

Protocole PPP : configurations routeur d'accès (Hub) & routeur d'agence (Spoke)

Philippe Latu

philippe.latu(at)linux-france.org

<http://www.linux-france.org/prj/inetdoc/>

Historique des versions		
\$Revision: 1619 \$	\$Date: 2011-04-05 00:08:00 +0200 (mar. 05 avril 2011) \$	\$Author: latu \$
Année universitaire 2010-2011		
Résumé		
<p>L'objectif de ce support de travaux pratiques est d'étudier les configurations d'un routeur d'accès (Hub) et d'un routeur d'agence (Spoke). On assimile ces deux configurations types à des routeurs qui réalisent l'interconnexion entre un réseau local et un réseau étendu. Le routeur d'agence assure l'interconnexion entre un réseau local comprend les serveurs et les postes de travail et un réseau étendu qui correspond à la liaison vers le fournisseur d'accès Internet. À l'autre extrémité, le routeur d'accès assure l'interconnexion entre le réseau étendu et le réseau local qui correspond au réseau d'agrégation de l'opérateur. La technologie RNIS sert de support au réseau étendu. C'est le moyen d'illustrer une communication à base de trames HDLC et le fonctionnement du protocole PPP.</p>		

Table des matières

1. Copyright et Licence	2
1.1. Méta-information	2
1.2. Conventions typographiques	2
2. Aide à la mise au point	3
3. Connexion avec le protocole PPP	3
3.1. Configuration de l'interface RNIS pour le protocole PPP	3
3.2. Connexion avec le protocole PPP en mode client sans authentification	4
3.3. Connexion avec le protocole PPP en mode client avec authentification CHAP	4
3.4. Connexion avec le protocole PPP en mode client avec authentification PAP	5
4. Système routeur d'accès (<i>Hub</i>)	6
4.1. Établissement de la route par défaut	6
4.2. Connexion au réseau local	6
4.3. Connexion au réseau étendu	7
4.4. Configuration du routeur d'accès (<i>Hub</i>)	7
4.5. Authentification PPP	7
5. Système Routeur d'agence (<i>Spoke</i>)	8
5.1. Connexion au réseau local	8
5.2. Connexion au réseau étendu	8
5.3. Configuration du routeur d'agence (<i>Spoke</i>)	9
5.4. Authentification PPP	9
6. Documents de référence	10

1. Copyright et Licence

Copyright (c) 2000,2011 Philippe Latu.
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Copyright (c) 2000,2011 Philippe Latu.
Permission est accordée de copier, distribuer et/ou modifier ce document selon les termes de la Licence de Documentation Libre GNU (GNU Free Documentation License), version 1.2 ou toute version ultérieure publiée par la Free Software Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture, et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est incluse dans la section intitulée « Licence de Documentation Libre GNU ».

1.1. Méta-information

Cet article est écrit avec *DocBook*¹ XML sur un système *Debian GNU/Linux*². Il est disponible en version imprimable aux formats PDF et Postscript : [interco.ppp.tp.pdf](#)³ | [interco.ppp.tp.ps.gz](#)⁴.

Toutes les commandes utilisées dans ce document ne sont pas spécifiques à une version particulière des systèmes UNIX ou GNU/Linux. C'est la distribution *Debian GNU/Linux* qui est utilisée pour les tests présentés. Voici une liste des paquets contenant les commandes :

- net-tools - The NET-3 networking toolkit
- ifupdown - High level tools to configure network interfaces
- iputils-ping - Tools to test the reachability of network hosts
- isdnutils - Most important ISDN-related packages and utilities
- ipppd - PPP daemon for syncPPP over ISDN

1.2. Conventions typographiques

Tous les exemples d'exécution des commandes sont précédés d'une invite utilisateur ou *prompt* spécifique au niveau des droits utilisateurs nécessaires sur le système.

- Toute commande précédée de l'invite \$ ne nécessite aucun privilège particulier et peut être utilisée au niveau utilisateur simple.
- Toute commande précédée de l'invite # nécessite les privilèges du super-utilisateur.

