جامعة مولاي إسماعيل
UNIVERSITÉ MOULAY ISMAÏL

كلية العلوم والتقنيات
FACULTÉ DES SCIENCES ET TECHNIQUES

Les Réseaux WAN

« Protocole PPP »

Réaliser et Présenter par :

- OUAZIZ Noureddine
- BELBEIDA Houssam
- SAIDI Med Anass
- OUBRA Ismail
- SAKTIWY Hamza
- TERMASS Bouchra
- HATIM Hafida
- OUKOURANE Karima
- DAMMOU Manal

Encadré par:

Mr. AIT KHOUYA Youssef

Plan :

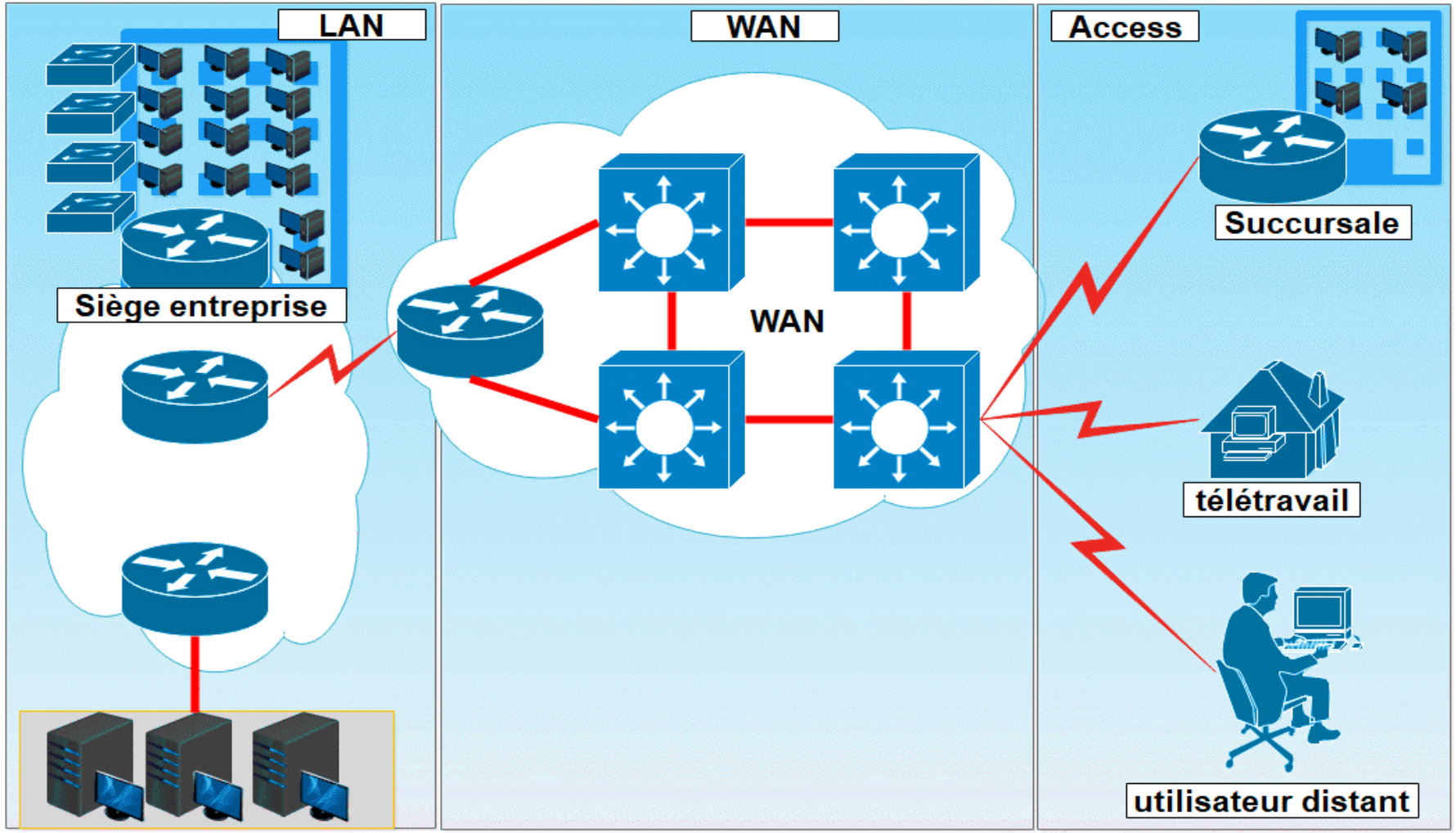
- Introduction
  - **Présentation des Réseaux WAN**
- Présentation de la connexion point à point
  - **Introduction**
  - **HDLC**
  - **Protocole PPP**
- Fonctionnement du protocole PPP
  - **LCP (Link Control Protocol)**
  - **NCP (Network Control Protocol)**
- Configuration du protocole PPP
  - **Configuration de PAP**
  - **Configuration de CHAP**
  - **Configuration de PAP et CHAP**
- Dépannage de la connectivité WAN
- Travail pratique
- Conclusion

Introduction
Présentation des Réseaux WAN

Introduction: C'est quoi un réseau WAN ?

- Un réseau étendu ou WAN (Wide Area Network) est un réseau de télécommunications géographiquement dispersé. Le terme permet de faire la distinction entre une structure de télécommunications élargie et un réseau local ou LAN (Local Area Network)
- Et aussi c'est eux qui relient les différentes entreprises, ou bien les utilisateurs particuliers.
- Aujourd'hui, Internet est le réseau étendu le plus connu dans le monde.
- Dans un WAN on peut y voir circuler différents types de trafic :
  - **comme de la voix**
  - **des données**
  - **et de la vidéo**

