Chapitre 3- Réseaux étendus

SMI-S6 - 2015

- Introduction aux connexions de réseaux étendus
- Commutation de paquets
- Commutation de circuits
- Protocoles d'encapsulation des réseaux WAN
- PPP
- Les Travaux Pratiques

Pr. Hafssa BENABOUD, benaboud@gmail.com

Introduction aux connexions de réseaux étendus

Le réseau étendu permet d'étendre le réseau d'entreprise en connectant les sites géographiquement éloignés entre eux. La connexion requise dépend des exigences des utilisateurs et des coûts.

→ Un WAN est différent d'un réseau local (LAN):

Abonnement à un fournisseur extérieur pour pouvoir utiliser les ressources d'un réseau que votre organisation ne possède pas. (exemple: service téléphonique)

Les standards WAN

Les standards WAN sont définis et gérés par un certain nombre d'autorités reconnus, parmi lesquelles:

- L'**UIT-T** (Union Internationale des Télécommunications, secteur normalisation) anciennement **CCITT** (Comité Consultatif International Télégraphique et Téléphonique)
- L'**ISO** (International Organisation for Standardization)
- L'**IETF** (Internet Engineering Task Force)
- L'**EIA** (Electronic Industries Association)

Les standards WAN décrivent généralement les méthodes de livraison de la couche physique et les exigences de la couche liaison de données, notamment ***l'adressage physique***, le ***contrôle de flux*** et l'***encapsulation***.

Réseaux étendus et modèle OSI

✓ Les opérations du réseau étendu concernent principalement les couches physique et Liaison de données du modèle OSI.

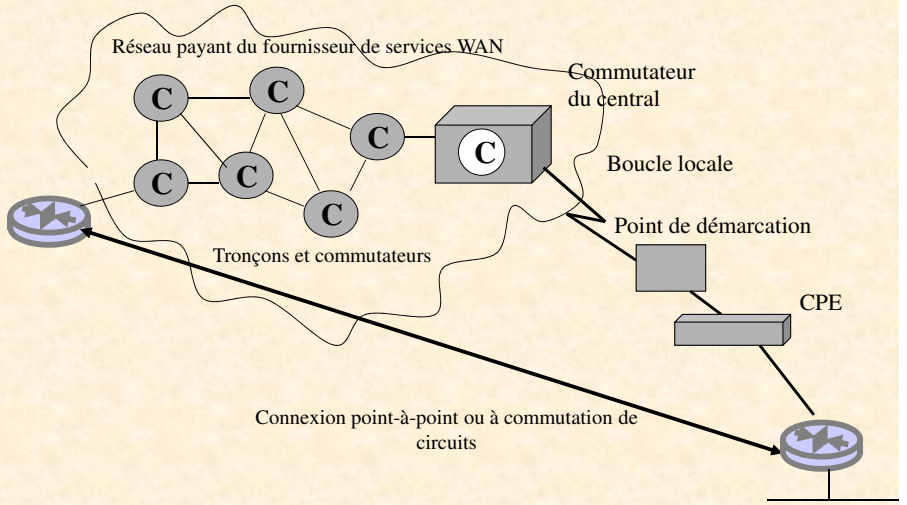
✓ Les protocoles de la couche1 décrivent comment fournir des connexions électriques, mécaniques, opérationnelles et fonctionnelles aux services offerts par un fournisseur de services de communications.

✓Les protocoles de la couche 2 définissent comment des données sont encapsulées pour être transmises vers un emplacement distant ainsi que les mécanismes de transfert des trames résultantes.