¹ <http://www.docbook.org>

² <http://www.debian.org>

³ <http://www.linux-france.org/prj/inetdoc/telechargement/interco.ppp.tp.pdf>

⁴ <http://www.linux-france.org/prj/inetdoc/telechargement/interco.ppp.tp.ps.gz>

2. Aide à la mise au point

Afin de résoudre les éventuels problèmes de connexion et de configuration, il existe différents niveaux d'informations systèmes. Voici la liste des trois niveaux principaux d'émission de messages :

Messages système émis par le noyau Linux

L'affichage des messages système est géré par le démon `syslogd`. Pour consulter ces messages, il faut ouvrir un des fichiers du répertoire `/var/log/`. Dans le cas des travaux pratiques, l'ensemble des informations nécessaires à la mise au point des connexions réseau se trouve dans le fichier `/var/log/syslog`. Pour visualiser les dernières lignes du fichier à la console on utilise la commande **tail** : `tail -50 /var/log/syslog`.

Messages système émis par le sous-système RNIS

Les messages du sous-système RNIS sont transmis vers les interfaces `/dev/isdnctrl*`. On peut les consulter à l'aide de la commande : `cat /dev/isdnctrl` ou les renvoyer automatiquement sur une console : `cat /dev/isdnctrl10 >/dev/tty10 &`. Les différents niveaux d'informations produits sont paramétrés à l'aide de l'utilitaire de contrôle du pilote d'interface RNIS : **hisaxctrl**. Ces niveaux sont détaillés dans les pages de manuels : `man hisaxctrl`. En ce qui concerne l'établissement des connexions téléphoniques, des codes sont renvoyés directement à la console en cas d'échec. Leur signification est donnée dans les pages de manuels `isdn_cause` : `man isdn_cause`.

Messages émis par le gestionnaire de connexion **ippdd**

Ces messages sont obtenus en configurant le démon de journalisation système `syslogd`. Les détails sur la configuration de ce démon sont obtenus à l'aide des pages de manuels : `man syslog.conf`. Vérifier que la ligne suivante est bien présente dans le fichier `/etc/syslog.conf` :

```
daemon.* /var/log/daemon.log
```

3. Connexion avec le protocole PPP

La connexion directe à l'aide du mode `rawip` présente l'avantage de la simplicité : authentification basée sur les numéros de téléphone et pas d'échange d'adresses IP. Ce mode de connexion présente cependant deux limitations importantes :

- La configuration des adresses IP doit être effectuée avant l'établissement de la connexion téléphonique. Il est donc impératif que les postes soient en état de marche au moment de la connexion.
- La sécurité de connexion étant basée sur les numéros de téléphone, il est impossible de se connecter depuis une autre installation.

Le protocole PPP permet de dépasser ces limitations en offrant une configuration indépendante de la technologie du réseau étendu après authentification et autorise une plus grande mobilité.

Les mécanismes de fonctionnement de ce protocole sont décrits dans le document [RFC1661 The Point-to-Point Protocol \(PPP\)](#)⁵. Dans le contexte de ces travaux pratiques, il doit remplir trois fonctions pour les deux configurations types étudiées :

- La possibilité de se connecter au serveur d'appel depuis n'importe quel poste ou numéro de téléphone.
- L'authentification de l'utilisateur appelant.
- L'attribution de l'adresse IP du poste appelant.

3.1. Configuration de l'interface RNIS pour le protocole PPP

Relativement à la configuration `rawip`, il faut changer quelques paramètres de configuration au niveau liaison de l'interface RNIS.

1. Quelle est l'encapsulation à configurer sur l'interface RNIS pour utiliser le protocole PPP ?

Consulter les pages de manuels de la commande **isdnctrl** en effectuant une recherche avec la clé : `ppp`.

⁵ <http://www.faqs.org/rfcs/rfc1661.html>

2. Quel est le démon de gestion de connexion qui utilise le mode de transmission synchrone des interfaces RNIS avec le protocole PPP ?

Lister les paquets liés au sous-système (RNIS|ISDN) et retrouver le gestionnaire de connexion associé.