Introduction: Exemple



Présentation de la connexion point à point

HDLC

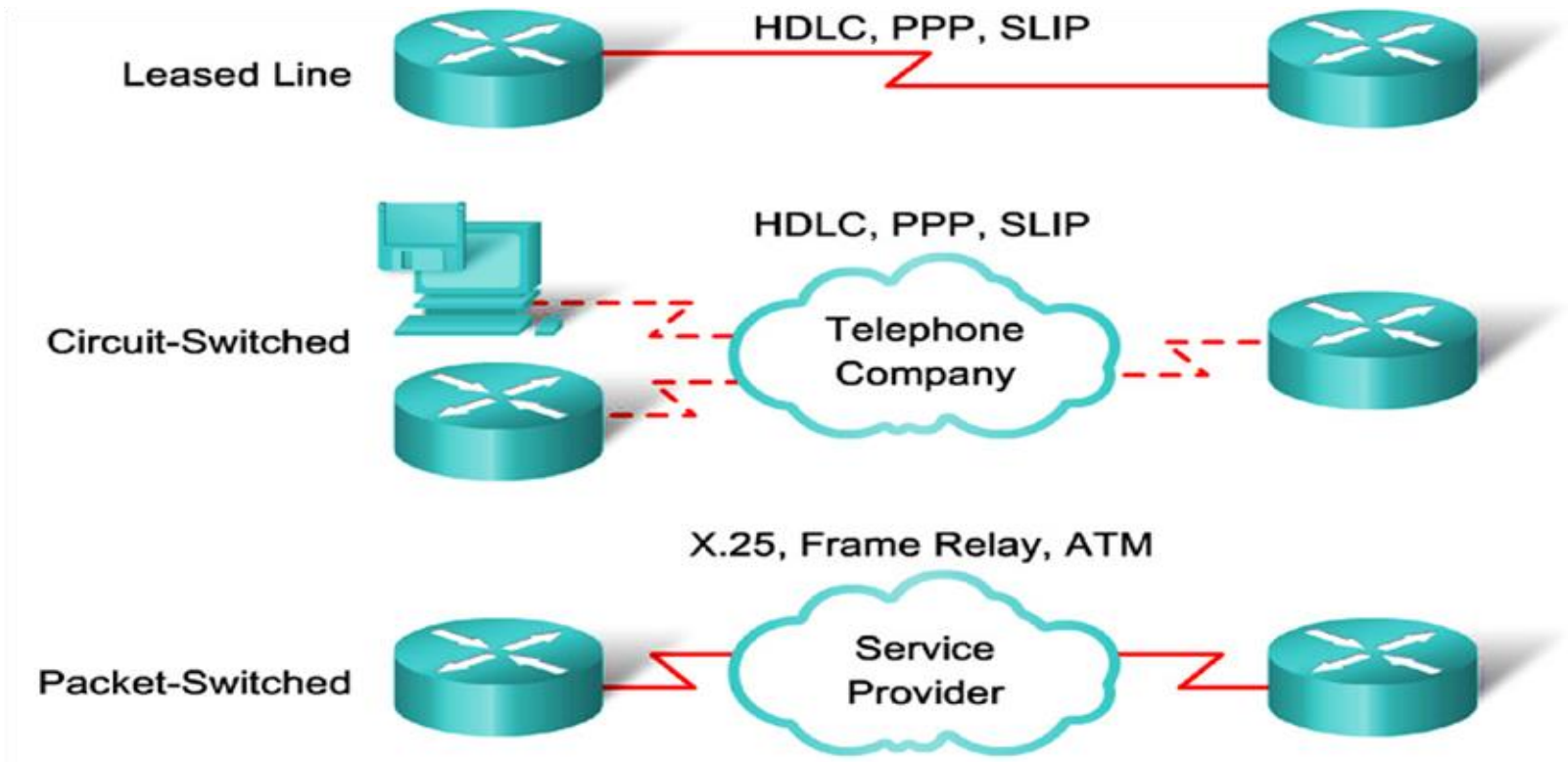
Protocole PPP

Présentation de la connexion point à point

- Les Liaisons WAN utilisent surtout les couches 1 et 2 du modelé OSI (la couche **physique** et la couche **Liaison de données**) .
- Les Protocoles de la couche physique décrivent comment fournir les connexions électriques, mécaniques, opérationnelles et fonctionnelles aux services fournis par un FAI (Orange, IAM ..)
- Les Protocoles de la couche liaison de données définissent la manière dont les donnés sont encapsulées en vue de leur transmissions vers des sites distants

Liaison	Protocoles
Séries	**C.HDLC, PPP, LAPB**
A commutation de paquet	**X25, Frame Relay**
A commutation de circuit	**RNIS**

Présentation de la connexion point a point



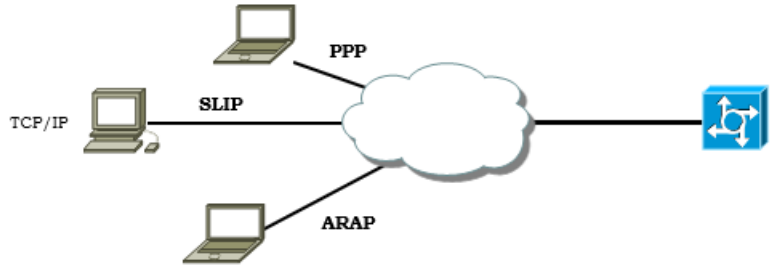
Liaisons Point à Point

Aujourd'hui il y a deux protocoles de couches liaison pour encapsuler TCP/IP :

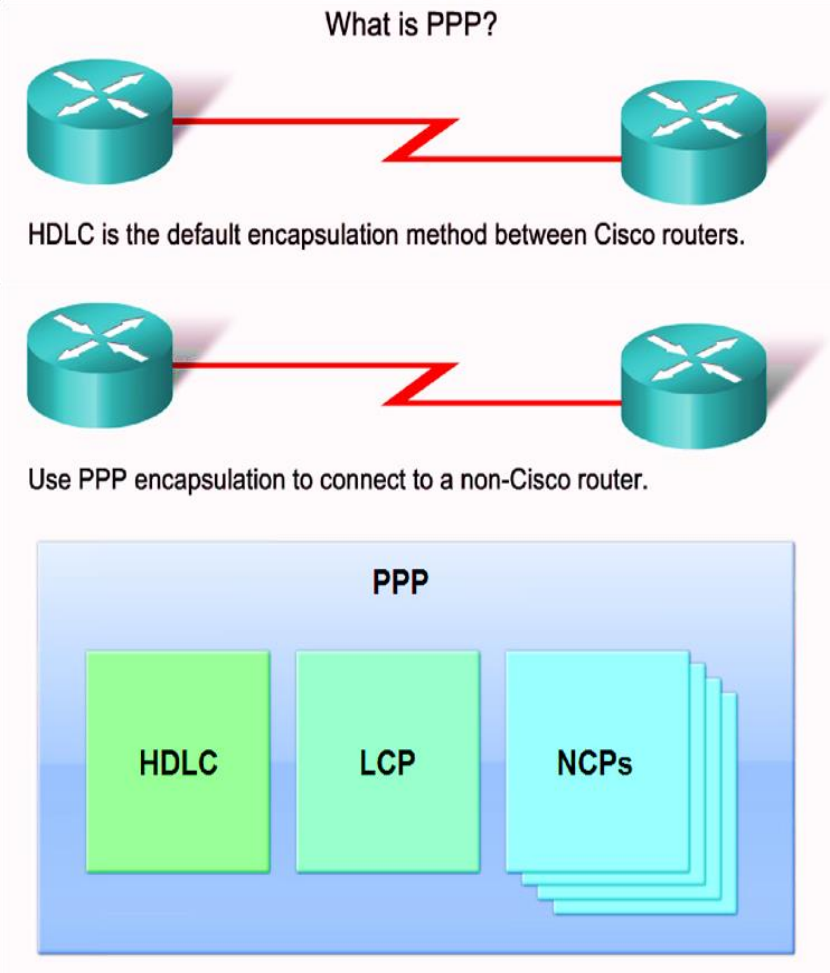
- **SLIP** : Serial Line Internet Protocol est un protocole standard pour les connexions point à point série utilisant TCP/IP
  - Prédécesseur de PPP
  - Encapsulation par défaut sur une interface asynchrone

