite)

Dépannage d'une interface série

Ligne d'état	Condition possible	Problème / Solution
Serial x is up, line protocol is up (looped)	Le circuit comporte une boucle. Le numéro de séquence du paquet de test d'activité adopte un numéro aléatoire à la détection initiale d'une boucle. Si le même numéro aléatoire est renvoyé sur la liaison, le circuit comporte une boucle.	1. Utilisez la commande d'exécution privilégiée `show running-config` pour rechercher les entrées de commande de configuration `loopback`. 2. Si vous trouvez une entrée de commande de configuration d'interface `loopback`, utilisez la commande de configuration d'interface `no loopback` pour supprimer la boucle. 3. S'il n'y a pas d'entrée de commande de configuration `loopback`, examinez le CSU/DSU pour déterminer s'ils sont configurés en mode de bouclage manuel. Si oui, désactivez le bouclage manuel. 4. Après avoir désactivé le mode de bouclage manuel sur le CSU/DSU, réinitialisez-le, puis inspectez le statut de la ligne. Si le protocole de ligne s'affiche, aucune autre action n'est nécessaire. 5. Si après inspection le CSU ou le DSU ne peuvent pas être configurés manuellement, contactez le service de la ligne louée ou de l'opérateur pour obtenir une assistance au dépannage de la ligne.

Dépannage d'une interface série (suite)

Dépannage d'une interface série

Ligne d'état	Condition possible	Problème / Solution
Serial x is up, line protocol is down (disabled)	Un taux élevé d'erreurs c'est produit, en raison d'un problème du fournisseur de services WAN. Un problème matériel du CSU ou du DSU s'est produit. Le matériel du routeur (interface) est défectueux.	1. Dépannez la ligne avec un analyseur série et une boîte de dérivation. Recherchez les signaux de basculement CTS et DSR. 2. Boucle CSU/DSU (boucle DTE). Si le problème persiste, un problème matériel est vraisemblablement en cause. Si le problème ne persiste pas, un problème du fournisseur de services WAN est vraisemblablement en cause.
		3. Changez le matériel défectueux si nécessaire (CSU, DSU, commutateur, routeur local ou distant).

Dépannage d'une interface série (suite)

Dépannage d'une interface série

Ligne d'état	Condition possible	Problème / Solution
Serial x is administratively down, line protocol is down	La configuration du routeur comprend la commande de configuration d'interface `shutdown`. Il existe une adresse IP dupliquée.	1. Vérifiez la configuration du routeur pour la commande `shutdown`. 2. Utilisez ensuite la commande de configuration d'interface `no shutdown` pour supprimer la commande `shutdown`. 3. Vérifiez qu'aucune adresse IP identique n'utilise la commande exécution privilégiée `show running-config`, ni la commande d'exécution `show interfaces`. 4. En présence d'adresses dupliquées, résolution du conflit par le remplacement d'une adresse IP.

Packet tracer 3.1.2.7

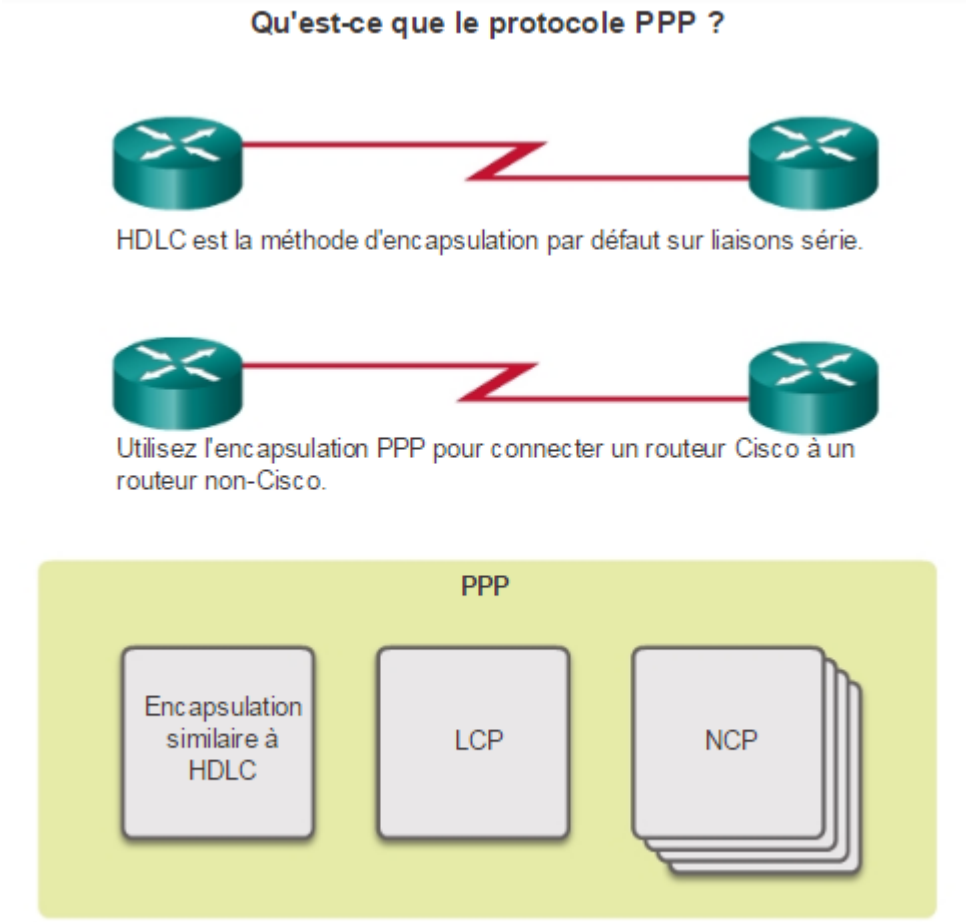
3.2 **Fonctionnement de PPP**

Cisco | Networking Academy®
Mind Wide Open™

Présentation du protocole PPP

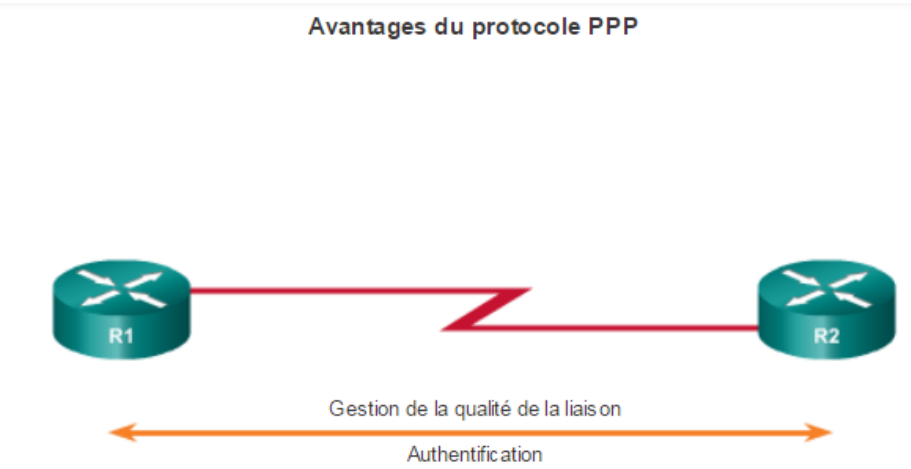
Le protocole PPP comprend trois parties principales :

- Un tramage similaire à celui du HDLC, pour le transport de paquets multiprotocoles sur les liaisons point à point.
- Le protocole extensible LCP (Link Control Protocol) qui permet d'établir, de configurer et de tester la connexion de la liaison de données.
- Une famille de protocoles NCP (Network Control Protocols) pour établir et configurer différents protocoles de couche réseau. (IPv4, IPv6, AppleTalk, Novell IPX, and SNA Control Protocol)