3. Quelles sont les noms d'interface RNIS à utiliser avec ce démon de gestion de connexion ?

Voir le support *L'architecture du sous-système RNIS Linux*⁶ et les pages de manuels de l'outil de configuration d'interface `isdnctrl`.

3.2. Connexion avec le protocole PPP en mode client sans authentification

Pour valider le fonctionnement de l'interface RNIS avec le protocole PPP, on utilise les postes de travaux pratiques par paires. Dans ce contexte, les deux modes : client et serveur ne se distinguent que par l'attribution d'adresses IP. C'est le serveur qui doit fournir les adresses données dans le tableau ci-dessous.

Tableau 1. Plan d'adressage IP et RNIS des liaisons WAN

bus	Poste serveur	n° tél.	adresses IP serveur:client	n° tél.	Poste client
S0.1	alderaan	104	192.168.101.1:192.168.101.2	105	bespin
S0.2	centares	106	192.168.102.1:192.168.102.2	107	coruscant
S0.3	dagobah	108	192.168.103.1:192.168.103.2	109	endor
S0.4	felucia	110	192.168.104.1:192.168.104.2	111	geonosis
S0.5	hoth	112	192.168.105.1:192.168.105.2	113	mustafar
S0.6	naboo	114	192.168.106.1:192.168.106.2	115	tatooine



Saisie des options PPP

Pour l'ensemble de ces travaux pratiques, les options du gestionnaire de connexion PPP `ipppd` doivent être saisies directement sur la ligne de commande. Il faut s'assurer que les fichiers `/etc/ppp/options*` sont vides. Dans le cas contraire, les paramètres contenus dans ces fichiers peuvent être utilisés par défaut sans tenir compte de ceux saisis sur la ligne de commande.

1. Quelles sont les options de configuration à fournir au gestionnaire de connexion pour ce mode de fonctionnement ?

Consulter les pages de manuels du démon `ipppd`.

2. Quelles sont les options qui permettent de visualiser en détails le dialogue PPP dans les journaux systèmes ?

C'est à nouveau dans les pages de manuels que les réponses se trouvent.

3. Quels sont les noms des deux sous-couches du protocole PPP qui apparaissent dans les journaux systèmes ? Quels sont les rôles de ces deux sous-couches ?

4. Quels sont les en-têtes du dialogue de la couche LCP qui identifient les requêtes (émises|reçues), les rejets et les acquittements ?

3.3. Connexion avec le protocole PPP en mode client avec authentification CHAP

Comme dans le cas précédent, les postes de travaux pratiques sont configurés par paires en mode routeur d'agence (*Spoke*) et routeur d'accès (*Hub*|FAI|ISP). On ajoute ici le volet authentification au dialogue PPP en utilisant le protocole CHAP.

⁶ <http://www.linux-france.org/prj/inetdoc/guides/rnis/part2.chapter1.arch.html>

Pour l'ensemble des postes de travaux pratiques les paramètres d'authentification *login/password* sont : *etu/stri*.

Tableau 2. Plan d'adressage IP et RNIS des liaisons WAN

bus	Poste serveur	n° tél.	adresses IP serveur:client	n° tél.	Poste client
S0.1	alderaan	104	192.168.1.1:192.168.1.2	105	bespin
S0.2	centares	106	192.168.2.1:192.168.2.2	107	coruscant
S0.3	dagobah	108	192.168.3.1:192.168.3.2	109	endor
S0.4	felucia	110	192.168.4.1:192.168.4.2	111	geonosis
S0.5	hoth	112	192.168.5.1:192.168.5.2	113	mustafar
S0.6	naboo	114	192.168.6.1:192.168.6.2	115	tatooine



Journalisation des échanges de mots de passe

Il existe une option spécifique du gestionnaire de connexion PPP *ipppd* qui permet de journaliser les échanges sur les mots de passe : *+pwlog*. En ajoutant cette option à celles déjà utilisées lors de l'appel à *ipppd* sur la ligne de commande, on peut observer l'état des transactions d'authentification.