- **PPP** : PPP fournit des connexions de routeur à routeur, de host à un réseau pour des circuits asynchrones et synchrones.
  - Liaisons appel par appel ou lignes louées
  - PPP peut être utilisé pour des protocoles de couche réseau comme IPX et AppleTalk

Liaisons Point à Point



- PPP peut supporter également les fonctionnalités suivantes :
  - Allocation dynamique d'adresse
  - Authentification PAP
  - Authentification CHAP
- SLIP ne supporte pas ces fonctionnalités
- SLIP est très rarement implémentés dans la conception de réseaux



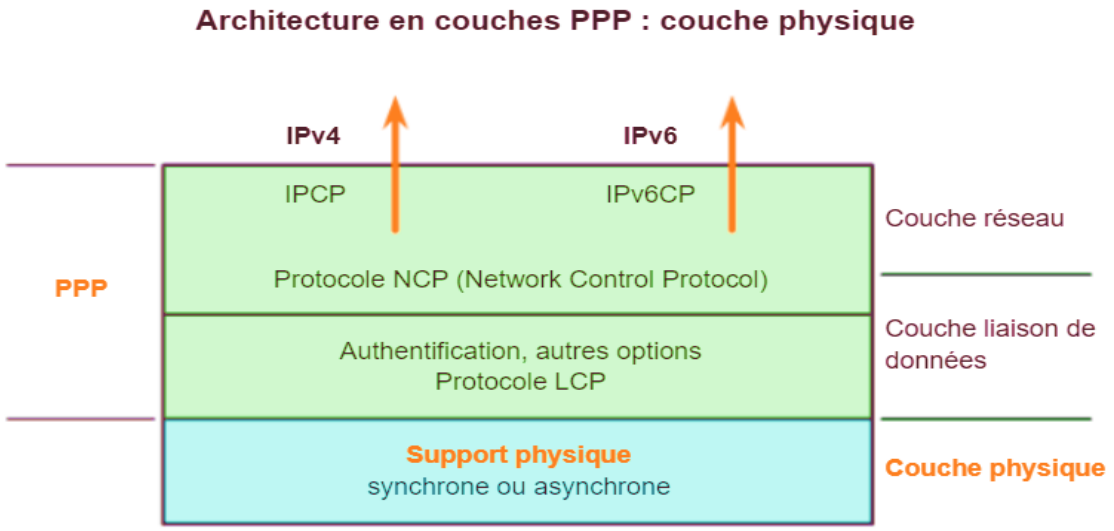
HDLC et PPP

Trame ISO HDLC					
Flag	Adresse	Contrôle	Données	FCS	Flag
1 Octet	1 Octet	1 ou 2 Octets	1 à 1500 Octets	2 (ou 4) Octets	1 Octet

Trame PPP						
Flag	Adresse	Contrôle	Protocole	Données	FCS	Flag
1 Octet	1 Octet	1 Octet	1 ou 2 Octets	1 à 1500 Octets	2 (ou 4) Octets	1 Octet

- HDLC (High Level Data Link Control) est l'encapsulation par défaut pour des interfaces série et RNIS sur un routeur Cisco
- Le HDLC Cisco n'est pas compatible avec le HDLC ISO
- PPP est le protocole choisi pour la configuration de lignes série dans un environnement multi-constructeurs
- PPP utilise HDLC comme base de l'encapsulation
- PPP offre des extensions par rapport à HDLC

Architecture PPP



- PPP est basé sur des standards ouverts toujours compatibles
- La trame PPP est basée sur la trame HDLC avec un format fixé par l'ISO
- Contrairement à HDLC, la trame PPP définit un champ protocole
- PPP peut négocier des options de liaison dynamiquement et peut supporter de multiples protocoles de couche 3 tels IP, IPX et AppleTalk.

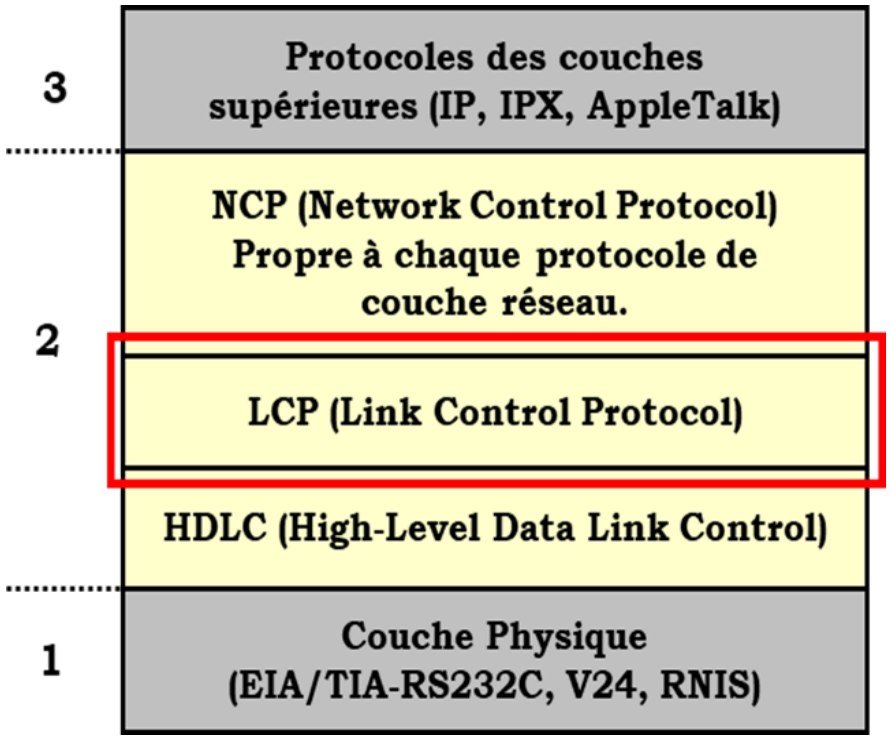
Fonctionnement du protocole PPP

LCP (Link Control Protocol)

