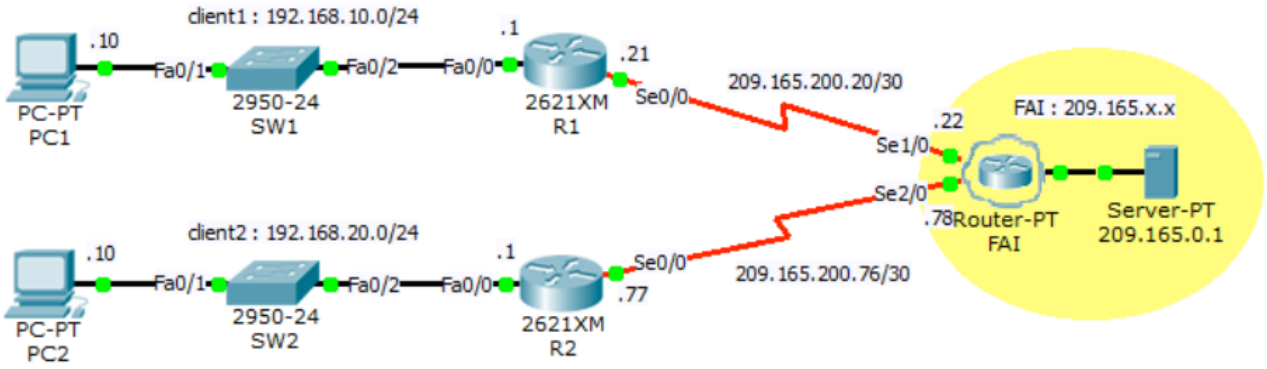

- TP 4 -
Protocole de couche liaison PPP (partie 2)

par Édouard Lumet

Sommaire

2. Configuration du réseau et de la traduction d'adresse

Une fois la maquette réalisée, on configure les adresses sur les deux PCs, le serveur web ainsi que les 3 routeurs selon le plan indiqué sur la maquette. À noter que les liaisons série sont de type DCE/DTE où le routeur FAI est le DCE. On configure l'horloge à 64000 par exemple sur ce dernier. On définit ensuite sur les deux routeurs R1 et R2 une route statique par défaut en ne précisant que l'interface de sortie Se0/0.

Le PAT se configure ainsi sur les deux routeurs clients :

```
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#ip nat inside source list 1 interface se0/0 overload
R1(config)#int fa0/0
R1(config-if)#ip nat inside
R1(config-if)#int se0/0
R1(config-if)#ip nat outside

R2(config)#access-list 1 permit 192.168.20.0 0.0.0.255
R2(config)#ip nat inside source list 1 interface se0/0 overload
R1(config)#int fa0/0
R1(config-if)#ip nat inside
R1(config-if)#int se0/0
R1(config-if)#ip nat outside
```

On définit via une ACL qui peut accéder à la fonction NAT. On indique que l'on fait du PAT (overload) sur l'interface se0/0. Enfin, on indique que fa0/0 connecte le réseau interne et que se0/0 connecte le réseau externe.

Le serveur web du FAI est accessible depuis les deux PCs car le protocole d'encapsulation utilisé est le même entre R1 et FAI et entre R2 et FAI. Ici, c'est HDLC. S'il y avait eu une encapsulation PPP sur FAI par exemple, le conflit de protocole n'aurait pas permis de communication. (**show interfaces se0/0**)

3. Encapsulation HDLC et PPP sur des liaisons série point à point

Normalement, le ping doit être possible entre PC1 ou R1 vers FAI ou le serveur Web. De même pour la connexion Web. En revanche, entre PC2 et le serveur Web, aucune connexion n'est possible. Par défaut, avec les routeurs et les noms d'interface de la maquette de l'énoncé, l'encapsulation en place sur R1 et sur FAI est la même : PPP. En revanche, sur R2 c'est HDLC qui est en place donc il y a un conflit d'encapsulation. L'interface de R2 connectant FAI doit être « up » mais le protocole doit être « down ». De même sur l'interface de FAI connectant R2.

Dans le cas présent, HDLC est le protocole utilisé sur toutes les interfaces connectant nos trois routeurs. Étant la même encapsulation, il n'y a pas de conflit compatibilité pour la transmission de données.

Sur une liaison série, les bits sont transmis les uns à la suite des autres. Les données doivent par conséquent être encadrées pour savoir quand elles commencent et quand elles finissent. L'encapsulation permet donc de spécifier à l'aide de flags où débute la trame et où elle se termine. Cela permet aussi d'ajouter des bits de redondance pour contrôler les erreurs dans les données. C'est donc un « outil » de synchronisation entre les deux équipements.

HDLC et PPP sont respectivement des protocoles décrits par des standards ISO et IETF (RFCs). Cependant un dérivé de HDLC, cHDLC, est propre à Cisco et il est maintenant largement ouvert et répandu. Parmi ces deux protocoles, seul PPP supporte l'authentification via PAP ou CHAP. PAP est une authentification simple par mot de passe, comme lorsque l'on se connecte au compte de son site préféré par exemple. CHAP quant à lui est basé sur l'échange d'un secret commun « hashé ».

Par défaut, c'est le protocole HDLC qui est utilisé sur les routeurs Cisco. Pour les liaisons séries dédiées longue distance, on utilise plutôt PPP car il offre des services tels que la gestion de congestion, la reprise sur erreur, la compression de données ainsi que l'agrégation de liens.