1. Quelles sont les options de configuration spécifiques à l'authentification CHAP à fournir au gestionnaire de connexion pour ce mode de fonctionnement ?
Consulter les pages de manuels du démon **ipppd** à la recherche du mot clé *chap*.
2. Dans quel fichier sont stockés les paramètres d'authentification *login/password* utilisés par le protocole CHAP ?
Consulter les pages de manuels du démon **ipppd** à la recherche du mot clé *chap*.
3. Quels sont les en-têtes du dialogue de la couche LCP qui identifient les requêtes d'authentification échangées entre les deux processus pairs ?
4. Quelles sont les informations échangées sur les mots de passe avec le protocole CHAP ? Est-il possible de relever le mot de passe avec ce protocole ?

3.4. Connexion avec le protocole PPP en mode client avec authentification PAP

On reprend exactement le cas précédent en changeant le protocole d'authentification. On utilise maintenant le protocole PAP qui est nettement moins intéressant que CHAP. Nous allons voir pourquoi !

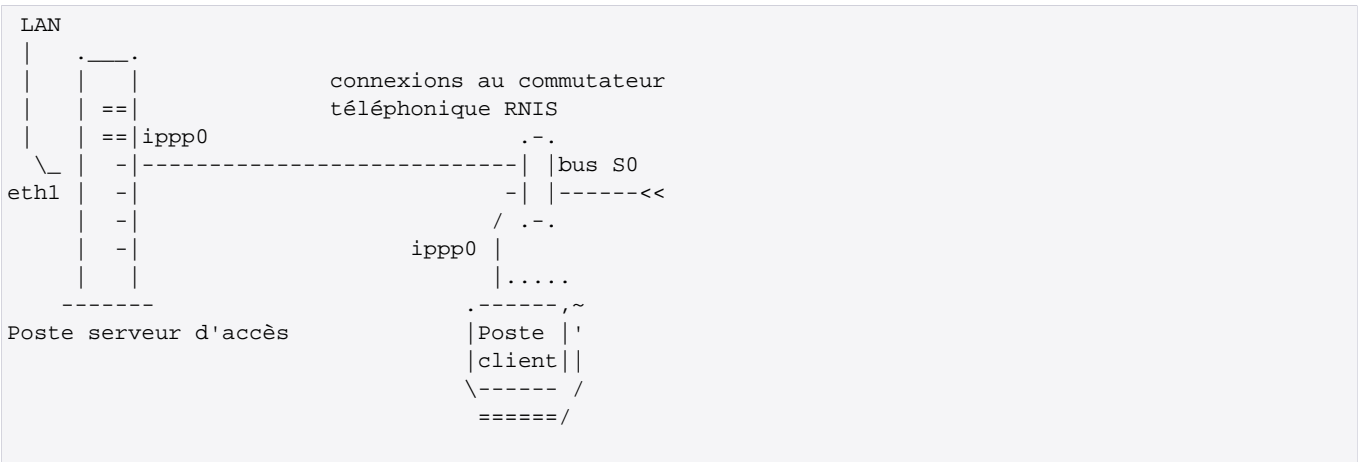
Les paramètres d'authentification *login/password* ne changent pas : *etu/stri*.

Le plan d'adressage téléphonique et IP ne change pas non plus.

1. Quelles sont les options de configuration spécifiques à l'authentification PAP à fournir au gestionnaire de connexion pour ce mode de fonctionnement ?
Consulter les pages de manuels du démon **ipppd** à la recherche du mot clé *pap*.
2. Dans quel fichier sont stockés les paramètres d'authentification *login/password* utilisés par le protocole PAP ?
Consulter les pages de manuels du démon **ipppd** à la recherche du mot clé *pap*.
3. Quels sont les en-têtes du dialogue de la couche LCP qui identifient les requêtes d'authentification échangées entre les deux processus pairs ?
4. Quelles sont les informations échangées sur les mots de passe avec le protocole PAP ? Est-il possible de relever le mot de passe avec ce protocole ?