NCP (Network Control Protocol)

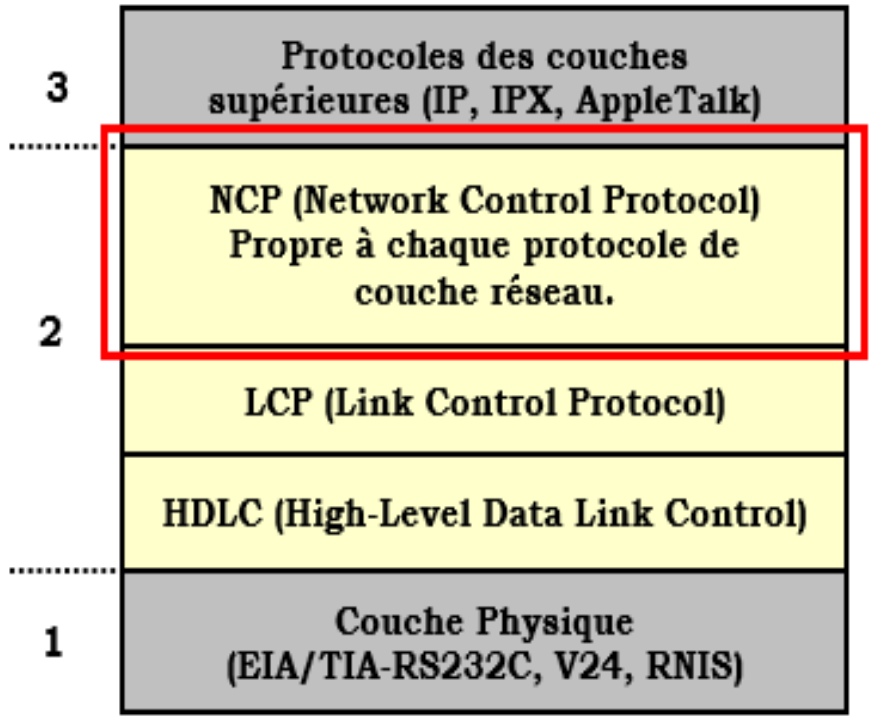
Architecture PPP : LCP

- PPP définit un LCP ou Link Control Protocol
- Le rôle de LCP est d'établir de configurer et de tester la couche liaison de données
- Quand les hosts négocient une connexion PPP, ils échangent des paquets LCP
- Le champ protocole permet d'identifier tous les protocoles utilisés sur la liaison
- Les paquets des différents protocoles permettent de négocier dynamiquement les options de liaison :
  - Authentification
  - Callback
  - Compression
  - Multilink PPP



Architecture PPP : NCP

- PPP définit un NCP ou Network Control Protocol
- Quand LCP a établi une connexion de couche 2, le NCP est activé
- Les extrémités de liaison échangent des paquets NCP pour établir et configurer des protocoles de couche réseau tels IP, IPX ou AppleTalk.
- Chaque couche 3 a son propre NCP
- Le NCP peut multiplexer plusieurs sessions de couche 3 sur un seule liaison de données
- Quand un host libère une connexion, le NCP libère la session couche 3 et le LCP libère la couche 2



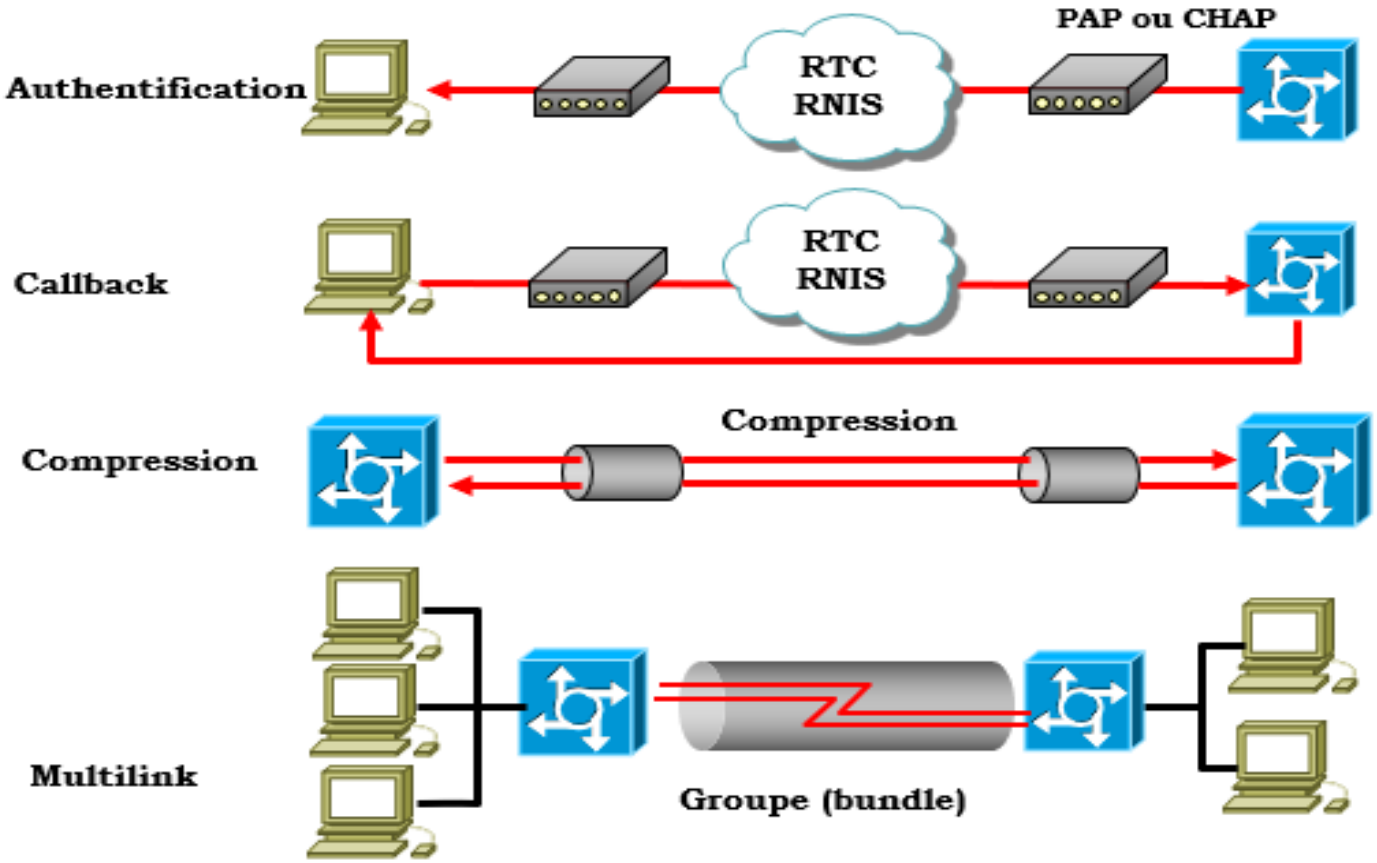
Configuration de PPP

Configuration de PPP

Dans la section précédente, des options de protocole LCP configurables ont été ajoutées pour répondre à des besoins de connexion WAN spécifiques. Le protocole PPP peut comprendre les options LCP suivantes :