Interface avec les fournisseurs des services WAN

Les termes les plus couramment utilisés pour les parties principales d'un réseau étendu entre un utilisateur et le fournisseur sont:

- *l'équipement d'abonné (**CPE**, Customer Premises Equipment)*
- *point de démarcation*
- *boucle locale*
- *commutateur du central*
- *réseau payant*



Equipement de télécommunication du client (CPE) *sont physiquement situés sur le site de l'abonné. Ils incluent à la fois les équipements que possède l'abonné et ceux loués au fournisseur de services. Par exemple, les terminaux, les téléphones et les modems, qui permettent la connexion au service du fournisseur, sont considérés comme des équipements du client. L'abonné doit savoir comment interfacer les dispositifs de son équipement avec le service du fournisseur.*

Point de démarcation *est l'endroit où l'équipement du client se termine et la portion boucle locale du service commence. Cette limite se situe souvent au niveau d'une armoire de télécommunication (une pièce contenant un bloc de câblage du fournisseur)*

Boucle locale *se compose de câbles (généralement en fil de cuivre) qui s'étendent du point de démarcation vers le centre du fournisseur de service. La boucle locale s'étend généralement sur une distance relativement courte vers les locaux les plus proches de la compagnie de téléphone.*

Commutateur *au niveau* **du central** *du fournisseur est un équipement de commutation qui fournit le point de présence le plus proche du service WAN du fournisseur*

Le central agit en tant que:

- *point d'entrée dans le nuage WAN pour appeler*
- *un point de sortie du WAN pour les équipements appelés*
- *un point de commutation pour les appels qui traversent le service.*

Réseau payant. *Les commutateurs et les services pris collectivement (appelés tronçons) à l'intérieur du nuage du fournisseur du réseau étendu constituent le réseau payant. Le trafic de l'appelant peut traverser un tronçon vers un centre principal, puis arriver sur un centre de section puis sur un centre de région ou d'un opérateur international à mesure qu'il traverse les longues distances qui le séparent de la destination.*

Les commutateurs opèrent au niveau des bureaux du fournisseur avec des frais calculés sur la base de tarifs ou de débits autorisés.

Souvent pour des circuits point à point s'étendant jusqu'à des limites régionales ou nationales, la connexion sur le réseau payant est gérée par plusieurs fournisseurs.

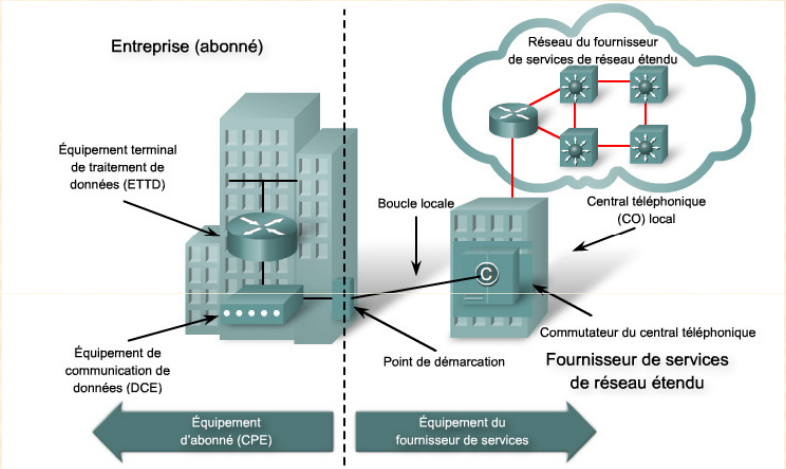
Couche physique WAN

*- La couche physique WAN décrit l'interface entre l'équipement terminal de traitement de données, ou **ETTD** (**DTE**, Data Terminal Equipement), et l'équipement terminal de circuit de données, l'**ETCD** (**DCE**, Data Circuit-terminating Equipement).*

- Habituellement, le DCE est un fournisseur de services, et le DTE est le dispositif connecté.