4. Système routeur d'accès (*Hub*)

Dans ce scénario, le routeur dispose d'un accès haut débit avec son interface Ethernet et doit fournir un accès à Internet par son interface WAN ou RNIS. On modélise ainsi le fonctionnement des équipements utilisés par les fournisseurs d'accès Internet (FAI/ISP). En plus de la dénomination *Network Access Sever*, on utilise aussi l'appellation *Dialin Server*.



Le plan d'adressage donné ci-dessous a pour but de fixer les numéros de téléphone pour éviter les «croisements» des connexions lors de la mise au point sur les paires de postes routeurs d'agence & routeurs d'accès.

Tableau 3. Plan d'adressage IP et RNIS des liaisons WAN

Poste routeur d'accès (<i>Hub</i>)	bus	N° tél.	Adresses IP serveur:client	N° tél.	Poste routeur d'agence (<i>Spoke</i>)
alderaan	S0.1	104	192.168.104.1:192.168.104.2	105	bespin
centares	S0.2	106	192.168.106.1:192.168.106.2	107	coruscant
dagobah	S0.3	108	192.168.108.1:192.168.108.2	109	endor
felucia	S0.4	110	192.168.110.1:192.168.110.2	111	geonosis
hoth	S0.5	112	192.168.112.1:192.168.112.2	113	mustafar
naboo	S0.6	114	192.168.114.1:192.168.114.2	115	tatooine

4.1. Établissement de la route par défaut

La configuration par défaut des paquets *pppd* suppose que le poste utilisé est un client pour lequel la route par défaut doit être établie à chaque nouvelle connexion PPP.

Dans le cas présent, le routeur d'accès (*Hub*) doit conserver sa route par défaut sur le réseau local indépendamment des demandes de connexion PPP. Il est donc nécessaire de modifier le script de connexion `/etc/ppp/ip-up.d/00-ipppd`. Voici un extrait avec les lignes à commenter :

```
PPP_NET=`echo $PPP_LOCAL | sed 's,\.[0-9]*\.[0-9]*$, .0.0/16, '`

case "$PPP_IFACE" in
  ipp0) route del default ❶
        # route add default netmask 0 $PPP_IFACE # usually necessary
        route add default netmask 0 gw $PPP_REMOTE ❷
        # The next lines are for simple firewalling.
```

- ❶ Commenter cette ligne pour éviter l'effacement de la route par défaut.
- ❷ Commenter cette ligne pour éviter l'établissement d'une nouvelle route par défaut.

4.2. Connexion au réseau local

1. Quelles sont les opérations nécessaires à la configuration de l'interface Ethernet ?

Reprendre les questions du support *Configuration d'une interface RNIS en mode rawip*⁷.

2. Quels sont les tests à réaliser pour s'assurer du fonctionnement de l'accès Internet ?

Reprendre la séquence «rituelle» des tests ICMP avec la commande **ping** et les adresses : boucle locale (*loopback*), interface locale, passerelle par défaut et une adresse réseau située sur un autre réseau. Ce n'est qu'en dernier lieu que l'on doit effectuer un test avec le service de noms de domaines à l'aide des commandes **host** ou **dig**. Enfin, si le protocole ICMP n'est pas disponible au delà du réseau local, il faut utiliser la commande **tcptraceroute** pour tester la connectivité inter réseau.

4.3. Connexion au réseau étendu

1. Quelles sont les opérations nécessaires à la configuration de l'interface RNIS en serveur d'appels ?

Reprendre les questions ci-avant : **Section 3, « Connexion avec le protocole PPP »**.

2. Donner la liste des options de la commande **isdnctrl** pour la configuration serveur d'appels ?

Rechercher dans les documents les éléments associés à l'option `diain`.

3. Quels sont les fichiers nécessaires à l'utilisation du démon `ippdpd` en serveur d'appels ?

Utiliser les pages de manuels du démon `ippdpd`.

4. Quelle est l'option de la commande **isdnctrl** qui permet de sauvegarder/restituer la configuration de l'interface (RNIS|ISDN) ?

Utiliser les pages de manuel de l'outil **isdnctrl**. Sauvegarder le fichier de configuration de l'interface pour les utilisations ultérieures.