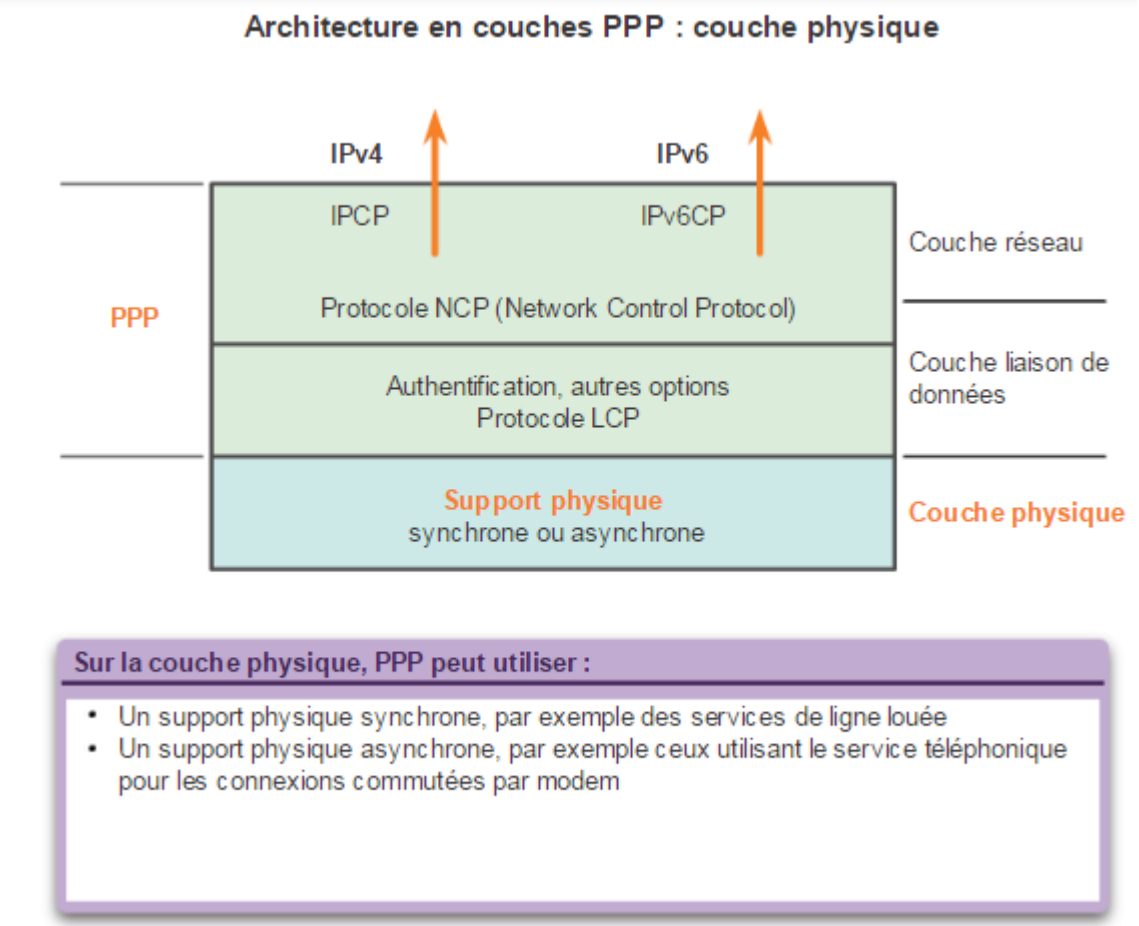
Avantages du protocole PPP

- PPP ne s'agit pas d'un protocole propriétaire.
- Le protocole PPP comprend de nombreuses fonctionnalités non disponibles dans HDLC :
  - La fonction de gestion de la qualité de la liaison, surveille la qualité de la liaison. Si un nombre trop important d'erreurs est détecté, le protocole PPP désactive la liaison.
  - Prend en charge l'authentification PAP et CHAP.



Architecture en couches PPP

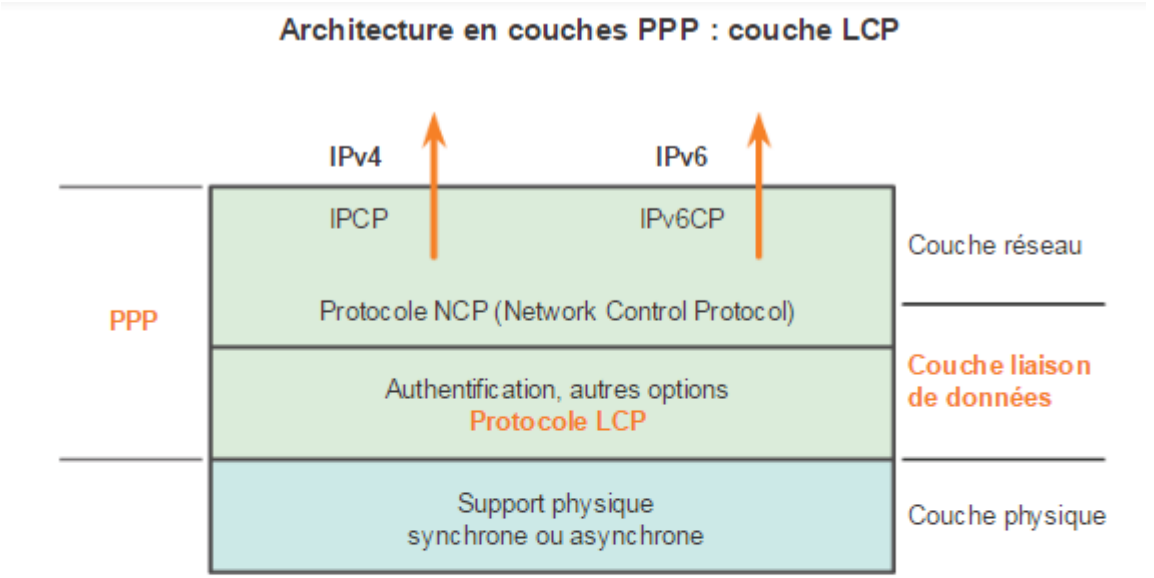
- Le protocole LCP configure la connexion PPP et ses paramètres
- Les protocoles NCP gèrent la configuration des protocoles des couches supérieures
- Le protocole LCP met fin à la connexion PPP



PPP - Protocole LCP (Link Control Protocol)

LCP fournit d'autre part la configuration automatique des interfaces à chaque extrémité, notamment les tâches suivantes

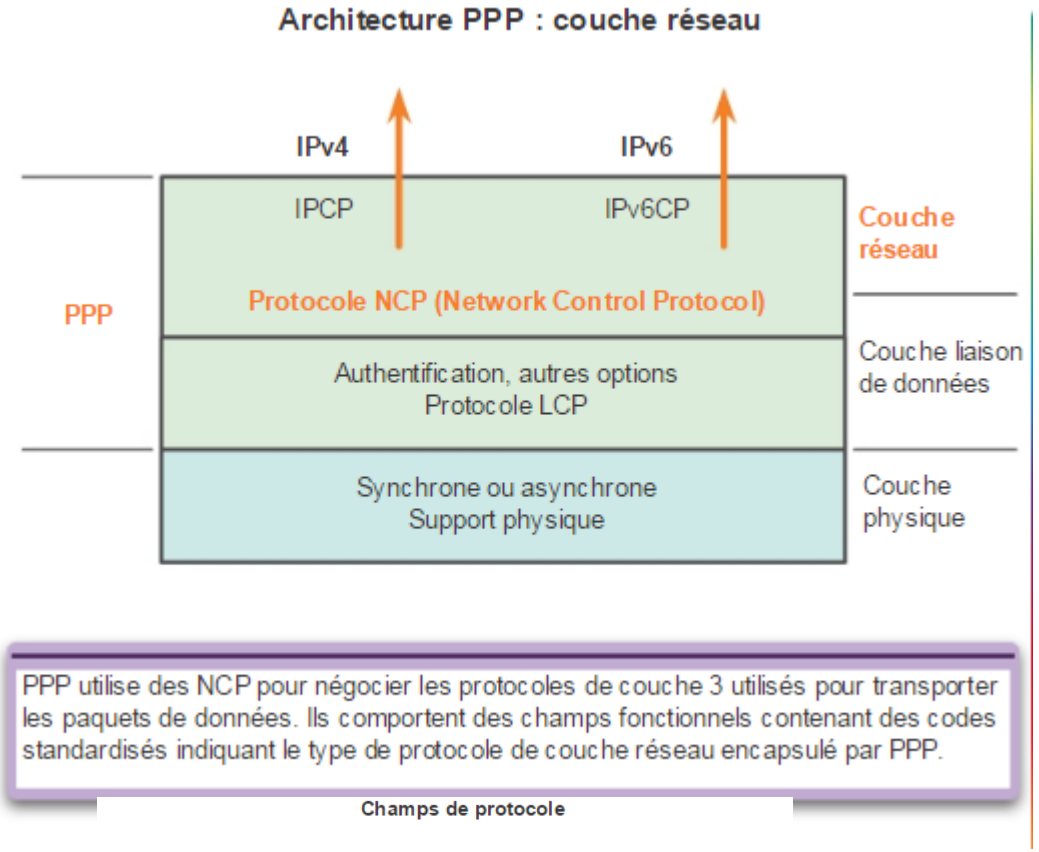
- Gérer les limites variables de taille de paquets.
- Détecter les erreurs de configuration courantes.
- Mettre fin à la liaison.
- Déterminer si une liaison fonctionne correctement ou présente des défaillances.