*- Les services offerts au DTE sont rendus disponibles via un modem ou **CSU/DSU** (Channel Service Unit/Data Service Unit)*

En français: Unité de service du canal/unité de service de données



Terminologie de couche physique de réseau étendu

Couche liaison de données: protocoles WAN

Les protocoles de liaison de données décrivent comment les trames sont transportées entre systèmes sur une seule liaison. Cela comprend des protocoles développés pour fonctionner sur différents types d'installations telles que:

*- **Services point à point dédiés.** Par exemple, un bureau connecté directement à un autre par l'intermédiaire d'une connexion WAN*

*- **Services multipoints basés sur des services dédiés.** Par exemple, un siège central connecté à trois succursale (connexion multipoint) et ces dernières connectées les unes aux autres au moyen du même type de connexion multipoint.*

*- **Services commutés multi-accès.** Par exemple, un siège central et trois succursale connectées au sein d'un nuage WAN, par exemple Frame Relay. Leur communications sont commutées à travers le nuage, et n'empruntent pas obligatoirement le même chemin chaque fois.*

Commutation de circuits

Un réseau à commutation de circuits établit un circuit (ou canal) dédié entre des nœuds et des terminaux avant que les utilisateurs puissent communiquer.

Le chemin interne emprunté par le circuit entre les échanges est partagé par un certain nombre de conversations. Le multiplexage temporel (TDM) permet de partager la connexion à tour de rôle entre chaque conversation. Le multiplexage temporel assure qu'une connexion de capacité fixe soit mise à la disposition de l'abonné.

RTPC et RNIS sont deux types de technologie à commutation de circuits qui peuvent être utilisés pour implémenter un réseau étendu dans une configuration d'entreprise.

Commutation de paquets

Contrairement à la commutation de circuits, la commutation de paquets fractionne les données de trafic en paquets acheminés sur un réseau partagé.

Les réseaux à commutation de paquets ne requièrent pas l'établissement d'un circuit et permettent à de nombreuses paires de nœuds de communiquer sur le même canal.

Des exemples de connexions à commutation de paquets ou de cellules sont X.25, Frame Relay et ATM

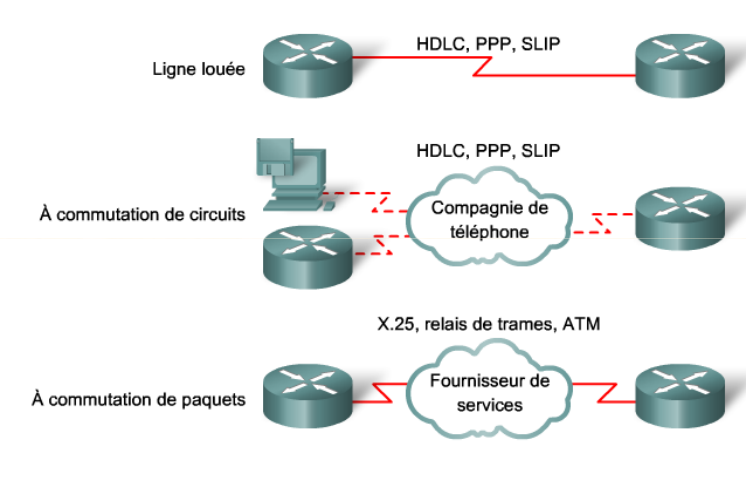
Protocoles d'encapsulation de réseau étendu

➢Sur chaque connexion de réseau étendu, des données sont encapsulées dans des trames avant d'atteindre la liaison de réseau étendu.

➢Pour s'assurer que le protocole correct est utilisé, vous devez configurer le type d'encapsulation de couche 2 approprié. Le choix du protocole dépend de la technologie de réseau étendu et de l'équipement de communication

les protocoles de réseau étendu les plus utilisés sont :

- HDLC- High-Level Data Control
- X25/ LAPB- Link Access Procedure, Balanced
- Version Frame Relay simplifiée du délimitage de trames HDLC
- SLIP - Serial Line Internet Protocol
- PPP- Point-to-Point Protocol
- ATM – Asynchronous Transfer Mode