4. Configuration de l'encapsulation PPP

Sur chaque routeur, on configure alors PPP sur les interfaces séries connectées. On active également le débuggage de la négociation du protocole pour visualiser les étapes de la connexion PPP (sans authentification dans un premier temps).

```
R2#debug ppp negotiation
PPP protocol negotiation debugging is on
R2#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up

Serial0/0 PPP: Using default call direction
Serial0/0 PPP: Treating connection as a dedicated line
Serial0/0 PPP: Phase is ESTABLISHING, Active Open

Serial0/0 LCP: State is Open

R2#
Serial0/0 PPP: Phase is FORWARDING, Attempting Forward
Serial0/0 Phase is ESTABLISHING, Finish LCP
Serial0/0 Phase is UP

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed
state to up
```

Établissement d'une connexion PPP

Lorsque l'on branche le câble série, on peut voir que PPP prend en compte la connexion comme une liaison série dédiée. Ensuite, c'est LCP (Link Control Protocol) qui configure et négocie les paramètres. Une fois fait (« Finish LCP »), le protocole est « up » sur l'interface connectée.

On remarque notamment 3 phases qui sont : 'establishing', 'forwarding' et 'up'.

Le serveur web est toujours joignable depuis PC1 et PC2.

5. Configuration de l'authentification PAP

On peut également activer le débuggage de l'authentification PPP pour voir ce qu'il se passe lors de la connexion avec PAP. Le principe est de créer un compte utilisateur sur le routeur FAI pour le client 1. Les identifiants lui seront communiqués, c'est avec ceux-ci qu'il pourra s'authentifier lors de la connexion. On active alors l'authentification PPP sur l'interface série connectant le client 1. Sur ce dernier, on indique sur l'interface connectant le FAI que l'on utilise l'authentification PAP de PPP avec le login/mdp fournit par le FAI. On peut aussi créer un login/mdp sur le routeur du client pour que le FAI s'y authentifie également. Cela permet d'empêcher un autre FAI ou tout autre tiers de s'y connecter et s'assurer que l'on est bien connecté à notre FAI.

```
R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up

Serial0/0 PPP: Using default call direction
Serial0/0 PPP: Treating connection as a dedicated line
Serial0/0 PPP: Phase is ESTABLISHING, Active Open

Serial0/0 LCP: State is Open

Serial0/0 PPP: Phase is AUTHENTICATING

Serial0/0 Using hostname from interface PAP

Serial0/0 Using password from interface PAP

Serial0/0 PAP: O AUTH-REQ id 17 len 15

Serial0/0 PAP: Phase is FORWARDING, Attempting Forward

R1(config-if)#
Serial0/0 PPP: Phase is FORWARDING, Attempting Forward
Serial0/0 Phase is ESTABLISHING, Finish LCP
Serial0/0 Phase is UP

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed
state to up
```

Le débuggage nous montre qu'il y a une étape supplémentaire pour la connexion PPP : 'authenticating'. On peut voir que c'est bien PAP qui est la méthode utilisée et que les identifiants sont échangés.

Le protocole finit par changer pour l'état « up » sur l'interface connectant le FAI.

6. Configuration de l'authentification CHAP

Le principe de l'authentification CHAP ici est de créer un identifiant sur le routeur FAI et sur le routeur client. Ce couple login/mdp doit être le même sur les deux routeurs car il sera hashé puis envoyer réciproquement afin de les comparer. C'est le « secret » commun. Si l'on créer un identifiant sur FAI uniquement, le protocole de ligne reste « down » sur l'interface connectant le client. De même si l'on crée un identifiant différent sur le routeur client. En revanche, lorsque l'on crée sur les deux routeurs le même couple login/mdp (FAI/cisco par exemple) le protocole de ligne passe à l'état « up ».

Il n'y a donc pas besoin de préciser quels identifiants envoyer à l'autre routeur mais seulement d'activer l'authentification CHAP sur l'interface désirée et de créer un identifiant dont le login doit être le nom du routeur (FAI ici). Le mot de passe n'est donc pas transmis, c'est un hash qui est transmis. Il doit donc être le même car en théorie il n'existe qu'un résultat unique en sortie de la fonction de hashage (MD5 par exemple).

```
R2#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up

Serial0/0 PPP: Using default call direction
Serial0/0 PPP: Treating connection as a dedicated line
Serial0/0 PPP: Phase is ESTABLISHING, Active Open

Serial0/0 LCP: State is Open

Serial0/0 PPP: Phase is AUTHENTICATING

Serial0/0 IPCP: O CONFREQ [Closed] id 1 len 10

Serial0/0 IPCP: I CONFACK [Closed] id 1 len 10

Serial0/0 IPCP: O CONFREQ [Closed] id 1 len 10

Serial0/0 IPCP: I CONFACK [REQsent] id 1 len 10

R2#
Serial0/0 IPCP: I CONFREQ [Closed] id 1 len 10

Serial0/0 IPCP: O CONFACK [Closed] id 1 len 10

Serial0/0 IPCP: I CONFREQ [REQsent] id 1 len 10

Serial0/0 IPCP: O CONFACK [REQsent] id 1 len 10

Serial0/0 PPP: Phase is FORWARDING, Attempting Forward
Serial0/0 Phase is ESTABLISHING, Finish LCP
Serial0/0 Phase is UP

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed
state to up
```

Étapes se déroulant lors de la connexion PPP avec authentification CHAP