PPP utilise LCP pour proposer des options de service. Ces options de service sont principalement utilisées pour la négociation et la vérification des trames lors de la mise en place de contrôles point à point spécifiés par un administrateur.

Protocole NCP (Network Control Protocol)

- Le protocole PPP permet à plusieurs protocoles de couche réseau de fonctionner sur la même liaison de communication.
- Pour chaque protocole de couche réseau utilisé, PPP utilise un NCP distinct.

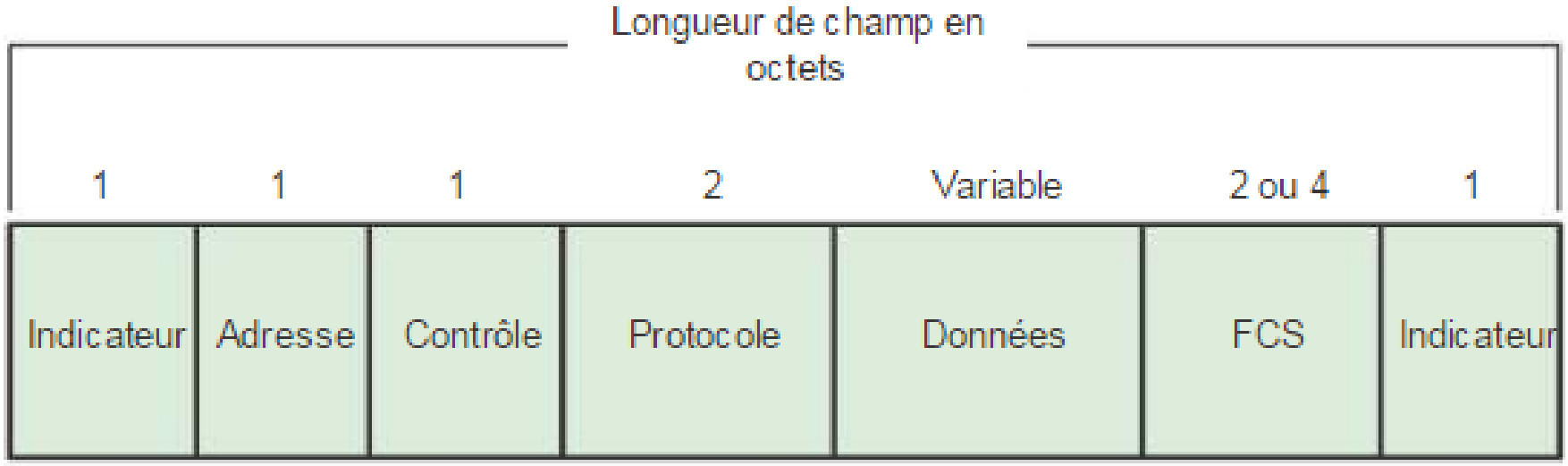


Valeur (hex)	Nom du protocole
8021	Protocole de contrôle du protocole IP (IPv4)
8057	Protocole de contrôle du protocole IP version 6 (IPv6)
8023	Protocole de contrôle de couche réseau OSI
8029	Protocole de contrôle Apple Talk
802b	Protocole de contrôle IPX de Novell
c021	Protocole LCP
c023	Protocole d'authentification du mot de passe (PAP)
c223	Protocole d'authentification à échanges confirmés (CHAP)

LCP et NCP

Structure de trame PPP

Champs de trame PPP

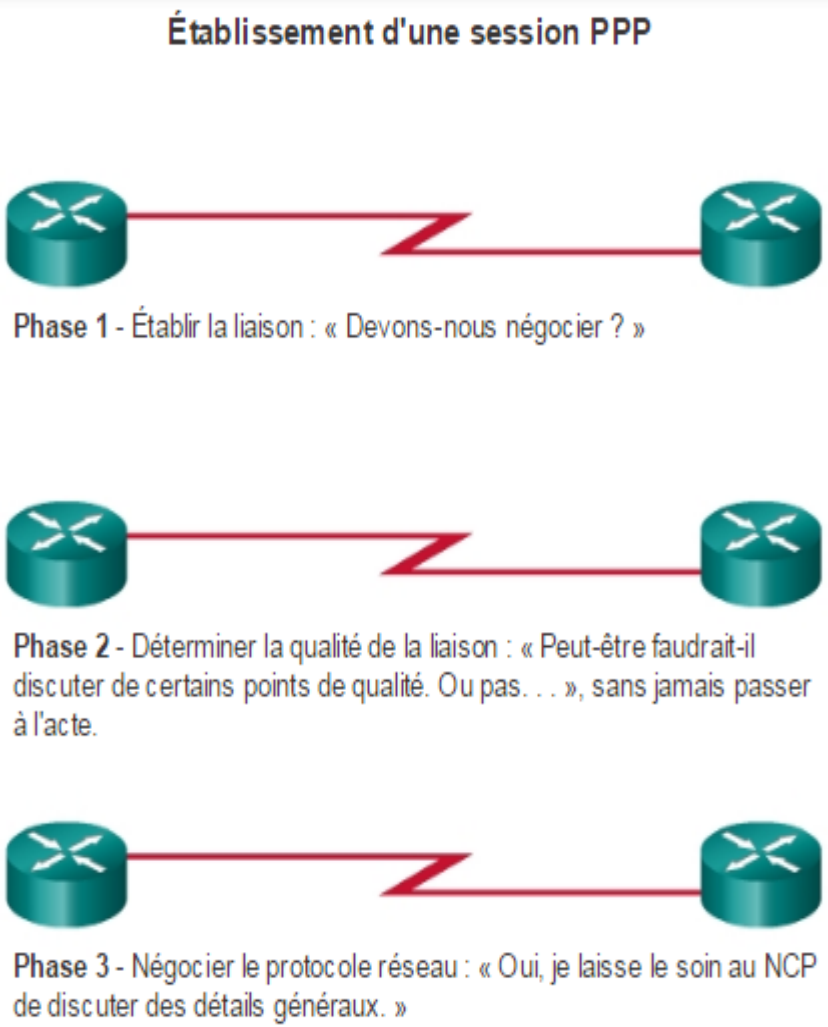


Établissement d'une session PPP

Phase 1 – le protocole LCP doit d'abord ouvrir la connexion et négocier les options de configuration. Cette phase se termine lorsque le routeur récepteur renvoie une trame de reçu de configuration vers le routeur établissant la connexion.

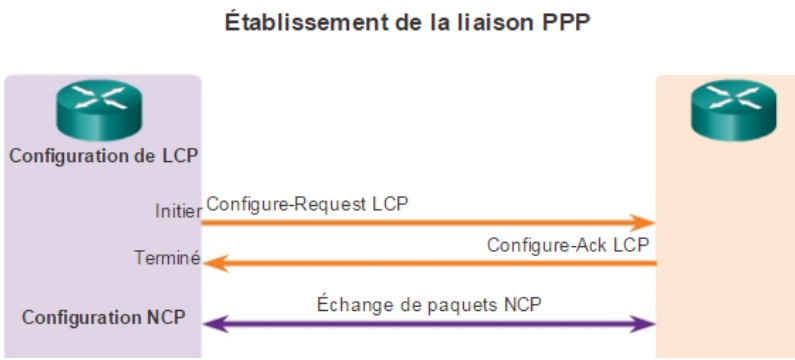
Phase 2 – Le protocole LCP teste la liaison pour déterminer si la qualité de la liaison est suffisante pour utiliser les protocoles de couche réseau.

Phase 3 – Lorsque le protocole LCP a terminé la phase liée à la qualité de la liaison, le protocole NCP correspondant peut configurer séparément les protocoles de couche réseau et les démarrer et les arrêter à tout moment.