HDLC *Type d'encapsulation par défaut sur des connexions point à point, des liaisons dédiées et des connexions à commutation de circuits lorsque la liaison utilise deux périphériques Cisco. HDLC sert maintenant de base au protocole PPP synchrone utilisé par de nombreux serveurs pour se connecter à un réseau étendu, le plus souvent Internet.*

PPP *a été développé par l'IETF et est décrit dans le RFC 1661. Il fournit des connexions entre des routeurs et entre un hôte et un réseau au moyen de circuits synchrones et asynchrones. Il contient un champ de protocole servant à identifier le protocole de couche réseau. Le protocole PPP possède également des mécanismes intégrés de sécurité, tels que PAP et CHAP.*

SLIP Protocole standard pour les connexions série point à point, qui utilise TCP/IP. SLIP a été largement remplacé par PPP.

LAPB *Procédure d'accès en mode équilibré, est principalement utilisé sur les réseaux X.25, mais peut également servir de simple moyen de transport de liaison de données. Il dispose de fonctions de détection des trames désordonnées ou manquantes, et d'échange, de retransmission, et d'acquittement des trames.*

X.25 *Norme d'ITU-T qui définit comment maintenir des connexions entre ETTD et DCE pour permettre l'accès à distance à des terminaux et la communication entre ordinateurs dans un réseau public de données. X.25 a précédé le relais de trames.*

Frame Relay *utilisent des techniques numériques perfectionnées dans lesquelles le contrôle d'erreur de LAPB est nécessaire. En utilisant une fonction de délimitation de trames simplifiée sans mécanisme de correction d'erreur, Frame Relay peut envoyer des informations de la couche 2 très rapidement par rapport aux autres protocoles WAN. Le relais de trames est la génération suivante après X.25. Le relais de trames élimine certains des processus fastidieux (tels que la correction des erreurs et le contrôle de flux) employés dans X.25.*

ATM *- Norme internationale en matière de relais de cellules, selon laquelle des périphériques envoient des types de services multiples (tels que la transmission de la voix, des données ou des vidéos) dans des cellules de longueur fixe (53 octets). Les cellules de longueur fixe permettent au traitement d'avoir lieu au niveau matériel, réduisant ainsi les délais d'acheminement. Le mode ATM exploite les supports de transmission à haut débit, tels que E3, SONET et T3.*

Le service SLIP: Serial Line IP

C'est un protocole simple développé par 3Com au début des années 1980 puis inclus dans 4.2BSD et SunOS en 1984.

Ce protocole se caractérise par:

- Aucun contrôle ni échange d'adresse des extrémités;

- Passage limité au protocole IP, aucune notion d'identificateur de protocole;

- Pas d'authentification;

- Pas de négociation des paramètres de communication;

- Pas de checksum.

- Pour plus d'information → RFC 1055

***SLIP** est un ancien protocole remplacé par **PPP**, qui ne pouvait permettre que le transport de paquets IP.*

Le service PPP

- L'origine de PPP
- Les protocoles PPP
- Composants de PPP en couches
- L'authentification PPP
- Etablir une liaison PPP
- Configuration de PPP sur un routeur Cisco

L'origine de PPP

- protocole développé sur VAX 4.3BSD début 1989.

- décrit dans les RFCs 1661 et 1332

- il encapsule des informations de protocoles de la couche réseau sur des liaisons point-à-point.