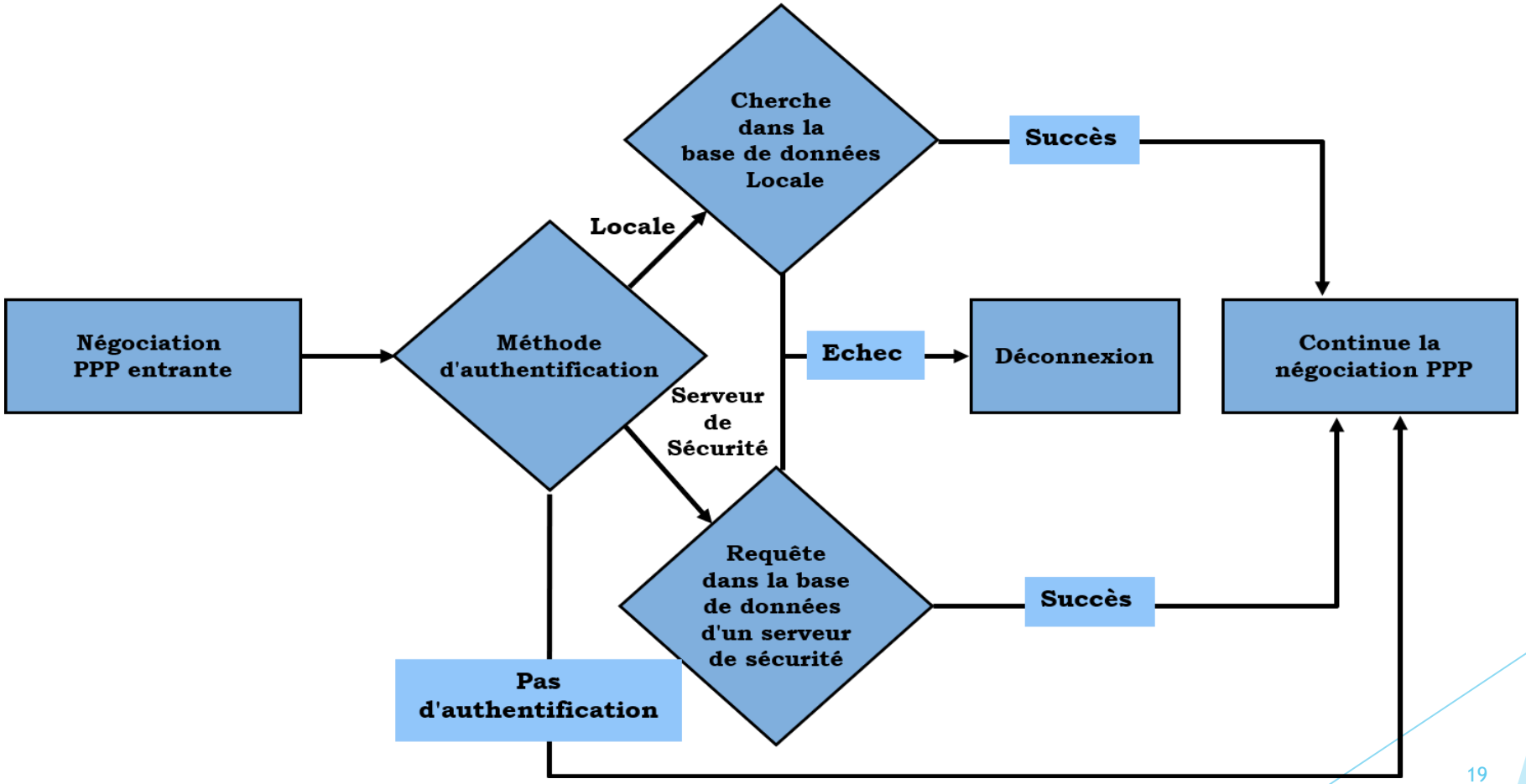
- **Authentification**: les routeurs homologues échangent des messages d'authentification. Pour l'authentification, les deux choix sont le protocole d'authentification du mot de passe (PAP: Password Authentication Protocol) et le protocole d'authentification à échanges confirmés (CHAP: Challenge Handshake 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.
- **Détection des erreurs**: identifie les défaillances
- **Rappel PPP** : le rappel PPP permet d'augmenter le niveau de sécurité
- **Multiliaison**: offre un équilibrage de la charge sur les interfaces de routeur utilisées par PPP

Configuration de PPP : Option LCP



Configuration de PPP : Option LCP

- Processus d'authentification :



Configuration de PPP

- **Activation de PPP sur une interface:**

Pour définir PPP comme méthode d'encapsulation utilisée par l'interface série, utilisez la commande de configuration d'interface encapsulation ppp.