4.4. Configuration du routeur d'accès (*Hub*)

1. Quelle est la fonction réseau du noyau LINUX qui permet d'activer le routage des paquets entre les interfaces du système ?

Consulter le support *Fonctions réseau du noyau Linux*⁸.

2. Quelle est la fonction de filtrage utilisée pour gérer l'espace d'adressage tout en contrôlant les accès ?

Consulter le support *Fonctions réseau du noyau Linux*⁹.

3. Donner la liste des options de la commande **iptables** pour activer les fonctions de traduction d'adresses et de suivi de communication pour le routeur d'accès ?

À partir du support *Fonctions réseau du noyau Linux*¹⁰ et des exemples donnés dans le guide *guide NAT-HOWTO*¹¹, établir une configuration simple de traduction d'adresse. Attention à adopter une syntaxe indépendante de l'adressage IP pour pouvoir changer de numérotation réseau à volonté.

4. Quels sont les tests à réaliser pour s'assurer du fonctionnement du routeur d'accès Internet ?

Reprendre la séquence «rituelle» des tests ICMP en direction du poste client et de l'Internet. Visualiser aussi l'utilisation des règles de filtrage avec l'outil **iptables**.

4.5. Authentification PPP

1. Quelles sont les options de configuration du démon `ippdpd` qui permettent d'activer l'authentification du routeur d'agence ?

⁷ <http://www.linux-france.org/prj/inetdoc/cours/interco.rawip.tp/>

⁸ <http://www.linux-france.org/prj/inetdoc/cours/interco.noyau/>

⁹ <http://www.linux-france.org/prj/inetdoc/cours/interco.noyau/>

¹⁰ <http://www.linux-france.org/prj/inetdoc/cours/interco.noyau/>

¹¹ <http://www.linux-france.org/prj/inetdoc/guides/NAT-HOWTO/NAT-HOWTO-4.html#ss4.1>

Consulter les pages de manuel du démon `ipppd` ainsi que le guide *Linux PPP HOWTO*¹²

2. Quelles sont les informations contenues dans les messages système qui permettent de valider la connexion téléphonique ?

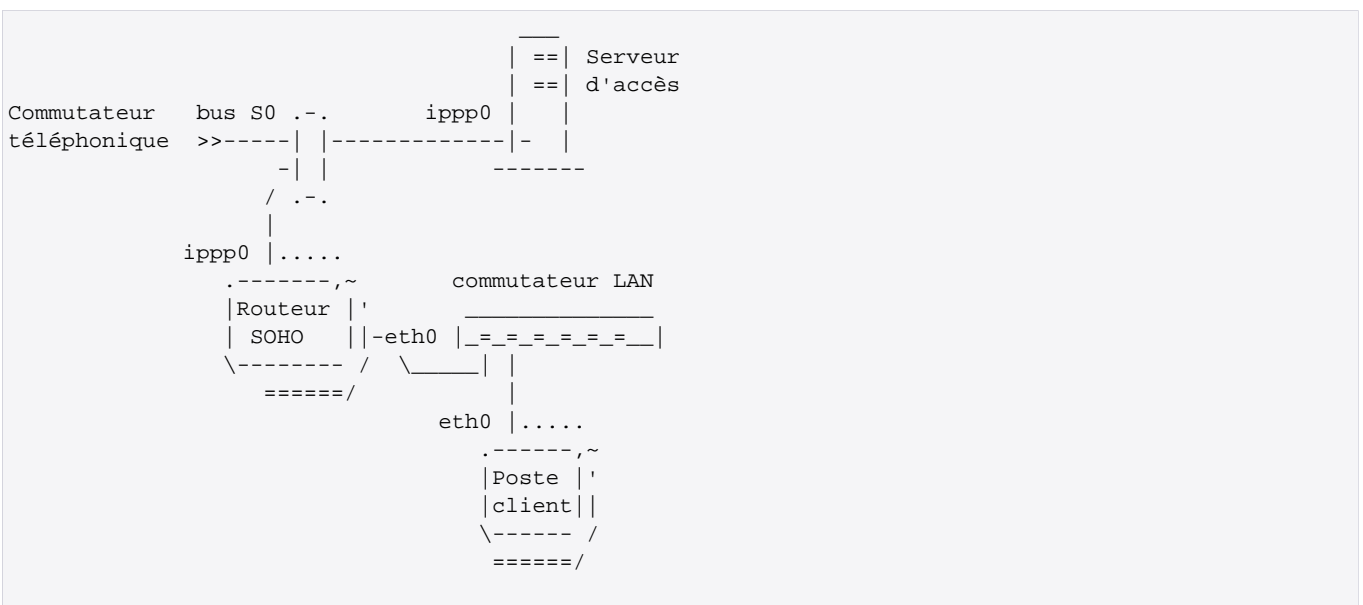
À partir du fichier `/var/log/syslog`, relever les informations relatives à la couche liaison du protocole PPP : le protocole LCP.