- est désigné pour travailler avec différents protocoles de la couche réseau et possède , en plus, un protocole sécurisé,

- c'est le protocole de réseau WAN le plus répandu, successeur du protocole SLIP, il permet:

- *la connexion entre routeurs ou entre un hôte et un routeur;*
- *la gestion des circuits synchrones et asynchrones;*
- *le contrôle de la configuration des liaisons;*
- *l'attribution dynamique des adresses de couche 3;*
- *le multiplexage des protocoles réseau (possibilité de faire passer plusieurs paquets de protocoles différents sur la même connexion);*
- *la configuration des liaisons et la vérification de leur qualité;*
- *la détection des erreurs;*
- *la négociation d'options (adresses de couche 3, compression, etc.)*

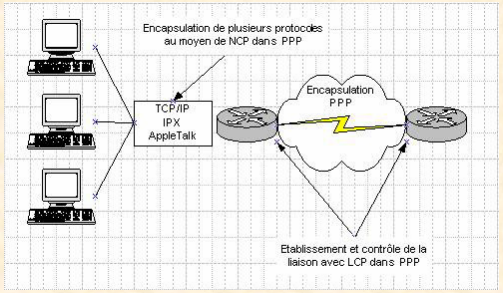
Les protocoles PPP

*- **PPP** utilise son composant **NCP** (Network Control Program/ Programme de contrôle de réseau) pour encapsuler plusieurs protocoles. Cet emploi de NCP dépasse les limites du prédécesseur de PPP, SLIP, qui ne pouvait permettre que le transport de paquets IP.*

*- **NCP** permet :*

- l'échange et l'attribution des adresses;

- le choix d'un système de compression des en-têtes IP



*- **PPP** utilise le protocole **LCP** (Link Control Protocol) pour négocier et mettre en place les options de contrôle sur le lien WAN.*

*- **LCP** permet aux extrémités de se mettre d'accord sur:*

- la taille maximale des trames;

- l'echappement de certains caractères du style XON/XOFF;

- l'authentification de bas niveau;

- la detection d'une boucle

- le contrôle de qualité;

- la compression des paquets

*- Le protocole **HDLC** (High-level Data Link Control) est le protocole par défaut pour l'encapsulation du point-à-point. C'est un protocole de liaison synchrone orienté bit.*

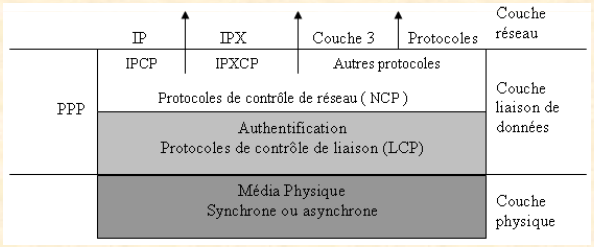
Composants de PPP en couches

PPP utilise une architecture en couches

Avec ses fonctions les plus basses, PPP peut employer :

-- Un média physique synchrone comme ceux qui connectent RNIS,

-- Un média physique asynchrone comme ceux qui utilisent les services téléphoniques de base pour les connexions par modems commutés.



Options de configuration de PPP LCP

Le RFC 1548 décrit l'exploitation de PPP et des options de configuration de LCP. Il a été mis à jour par le RFC 1570 " PPP LCP Extensions ".

Les routeurs Cisco qui utilisent l'encapsulation PPP, incluent les options LCP du tableau suivant :

Fonction	***Mode opératoire***	***Protocole***
Authentification	*Nécessite un mot de passe* *Effectue la négociation par tests*	*PAP* *CHAP*
Compression	*Compresse les données sur la source; reproduit les données sur la destination*	*Stacker ou Predictor*
Détection d'erreur	*- Surveille les données supprimées sur la liaison* *- Evite le bouclage de trame*	*Quality* *Magic Number*
Multilink	*Equilibrage de charge sur plusieurs Liaisons*	*MultiLink Protocole (MP)*

*Les options **d'authentification** nécessitent que le côté appelant de la liaison spécifie des informations qui permettent de vérifier que l'appelant a la permission de l'administrateur d'établir la connexion. Les routeurs homologues échangent des messages d'authentification.*

---

*Les options **de compression** augmentent le débit effectif sur les connexions PPP en réduisant la quantité de données dans la trame qui doivent transiter sur la liaison.*

Le protocole décompresse la trame sur sa destination.