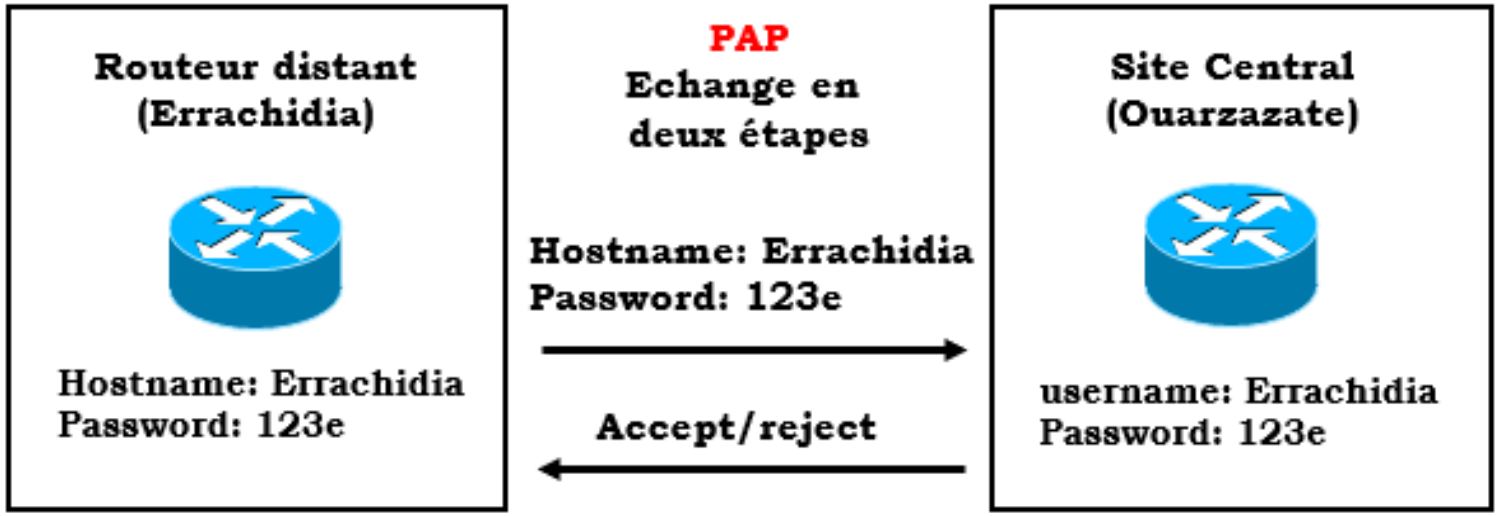
L'exemple suivant active l'encapsulation PPP sur l'interface série 0/0/0 :

```
R3# configure terminal

R3(config)# interface serial 0/0/0

R3(config-if)# encapsulation ppp
```

- La commande d'interface encapsulation ppp n'a pas d'arguments. Souvenez-vous que si le protocole PPP n'est pas configuré sur un routeur Cisco, l'encapsulation par défaut pour les interfaces série est **HDLC**.

Authentification PAP

- **PAP** : (Password Authentication Protocol) est un protocole réseau bidirectionnel ayant lieu en deux étapes et qui n'utilise pas le chiffrement : les noms d'utilisateur et mot de passe sont envoyés en Clair dans le réseau.
- S'ils sont acceptés, la connexion est autorisée. l'authentification sera effectuée en une seule fois. Le nom d'hote d'un routeur doit correspondre au nom d'utilisateur configuré sur l'autre routeur.



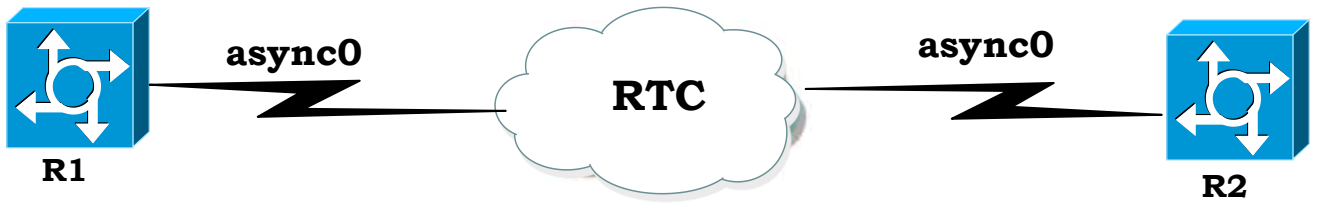
Configuration de PPP : PAP

- PAP fournit une méthode simple d'établissement d'identité pour un nœud distant en utilisant un échange en deux étapes.
- Après que la phase d'établissement de la liaison PPP soit terminée, une paire "**username/password"** est transmise de manière répétitive par un nœud distant jusqu'à ce qu'un acquittement d'authentification soit reçu ou que la connexion soit libérée.
- PAP n'est pas un protocole d'authentification très évolué.
- Les mots de passe sont transmis en clair sur la liaison ainsi il n'y a aucune protection contre les attaques.

Configuration de PAP

```
Router#configure terminal
Router(config)#hostname R1
R1(config)#username R2 password cisco2
R1(config)#interface serial 0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1
password cisco1
```

```
Router#configure terminal
Router(config)#hostname R2
R2(config)#username R1 password cisco1
R2(config)#interface serial 0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R2
password cisco2
```



Configuration de PPP : PAP

```
R1(config)#username R2 password cisco2
```

- Ceci doit correspondre à ppp pap sent-username sur le host distant.

```
R1(config-if)#ppp pap sent-username R1 password cisco1
```

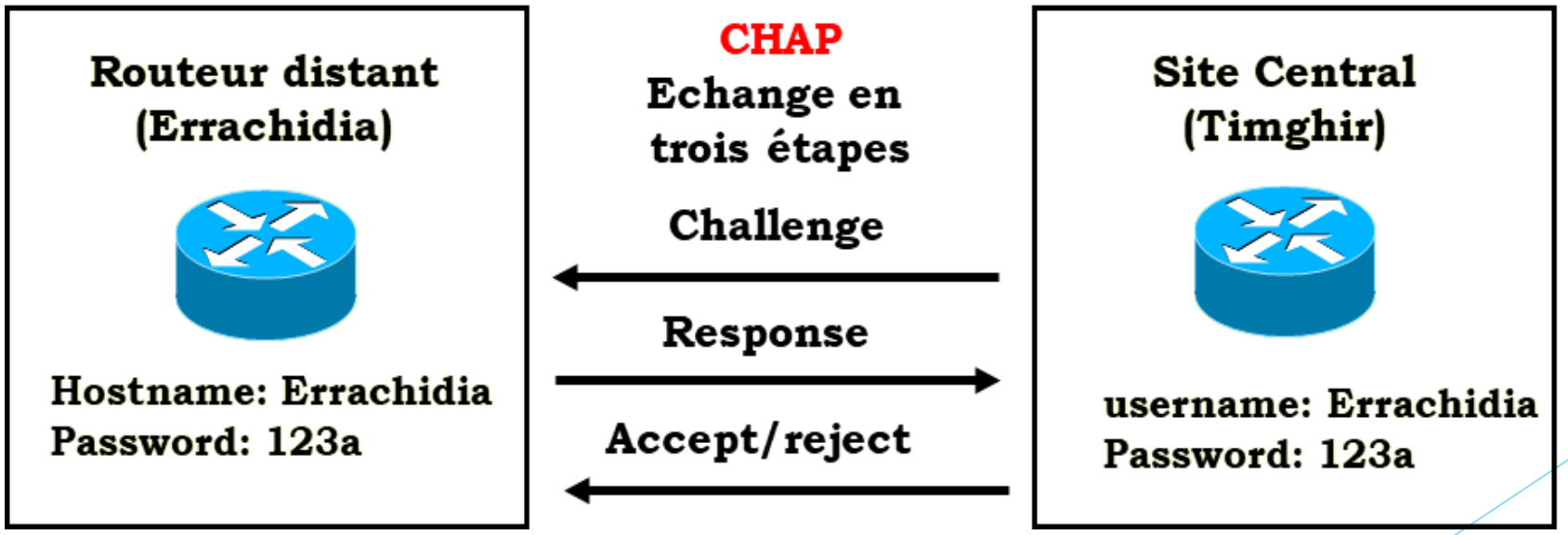
- Les mots de passe du host local et du distant n'ont pas besoin d'être identiques
- Ils ne doivent pas être identiques au mot de passe enable-secret