Fonctionnement du protocole LCP

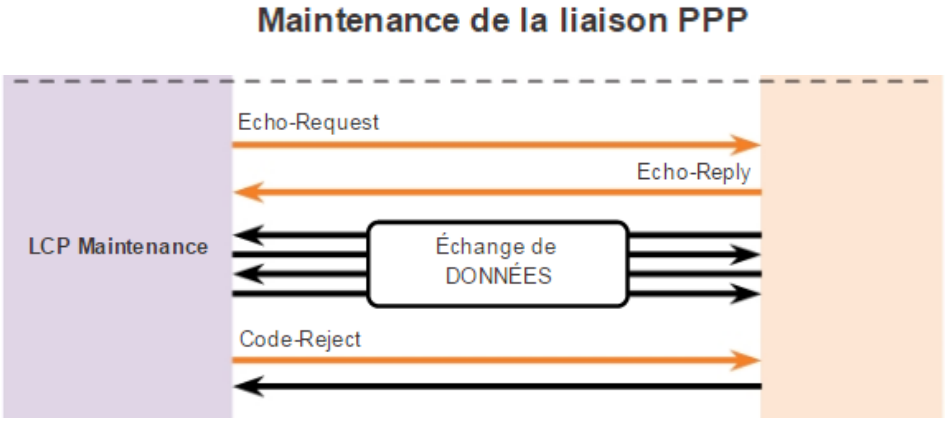
- Le fonctionnement du protocole LCP comprend l'établissement de la liaison, sa maintenance et sa fermeture.
- LCP utilise trois classes de trames LCP pour effectuer le travail de chaque phase LCP :
  - Les trames d'établissement de liaison établissent et configurent la liaison (Configure-Request, Configure-Ack, Configure-Nak et Configure-Reject).
  - Les trames de maintenance de liaison gèrent et déboguent la liaison (Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply et Discard-Request).
  - Les trames de terminaison de liaison mettent fin à la liaison (Terminate-Request et Terminate-Ack).



Fonctionnement du protocole LCP (suite)

Pendant la maintenance de la liaison, LCP peut utiliser des messages pour fournir des commentaires et tester la liaison.

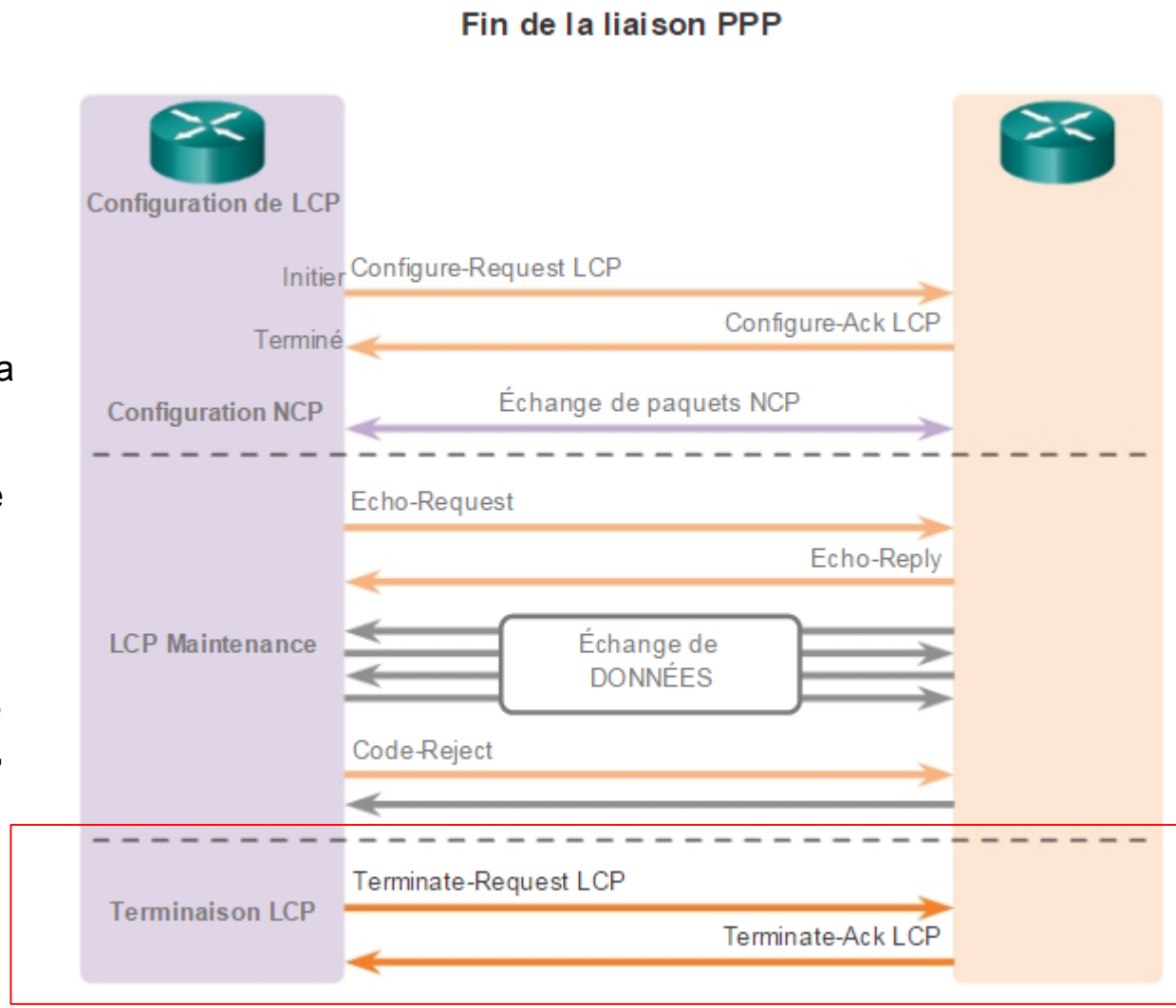
- **Echo-Request, Echo-Reply, and Discard-Request** : ces trames peuvent servir à tester la liaison.
- **Code-Reject and Protocol-Reject** : ces types de trames peuvent fournir des commentaires lorsqu'un des périphériques reçoit une trame non valide, à cause d'un code LCP non reconnu (type de trame LCP) ou d'un identificateur de protocole incorrect. .



Fonctionnement du protocole LCP (suite)

Fin de la liaison

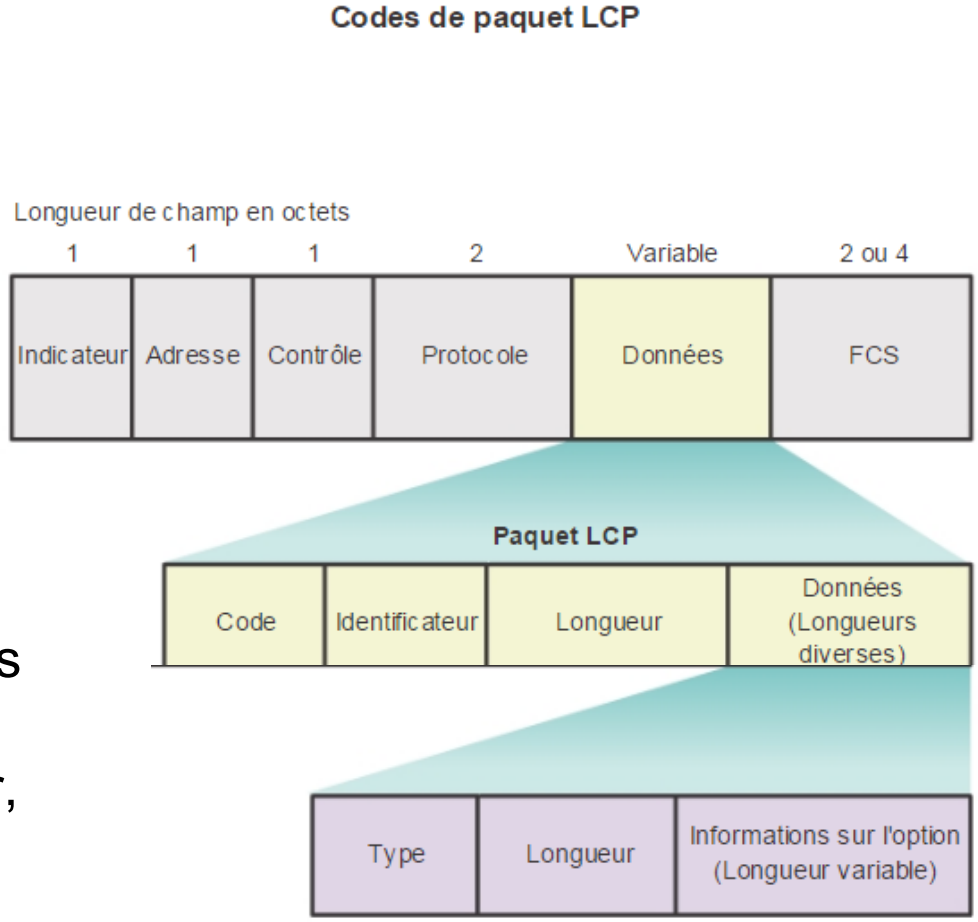
- Une fois le transfert de données effectué au niveau de la couche réseau, le LCP met fin à la liaison, comme illustré à la Figure 3.
- Le protocole NCP ne met fin qu'à la couche réseau et à la liaison NCP. La liaison reste ouverte jusqu'à ce que le protocole LCP la ferme. Si le protocole LCP met fin à la liaison avant le protocole NCP, la session NCP est aussi fermée.
- PPP peut mettre fin à la liaison à tout moment. Cela peut se produire en raison de la perte de l'opérateur, d'un échec d'authentification, d'une défaillance de la qualité de la liaison, de l'expiration d'un compteur de période d'inactivité ou de la fermeture administrative de la liaison.