3. Quelles sont les informations contenues dans les messages système qui permettent de valider l'échange des adresses IP entre le serveur et le client ?

Toujours à partir du fichier `/var/log/syslog`, relever les informations relatives à la couche réseau du protocole PPP : le protocole IPCP.

5. Système Routeur d'agence (*Spoke*)

Dans ce scénario, le routeur accède à Internet par son interface WAN ou RNIS et redistribue cet accès sur un réseau local. Ce genre de routeur est appelé «routeur d'agence». Il fait partie de la catégorie d'équipement *Small Office Home Office* ou SOHO.



5.1. Connexion au réseau local

1. Quelles sont les opérations nécessaires à la configuration de l'interface Ethernet ?

Reprendre les questions du support *Configuration d'une interface RNIS en mode rawip*¹³.

2. Quels sont les tests à réaliser pour s'assurer du fonctionnement de l'accès Internet ?

Reprendre la séquence «rituelle» des tests ICMP avec la commande **ping** et les adresses : boucle locale (*loopback*), interface locale, passerelle par défaut et une adresse réseau située sur un autre réseau. Ce n'est qu'en dernier lieu que l'on doit effectuer un test avec le service de noms de domaines à l'aide des commandes **host** ou **dig**. Enfin, si le protocole ICMP n'est pas disponible au delà du réseau local, il faut utiliser la commande **tcptraceroute** pour tester la connectivité inter réseaux.

5.2. Connexion au réseau étendu

1. Quelles sont les opérations nécessaires à la configuration de l'interface RNIS en serveur d'appels ?

Reprendre les questions ci-avant : **Section 3, « Connexion avec le protocole PPP »**.

¹² <http://tldp.org/HOWTO/PPP-HOWTO/>

¹³ <http://www.linux-france.org/prj/inetdoc/cours/interco.rawip.tp/>

2. Donner la liste des options de la commande **isdnctrl** pour la configuration serveur d'appels ?
Rechercher dans les documents les éléments associés à l'option `diout`.
3. Quels sont les fichiers nécessaires à l'utilisation du démon `ippd` en serveur d'appels ?
Utiliser les pages de manuels du démon `ippd`.
4. Quelle est l'option de la commande **isdnctrl** qui permet de sauvegarder/restituer la configuration de l'interface (RNIS|ISDN) ?
Utiliser les pages de manuel de l'outil **isdnctrl**. Sauvegarder le fichier de configuration de l'interface pour les utilisations ultérieures.