Configuration de PPP : PAP

- **sent-username** et **password** doivent correspondre aux **username** et **password** distants.
- Les mots de passe sont sensibles à la casse pas les "**hostname**".
- Le nom inclus dans les commandes **username** et **dialer map** sont sensibles à la casse.
- Si le nom du host distant est R1 et que le username est crée avec r1, l'authentification échouera.

Authentification CHAP

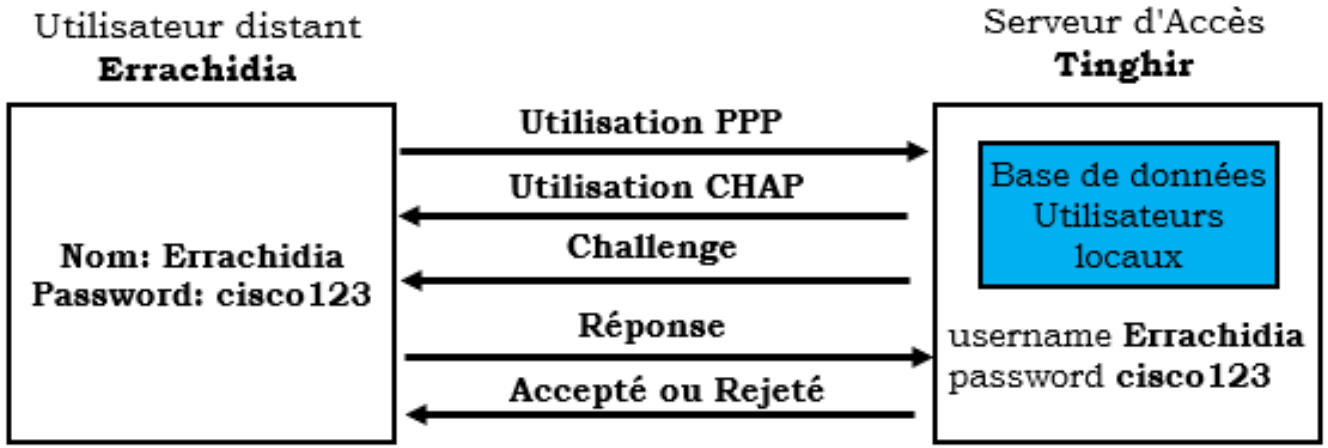
- **CHAP** : (Challenge Handshake Authentication Protocol) le protocole CHAP effectue des vérifications régulières pendant l'existence de Ia liaison. Le routeur R1 souhaite établir une connexion CHAP avec le routeur R2. Une fois l'établissement de Ia liaison terminée, un échange en trois étapes aura lieu.



Configuration PPP : CHAP

- CHAP est utilisé pour l'authentification à la connexion et vérifie périodiquement l'identité du nœud distant en utilisant une échange en trois étapes.
- Après que la phase d'établissement de la liaison PPP soit terminée, le routeur local transmet un message "challenge" au nœud distant.
- Cette réponse est basée sur le mot de passe et le message "challenge".
- CHAP fournit une protection contre les attaques de réutilisation de mot de passe en utilisant un message challenge variable, unique est non prédictible.
- Le routeur local ou serveur d'authentification tierce partie contrôle la fréquence et le timing des challenges.

Configuration PPP : CHAP



- Les serveurs d'accès configurés avec CHAP contrôlent les tentatives de login
- Le serveur doit transmettre un paquet challenge
- Le mot de passe secret n'est jamais transmis en clair
- Le protocole CHAP permet également aux serveurs de demander aux hosts distants de se réauthentifier à tout moment

Configuration de CHAP

```
Router#configure terminal
Router(config)#hostname R1
R1(config)#username R2 password cisco1
R1(config)#interface serial 0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
```

```
Router#configure terminal
Router(config)#hostname R2
R2(config)#username R1 password cisco1
R2(config)#interface serial 0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
```

- Notes:
  - Les "hostname" sont utilisés sauf si la commande ppp chap hostname a été exécutée. Ils doivent correspondre aux "username" des routeurs distants (non sensibles à la casse).
  - Les mots de passe doivent être identiques.

Configuration de CHAP

```
Router(config-if)#ppp chap hostname name
Router(config-if)#ppp chap password password
```