Paquet LCP

Champs du paquet LCP :

- Code : le champ de code, d'une longueur d'un octet, identifie le type de paquet LCP.
- Identificateur : le champ d'identificateur, d'une longueur d'un octet, sert à mettre en relation les demandes de paquets et les réponses.
- Longueur : le champ de longueur, d'une longueur de deux octets, indique la longueur totale du paquet LCP (avec tous les champs).
- Données : le champ de données est de zéro à plusieurs octets, comme indiqué par le champ de



Paquet LCP

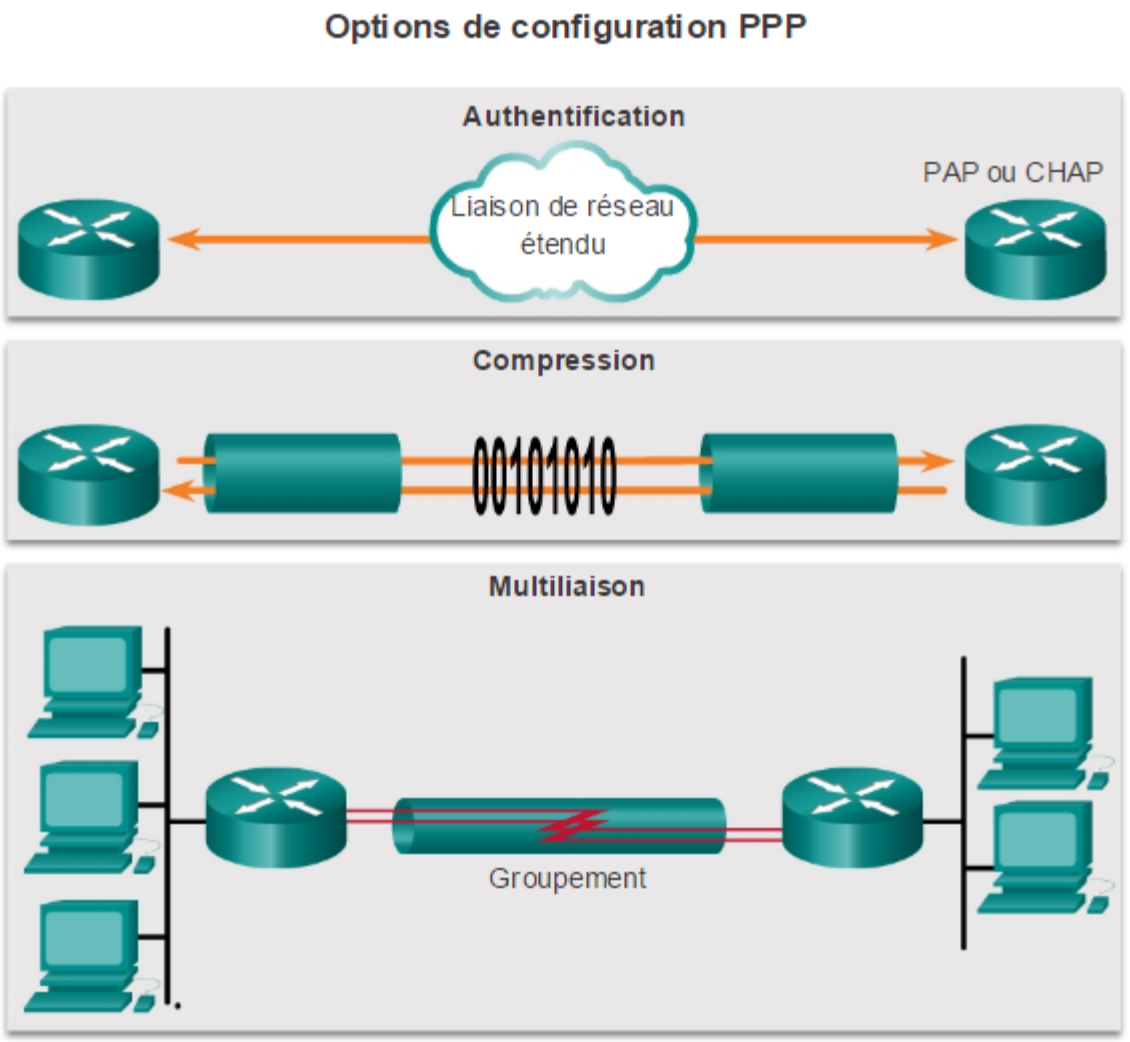
Champs de paquet LCP

Code LCP	Type de paquet LCP	Description
1	Configure-Request	Envoyé pour ouvrir ou demander une connexion PPP. Configure-Request contient une liste des options LCP avec les changements des valeurs par défaut.
2	Configure-Ack	Envoyé lorsque toutes les valeurs des options LCP de la dernière demande Configure-Request reçue sont reconnues et acceptables. Lorsque les deux homologues PPP envoient et reçoivent des messages Configure-Acks, la négociation LCP est terminée.
3	Configure-Nak	Envoyé lorsque toutes les options LCP sont reconnues, mais que les valeurs de certaines options ne sont pas acceptables. Configure-Nak comprend les options qui diffèrent, ainsi que les valeurs acceptables.
4	Configure-Reject	Envoyé lorsque les options LCP ne sont pas reconnues ou ne sont pas acceptables pour la négociation. Configure-Reject comprend les options non reconnues ou non négociables.
5	Terminate-Request	Envoyé éventuellement pour fermer la connexion PPP.
6	Terminate-Ack	Envoyé en réponse au message Terminate-Request.
7	Code-Reject	Envoyé lorsque le code LCP est inconnu. Le message Code-Reject comprend le paquet LCP rejeté.
8	Protocol-Reject	Envoyé lorsque la trame PPP contient un ID de protocole inconnu. Le message Protocol-Reject comprend le paquet LCP rejeté. Protocol-Reject est normalement envoyé par un homologue PPP en réponse à un NCP PPP pour un protocole LAN qui n'est pas activé sur l'homologue PPP.
9	Echo-Request	Envoyé éventuellement pour tester la connexion PPP.
10	Echo-Reply	Envoyé en réponse au message Echo-Request. Les messages Echo-Request et Echo-Reply ne sont pas liés aux messages ICMP Echo Request and Echo Reply.
11	Discard-Request	Envoyé éventuellement pour tester la liaison en sortie.

Options de configuration PPP

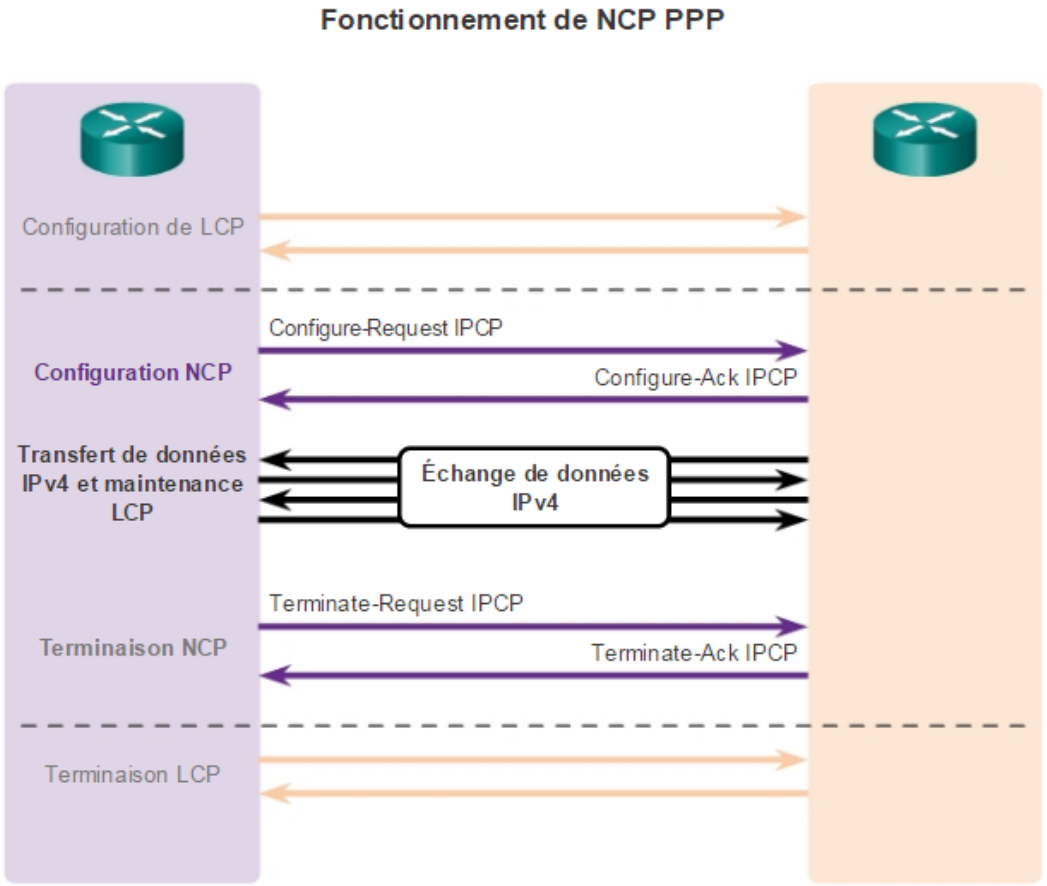
Le protocole PPP peut être configuré pour prendre en charge différentes fonctions optionnelles soient:

- Authentification à l'aide de PAP ou CHAP
- Compression à l'aide de Stacker ou Predictor
- Multiliaison combinant deux canaux ou plus pour étendre la bande passante du WAN



Présentation de NCP

- Une fois la liaison initiée, le protocole LCP transfère le contrôle au NCP correspondant.
- le NCP correspondant est invoqué pour terminer la configuration du protocole de couche réseau utilisé.
- Lorsque le protocole NCP a correctement configuré le protocole de couche réseau, le protocole de réseau présente l'état ouvert sur la liaison LCP établie.
- À ce stade, le protocole PPP peut transporter les paquets de



3.3 Configuration de PPP

Cisco | Networking Academy®
Mind Wide Open™

Options de configuration PPP

- **Authentification** : – Pour l'authentification, les deux choix sont le protocole d'authentification du mot de passe (PAP, Password Authentication Protocol) et le protocole d'authentification à échanges confirmés (CHAP, Challenge Handshake Authentication Protocol).
- **Compression :** – augmente le débit effectif des connexions PPP en diminuant la quantité de données dans la trame qui doit être acheminée sur la liaison. Le protocole décompresse la trame à l'arrivée. Les deux protocoles de compression disponibles sur les routeurs Cisco sont Stacker et Predictor.
- **Détection des erreurs** : identifie les défaillances. Les options Quality et Magic Number aident à assurer que la liaison de données reste fiable et sans boucle. Le champ Magic Number permet de détecter les liaisons qui présentent une boucle. Les numéros magiques sont générés de façon aléatoire à chaque extrémité de la connexion.

PPP Configuration Options (suite)

- **Rappel PPP** : – le rappel PPP permet d'augmenter le niveau de sécurité. Grâce à cette option LCP, un routeur Cisco peut servir de client ou de serveur de rappel. Le client effectue l'appel initial, demande à être rappelé, puis met fin à son appel initial. Le routeur de rappel répond à l'appel initial et rappelle le client en s'appuyant sur ses instructions de configuration. La commande est **ppp callback**[**accept** | **request**].
- **Multiliaison** : – offre un équilibrage de la charge sur les interfaces de routeur utilisées par PPP. Le protocole PPP multiliaison, aussi appelé MP, MPPP, MLP ou Multiliaison, permet de répartir le trafic sur plusieurs liaisons WAN physiques, tout en assurant la fragmentation et le réassemblage des paquets, le séquençage, l'interopérabilité entre fournisseurs et l'équilibrage de la charge de travail sur le trafic entrant et sortant.

Commande de configuration PPP de base

Configuration PPP de base


```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
encapsulation ppp
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
encapsulation ppp
```

Configuration de PPP

Commandes de compression PPP

Compression PPP


```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
compress predictor
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
compress predictor
```

```
Router(config if)# compress [predictor | stac]
```

Mot-clé	Description
`predictor`	(Facultatif) Spécifie qu'un algorithme de compression Predictor va être utilisé.
`stac`	(Facultatif) Spécifie qu'un algorithme de compression Stacker (LZS) va être utilisé.

Commande de contrôle de la qualité de la liaison PPP

La commande **ppp quality** *percentage* permet de s'assurer que la liaison répond aux exigences de qualité qui ont été définies, sinon la liaison se ferme.

Contrôle de la qualité de la liaison PPP


```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
 ppp quality 80
```

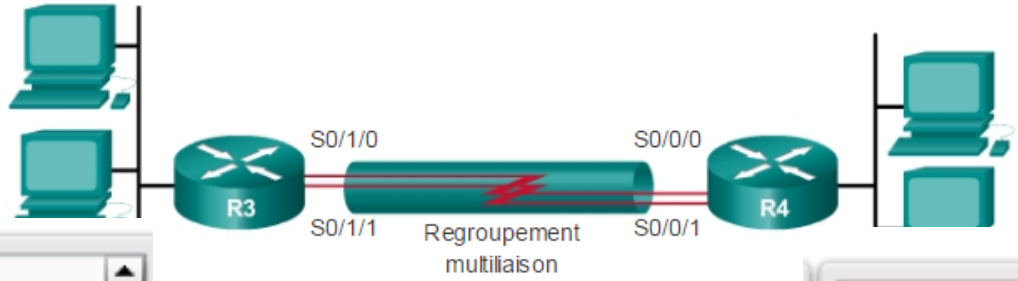
```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp quality 80
```

```
Router(config-if)# ppp quality percentage
```

Mot-clé	Description
percentage	Spécifie le seuil de qualité de la liaison. Compris entre 1 et 100.

Commandes de multiliaison PPP

Multiliaison PPP




```
hostname R3
!
interface Multilink 1
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

```
hostname R4
!
interface Multilink 1
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

Configuration de PPP

Vérification de la configuration PPP

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.
show interfaces serial	Displays information about a serial interface.
show ppp multilink	Displays information about a PPP multilink interface.

```
R2# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, IPV6CP, CCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters 01:29:06
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: weighted fair
```

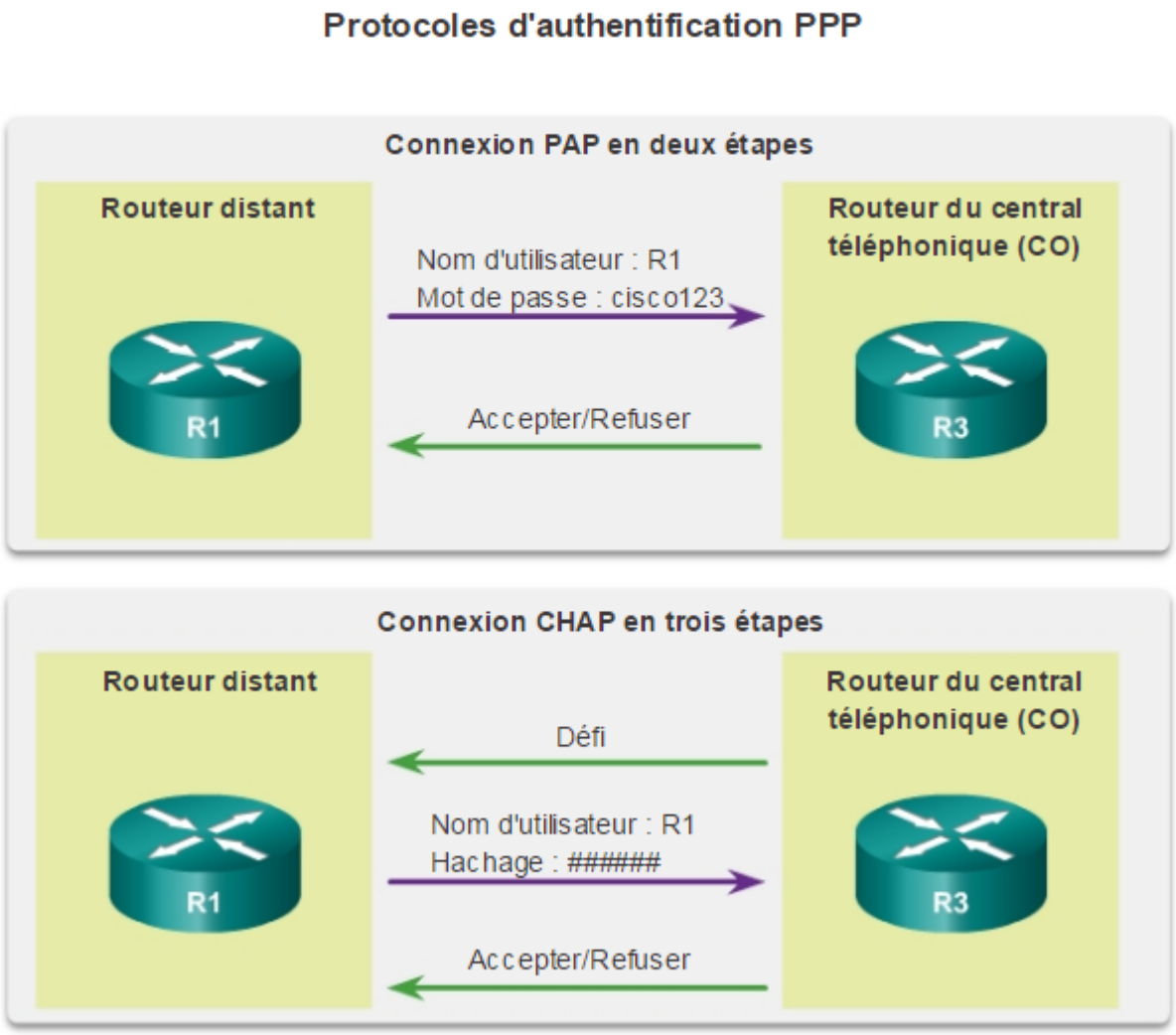
Vérification de la configuration PPP(suite)