Les deux protocoles de compression disponibles sur les routeurs Cisco sont Stacker et Predictor.

*Les mécanismes **de détection d'erreurs** avec PPP permettent à un processus d'identifier les conditions de faute.*

Les solutions Quality et Magic Number apportent une aide au maintien d'une liaison de données exempte de boucles.

---

*Depuis la version 11.1 de Cisco IOS, **Multilink PPP** est supporté. Cette solution apporte l'équilibrage de charge sur les interfaces du routeur que PPP utilise.*

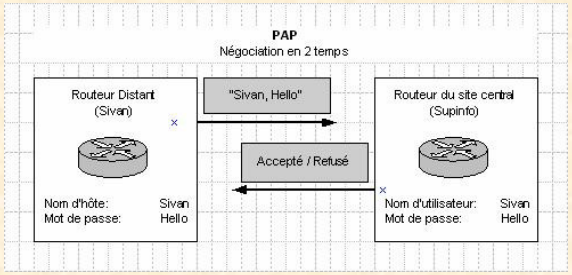
La fragmentation et le séquencement de paquets, comme spécifié dans le RFC 1717, scindent la charge de PPP et envoient des fragments sur des circuits parallèles. Dans certains cas, ce « faisceau » de tubes Multilink PPP fonctionne comme une seule liaison logique, améliorant le débit et réduisant la latence entre routeur homologues.

Le RFC 1990 , " The PPP Multilink Protocol (MP) " rend obsolète le RFC 1717

L'authentification PPP

Lors de la configuration de l'authentification PPP, vous pouvez choisir entre les protocoles PAP ou CHAP. En général, ce dernier est le protocole préféré.

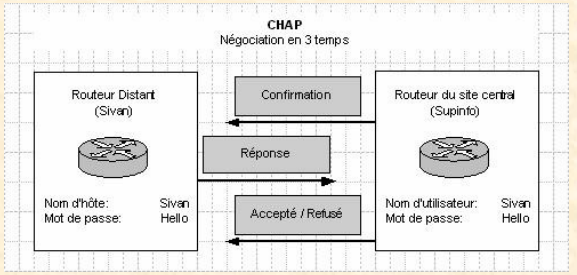
***PAP** (Password Authentication Protocol) fournit une méthode simple pour qu'un nœud distant puisse décliner son identité au moyen d'une négociation en deux temps. L'authentification n'est réalisée qu'au moment de l'établissement de la liaison initiale.* **(RFC 1334 et le RFC 1994)**



Après que la phase d'établissement de liaison PPP a été accompli, un ensemble nom d'utilisateur / mot de passe est envoyé de façon répétée pour le nœud distant vers le routeur jusqu'à ce que l'authentification soit acquittée ou que la connexion soit terminée.

***- CHAP** (Challenge Handshake Authentication Protocol) est le protocole le plus utilisé,*

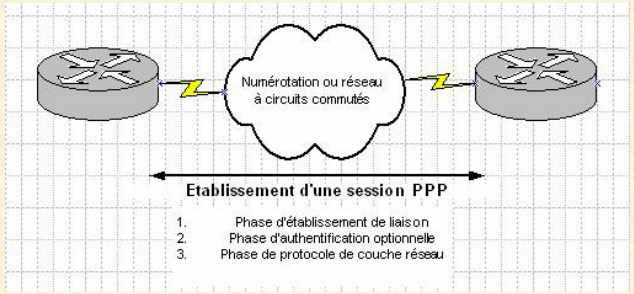
- il est utilisé au démarrage d'une liaison et périodiquement pour vérifier l'identité d'un nœud distant au moyen d'une négociation en trois temps. **(RFC 1994)**



Après l'établissement de la liaison PPP, le routeur local envoie un message de test vers le nœud distant. Celui-ci répond avec un numéro d'identifiant crypté, un mot de passe secret et un nombre aléatoire. Le routeur local compare la valeur de réponse avec le résultat de ses propres calculs. Si les valeurs correspondent, l'authentification est acquittée; autrement, la connexion est immédiatement terminée.