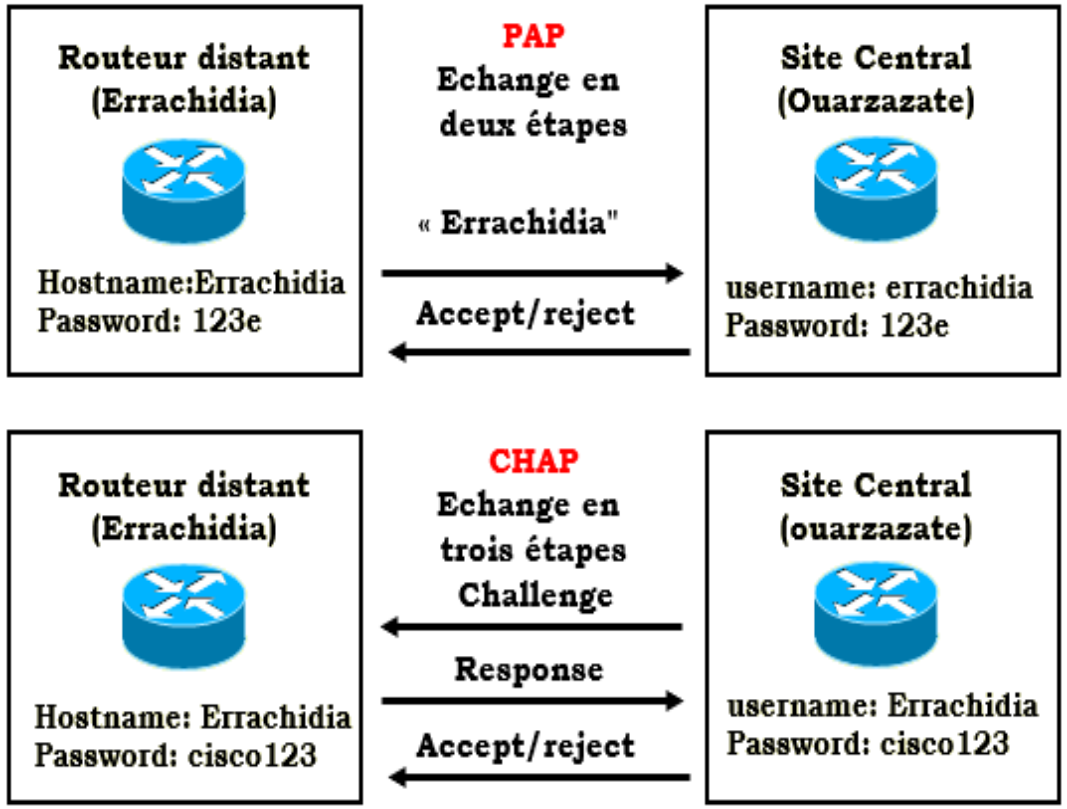
- **ppp chap hostname** *name*

  Cette commande définit un nom de host CHAP propre à l'interface.

- **ppp chap password** *password*

  Cette commande définit un mot de passe CHAP propre à l'interface.

Protocoles d'authentification de PPP



- Mot de passe transmis en clair
- Le site distant contrôle les tentatives d'accès.
- Mot de passe crypté
- Répétition de la demande d'authentification

Configuration de CHAP et PAP

```
Router(config-if)#ppp authentication pap chap
```

Ou

```
Router(config-if)# ppp authentication chap pap
```

- Les authentifications PAP et CHAP peuvent être validées sur une interface.
- La première méthode spécifiée est celle requise pendant la négociation de liaison.
- Si le distant suggère d'utiliser la seconde méthode ou simplement refuse la première méthode alors la seconde méthode sera essayée.
- Cette commande est très utile car certains équipements acceptent PAP uniquement et d'autres CHAP uniquement.

Dépannage de la connectivité WAN

Vérification de la Configuration PPP

- **Show dialer**

```
Lyon#show dialer
BRI0/0:1 - dialer type - ISDN
Idle timer (60 secs), fast idle timer (20 secs)
Wait for carrier (30 secs), re-enable (15 secs)
Dialer state is multilink member
Dial reason: ip (s=192.168.1.2, d=192.168.0.1)
Connected to 0556123456 (Bordeaux)

BRI0/0:2 - dialer type - ISDN
Idle timer (60 secs), fast idle timer (20 secs)
Wait for carrier (30 secs), re-enable (15 secs)
Dialer state is multilink member
Dial reason: Multilink bundle overload
Connected to 0556123456 (Bordeaux)
```

- Si la sortie de la commande show dialer affiche le nom du routeur distant c'est que l'authentification a réussi.
- **Remarque** : la commande show dialer fonctionne mieux à partir de Trois routeurs ou plus .

Vérification de la Configuration PPP

Debug PPP negotiation:

- La commande debug ppp negotiation est un excellent outil pour résoudre les problèmes d'authentification, de compression et de Multilink PPP.
  Quand l'état LCP est "OPEN", la négociation NCP débute.

- Les négociations suivantes peuvent être observées:
  - Authentification CHAP
  - Compression Control Protocol (CCP)
  - Protocoles NCP: IPCP, IPXCP ..

```
Lyon#debug ppp negotiation
BR0:1 PPP: Treating connection as a callin
BR0:1 PPP: Phase is ESTABLISHING, passive Open
BR0:1 LCP: State is Listen
BR0:1 LCP: I CONFREQ (Listen) id 116 len 30
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
BR0:1 LCP:    MagicNumber 0x1109DB3A (0x05061109DB3A)
BR0:1 LCP:    MRRU (1524) (0x110405F4)
BR0:1 LCP:    EndpointDisc 1 Local (0x130B0143656E7472616C42)
BR0:1 LCP: O CONFREQ (Listen) id 68 len 15
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
BR0:1 LCP:    MagicNumber 0x156A31E0 (0x0506156A31E0)
BR0:1 LCP: O CONFREJ (Listen) id 116 len 19
BR0:1 LCP:    MRRU 1524(0x110405F4)
BR0:1 LCP:    EndpointDisc 1 Local (0x130B0143656E7472616C42)
```

Vérification de la Configuration PPP

debug ppp authentication

Affichage	Description
Se0/0 PPP: Phase is AUTHENTICATION, by both	Authentification bidirectionnelle
Se0/0 PAP: O AUTH-REQ id 4 len 18 from "Rg1"	Requête d'authentification sortante
Se0/0 PAP: I AUTH-REQ id 1 len 18 from "Rg2"	Requête d'authentification entrante
Se0/0 PAP: Authenticating peer Rg1	Authentification entrante
Se0/0 PAP: O AUTH-ACK id 1 len 5	Acquittement transmis
Se0/0 PAP: I AUTH-ACK id 4 len 5	Acquittement reçu

- La commande debug ppp authentication affiche la séquence des messages échangés pour l'authentification.

Vérification de la Configuration PPP

- On peut utiliser la commande debug ppp lorsque on recherche des éléments suivants :
  - Les boucles dans un interréseau PPP
  - Les nœuds qui négocient correctement les connexions PPP
  - Les erreurs sur la connexion PPP
  - Les causes d'échec de la session PAP ou CHAP

- La commande debug ppp authentication peut être utilisée pour résoudre des problèmes d'authentification avec CHAP ou PAP

- La commande debug ppp authentication donne la même sortie que la commande debug ppp négociation mais cette sortie est limitée aux évènements d'authentification CHAP et PAP

Conclusion

- Le protocole PPP synchrone est utilisé pour:
  - la connexion aux périphériques non-Cisco
  - surveiller la qualité de la liaison
  - fournir l'authentification
  - regrouper les liaisons pour une utilisation partagée
- PPP utilise HDLC pour l'encapsulation de datagrammes

Conclusion

- LCP est le protocole PPP utilisé pour établir, configurer, tester la connexion de liaison de données et y mettre fin.
- LCP peut aussi authentifier un homologue à l'aide du protocole PAP ou CHAP.
- Un ensemble de NCP est utilisé par le protocole PPP pour prendre en charge plusieurs protocoles de couche réseau en même temps.
- Le protocole PPP multiliaison répartit le trafic sur des liaisons groupées en découpant les paquets en morceaux, et en envoyant ces morceaux simultanément sur plusieurs liaisons à la même adresse distante, où ils sont réassemblés

Merci pour votre Attention