La commande **show ppp multilink** vérifie que la multiliaison PPP est activée sur R3, comme illustré à la Figure 3. Le résultat indique l'interface Multilink 1, les noms d'hôte des terminaux locaux et distants, ainsi que les interfaces série affectées au regroupement multiliaison.

```
R3# show ppp multilink

Multilink1
  Bundle name: R4
  Remote Endpoint Discriminator: [1] R4
  Local Endpoint Discriminator: [1] R3
  Bundle up for 00:01:20, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x2 received sequence, 0x2 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/1/1, since 00:01:20
    Se0/1/0, since 00:01:06
No inactive multilink interfaces
R3#
```

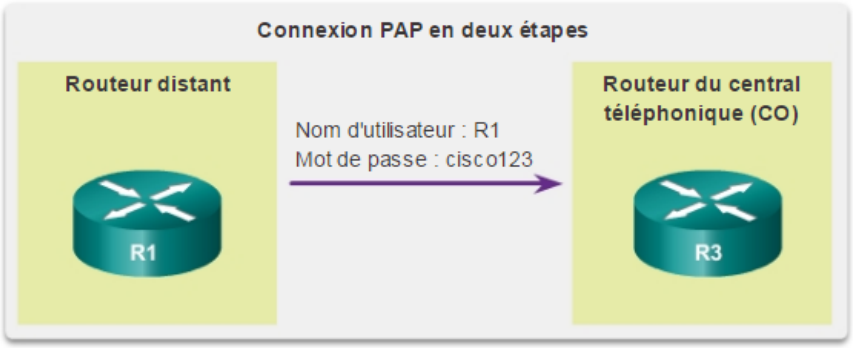
Protocoles d'authentification PPP



Protocole d'authentification du mot de passe (PAP)

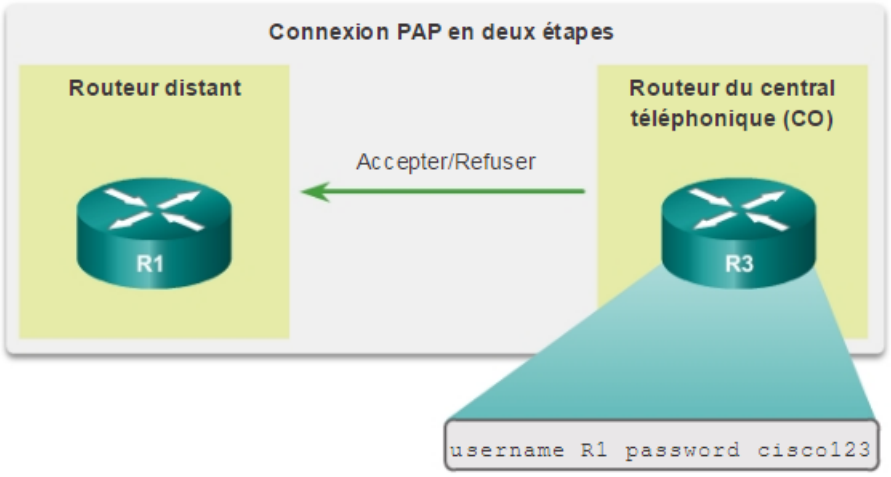
Initialisation PAP

R1 envoie son nom d'utilisateur et son mot de passe PAP à R3.



Finalisation PAP

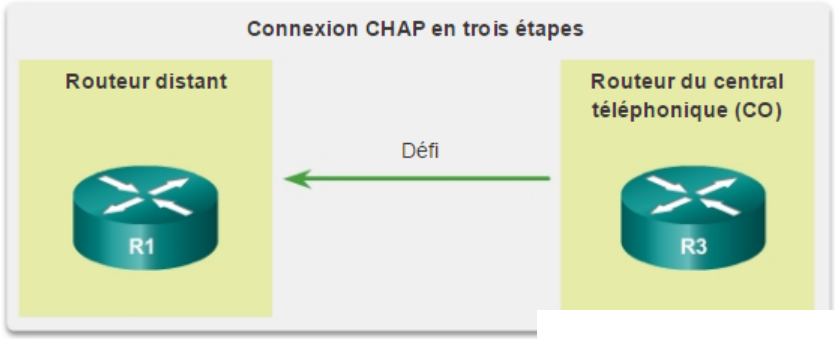
R3 compare le nom d'utilisateur et le mot de passe de R1 avec les informations de sa base de données locale. S'ils correspondent, il accepte la connexion. Sinon, il rejette la connexion.



Protocole d'authentification à échanges confirmés (CHAP)

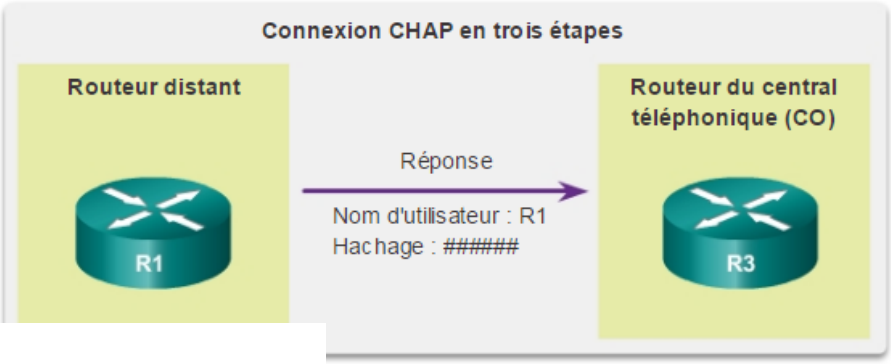
Initialisation CHAP

R3 initie la connexion en 3 étapes et envoie un message de confirmation à R1.



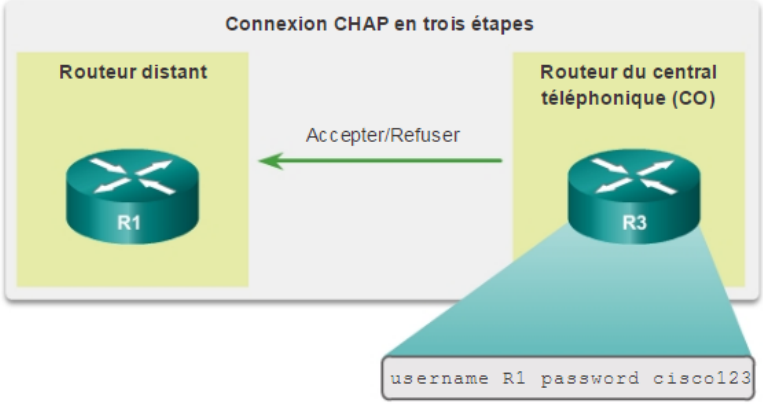
Réponse CHAP

R1 répond au message de confirmation CHAP de R3 en envoyant son nom d'utilisateur CHAP et une valeur de hachage basée sur le mot de passe CHAP.