Etablir une liaison PPP

L'établissement d'une session PPP fait intervenir trois phases :



Phase d'établissement de la ligne

- chaque équipement PPP envoie des paquets LCP pour configurer et tester la liaison de données.

- les paquets LCP contiennent des champs d'option de configuration qui permettent aux équipements de négocier l'utilisation d'options telles que l'unité maximale de réception, la compression de certains champs PPP et le protocole d'authentification de liaison.

- si une option de configuration n'est pas incluse dans un paquet LCP, la valeur par défaut pour cette option sera utilisée.

Phase d'authentification

- après que la liaison a été établie et que le protocole d'authentification a été choisi, le routeur homologue peut être authentifié.

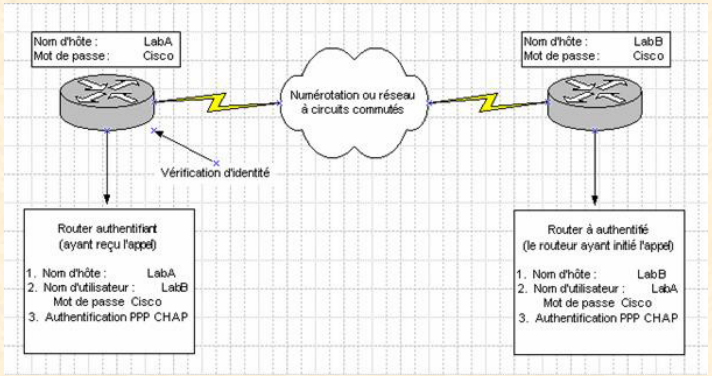
- l'authentification, si elle est utilisée, a lieu avant d'entrer dans la phase de protocole de la couche réseau.

Phase du protocole de la couche réseau

- les équipements PPP envoient des paquets NCP pour choisir et configurer un ou plusieurs protocoles de la couche réseau (tels que IP)

- après que chacun des protocoles choisis a été configuré, des datagrammes de chaque protocole peuvent être envoyés sur la liaison. PPP supporte plusieurs protocoles dont IP, IPX, AppleTalk, etc.

Configuration de PPP sur un routeur Cisco



Les routeurs de chaque côté de la liaison doivent être configurés pour l'authentification PPP.

Pour configurer l'authentification PPP, il faut procéder comme suit :

1. *Sur chaque routeur, il faut définir le nom d'utilisateur et le mot de pass attendus de la part du routeur distant. Voici la syntaxe de la commande :*

Router(config)# ***username*** *nom* ***password*** *secret*

Les paramètres de la commande sont les suivants :

- Nom : c'est le nom d'hôte du routeur distant,

- Secret : Sur les routeur Cisco, le mot de passe secret doit être le même pour les deux routeur

2. *Il faut ensuite entrer en mode de configuration d'interface pour l'interface appropriée.*

3. *Il faut ensuite configurer l'interface pour l'encapsulation PPP.*

Router (config)# encapsulation PPP

4. *Puis configurer l'authentification PPP.*

Router (config)# PPP authentication {CHAP | CHAP PAP | PAP CHAP }

Il existe quatre options disponibles pour l'authentification PPP :

Si PAP et CHAP sont tous les deux activés, la première méthode spécifiée sera demandée durant la négociation de liaison. Si l'homologue suggère l'emploi de la deuxième méthode ou refuse simplement la première, la deuxième méthode sera utilisée.

VERIFICATION PPP

Lorsque PPP est configuré, vous pouvez vérifier ses états LCP et NCP au moyen de la commande ***show interfaces***

Configuration HDLC

Conf term

Int serial0

Encapsulation HDLC

Vérification de l'encapsulatrion PPP et HDLC

Debug ppp authentication