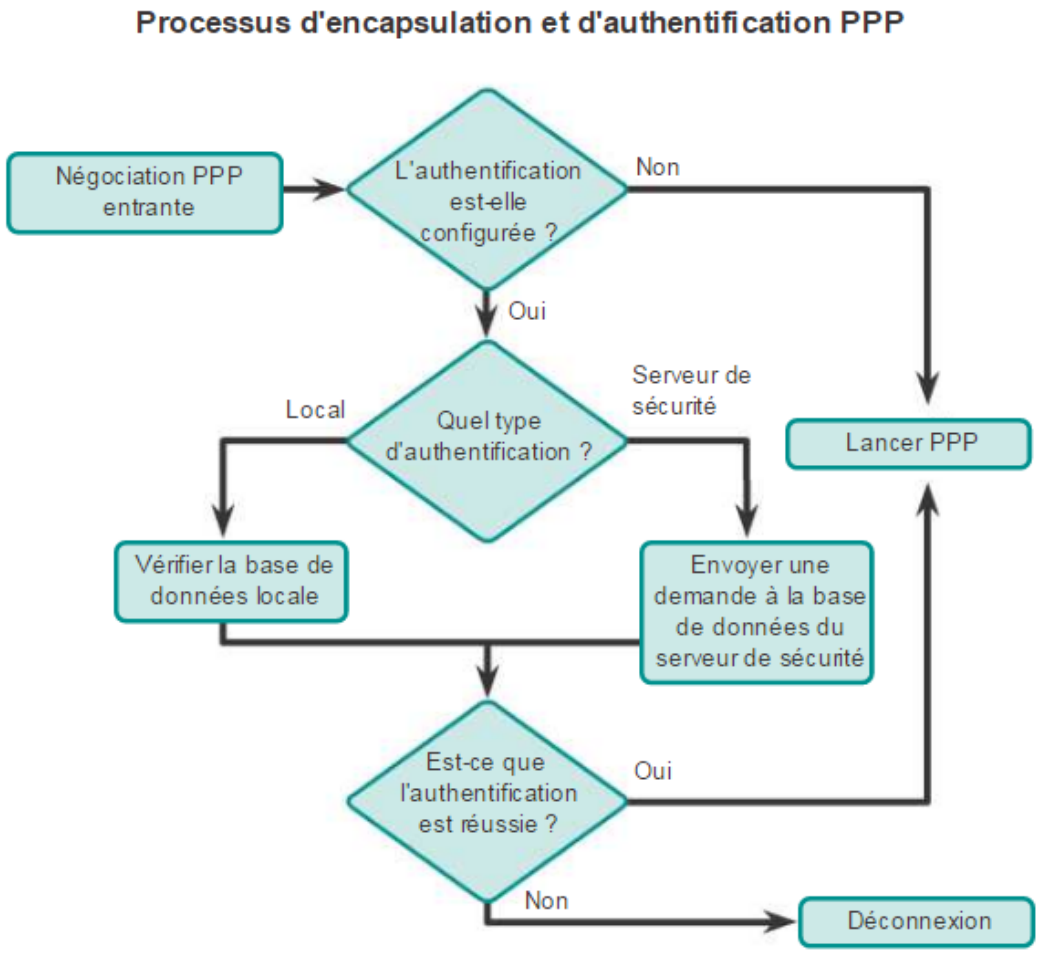
Finalisation CHAP

Avec le nom d'utilisateur et le mot de passe de R1 stockés dans sa base de données locale, R3 compare sa valeur de hachage calculée avec celle envoyée par R1.



Authentification PPP

Processus d'encapsulation et d'authentification PPP



Authentification PPP

Configuration de l'authentification PPP

Commande `ppp authentication`

```
ppp authentication {chap | chap pap | pap chap | pap} [if-needed]
[list-name | default] [callin]
```

Commande `ppp authentication`	
`chap`	Active CHAP sur une interface série.
`pap`	Active PAP sur une interface série.
`chap pap`	Active CHAP et PAP, et exécute l'authentification CHAP avant PAP.
`pap chap`	Active CHAP et PAP, et exécute l'authentification PAP avant CHAP.
`if-needed` (Optional)	Utilisée avec TACACS et XTACACS. N'exécute pas l'authentification CHAP ou PAP si l'utilisateur a déjà fourni une authentification. Cette option n'est disponible que sur les interfaces asynchrones.
`list-name` (Optional)	Utilisé avec AAA/TACACS+. Spécifie le nom d'une liste de méthodes d'authentification TACACS+ à utiliser. Si aucun nom de liste n'est spécifié, le système utilise celle par défaut. Les listes sont créées avec la commande `aaa authentication ppp` .
`default` (Optional)	Utilisé avec AAA/TACACS+. Créé avec la commande `aaa authentication ppp` .
`callin`	Spécifie l'authentification sur les appels entrants (reçus) uniquement.

Configuration du protocole PPP avec authentification **(suite)**

Configuration de l'authentification PAP


```
hostname R1
username R2 password someone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R1 password
 someone
```

```
hostname R2
username R1 password someone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password
 someone
```

Configuration du protocole PPP avec authentification **(suite)**

Configuration de l'authentification CHAP


```
hostname R1
username R2 password sameone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication chap
```

```
hostname R2
username R1 password sameone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication chap
```

3.4 Dépannage de la connectivité WAN

Cisco | Networking Academy®
Mind Wide Open™

Dépannage du protocole PPP avec encapsulation de série

Paramètres de la commande debug ppp

```
debug ppp {packet | negotiation | error | authentication |
compression | cbcp}
```

Paramètre	Utilisation
packet	Affiche les paquets PPP envoyés et reçus. (Cette affiche les sorties de paquets de bas niveau.)
negotiation	Affiche les paquets PPP transmis lors du démarrage de PPP, au moment où les options PPP sont négociées.
error	Affiche les erreurs de protocole et les statistiques d'erreur associées à la négociation et à l'utilisation de la connexion PPP.
authentication	Affiche les messages du protocole d'authentification, notamment les échanges de paquets CHAP (Challenge Handshake Authentication Protocol) et les échanges PAP (Password Authentication Protocol).
compression	Affiche les informations spécifiques à l'échange de connexions PPP avec le protocole MPPC. Cette commande est utile pour obtenir le numéro de séquence des paquets incorrects lorsque la compression MPPC est activée.
cbcp	Affiche les erreurs de protocole et les statistiques d'erreur associées aux négociations de connexion PPP via MSCB.

Dépannage d'une configuration PPP avec authentification

```
R2# debug ppp authentication

Serial0: Unable to authenticate. No name received from peer
Serial0: Unable to validate CHAP response. USERNAME pioneer not
found.
Serial0: Unable to validate CHAP response. No password defined for
USERNAME pioneer
Serial0: Failed CHAP authentication with remote.
Remote message is Unknown name
Serial0: remote passed CHAP authentication.
Serial0: Passed CHAP authentication with remote.
Serial0: CHAP input code = 4 id = 3 len = 48
```

Configuration de PPP avec l'authentification

- Commandes: Configuration de R1 et R2 pour utiliser l'authentification PAP

Routeur Source (Configuration de R1 pour utiliser l'authentification PAP avec R2)
R1(config)#username R2 password cisco123 (cette commande permet au routeur distant R2 de se connecter à R1 en utilisant le mot de passe
cisco123, le nom étant toujours celui du routeur distant))
R1(config)#interface s0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password cisco123 (c'est le nom d'utilisateur et le mot de passe du routeur source qui seront envoyés à R2)
R1(config-if)#end

Routeur Distant (Configuration de R2 pour utiliser l'authentification PAP avec R1)
R2(config)#username R1 password cisco123 (cette commande permet au routeur distant R2 de se connecter à R1 en utilisant le mot de passe cisco123, le nom étant toujours celui du routeur distant))
R2(config)#interface s0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R2 password cisco123 (c'est le nom d'utilisateur et le mot de passe du routeur source qui seront envoyés à R1)

Chapter 3: Summary

- Point-to-Point links are usually more expensive than shared services; however, the benefits may outweigh the costs. Constant availability is important for some protocols, such as VoIP.
- SONET is an optical network standard that uses STDM for efficient use of bandwidth.
- The demarcation point is the point in the network where the responsibility of the service provider ends and the responsibility of the customer begins. The CPE, usually a router, is the DTE device. The DCE is usually a modem or CSU/DSU.
- Cisco HDLC is a bit-oriented synchronous data link layer protocol extension of HDLC and is used by many vendors to provide multiprotocol support. This is the default encapsulation method used on Cisco synchronous serial lines.
- Synchronous PPP is used to connect to non-Cisco devices, to monitor link quality, provide authentication, or bundle links for shared use
- LCP is the PPP protocol used to establish, configure, test and terminate the data link connection. LCP can optionally authenticate a peer using PAP or CHAP.