5.3. Configuration du routeur d'agence (*Spoke*)

1. Quelle est la fonction réseau du noyau LINUX qui permet d'activer le routage des paquets entre les interfaces du système ?
Consulter le support *Fonctions réseau du noyau Linux*¹⁴.
2. Quelle est la fonction de filtrage utilisée pour gérer l'espace d'adressage tout en contrôlant les accès ?
Consulter le support *Fonctions réseau du noyau Linux*¹⁵.
3. Donner la liste des options de la commande **iptables** pour activer les fonctions de traduction d'adresses et de suivi de communication pour le routeur d'agence ?
À partir du support *Fonctions réseau du noyau Linux*¹⁶ et des exemples donnés dans le guide *guide NAT-HOWTO*¹⁷, établir une configuration simple de traduction d'adresse. Attention à adopter une syntaxe indépendante de l'adressage IP pour pouvoir changer de numérotation réseau à volonté.
4. Quels sont les tests à réaliser pour s'assurer du fonctionnement du routeur d'agence ?
Reprendre la séquence «rituelle» des tests ICMP en direction du poste client et de l'Internet. Visualiser aussi l'utilisation des règles de filtrage avec l'outil **iptables**. Consulter les pages de manuels de la commande **iptables**.

5.4. Authentification PPP

1. Quelles sont les options de configuration du démon `ippd` qui permettent d'activer l'authentification auprès du routeur d'accès ?
Consulter les pages de manuel du démon `ippd` ainsi que le guide *Linux PPP HOWTO*¹⁸
2. Quelles sont les informations contenues dans les messages système qui permettent de valider la connexion téléphonique ?
À partir du fichier `/var/log/syslog`, relever les informations relatives à la couche liaison du protocole PPP : le protocole LCP.
3. Quelles sont les informations contenues dans les messages système qui permettent de valider l'échange des adresses IP entre le serveur et le client ?
Toujours à partir du fichier `/var/log/syslog`, relever les informations relatives à la couche réseau du protocole PPP : le protocole IPCP.

¹⁴ <http://www.linux-france.org/prj/inetdoc/cours/interco.noyau/>

¹⁵ <http://www.linux-france.org/prj/inetdoc/cours/interco.noyau/>

¹⁶ <http://www.linux-france.org/prj/inetdoc/cours/interco.noyau/>

¹⁷ <http://www.linux-france.org/prj/inetdoc/guides/NAT-HOWTO/NAT-HOWTO-4.html#ss4.1>

¹⁸ <http://tldp.org/HOWTO/PPP-HOWTO/>

6. Documents de référence

The Point-to-Point Protocol (PPP)

RFC1661 *The Point-to-Point Protocol (PPP)*¹⁹ : Le protocole point-à-point PPP fournit une méthode standard de transport de datagrammes multi-protocoles sur des liaisons point à point. PPP comprend 3 composants principaux :

1. Une méthode d'encapsulation des datagrammes multi-protocoles.
2. Un protocole de contrôle de niveau liaison ou *Link Control Protocol (LCP)* pour établir, configurer et tester une connexion de données à ce niveau.
3. Une famille de protocoles de contrôle de niveau réseau pour établir et configurer différents protocoles de niveau réseau.

Dans la plupart des cas, on retrouve des trames HDLC au niveau liaison et IP est le seul protocole réseau utilisé.

L'architecture du sous-système RNIS

L'architecture du sous-système RNIS Linux²⁰ : présentation des différents types d'interfaces accessibles avec le sous-système (RNIS|ISDN) du noyau LINUX.

Configuration d'une interface RNIS en mode rawip

Configuration d'une interface RNIS en mode rawip²¹ : support de travaux pratiques utilisant la connexion directe sur le réseau téléphonique.

Configuration d'une interface de réseau local

Configuration d'une interface de réseau local²² : identification du type d'interface, de ses caractéristiques et manipulations des paramètres. Ce support fournit une méthodologie de dépannage simple d'une connexion réseau.

Debian Reference Chapter 10 - Network configuration

Guide de référence pour Debian Chapitre 10 - Configuration réseau²³ : chapitre du manuel de référence *Debian* consacré à l'administration réseau.

Fonctions réseau du noyau Linux

Fonctions réseau du noyau Linux²⁴ : présentation et configuration des fonctions réseau du noyau LINUX

Guide Pratique du NAT sous Linux 2.4

guide NAT-HOWTO²⁵ : Ce document décrit comment réaliser du camouflage d'adresse IP, un serveur mandataire transparent, de la redirection de ports ou d'autres formes de traduction d'adresse réseau (*Network Address Translation* ou NAT) avec le noyau Linux 2.4.

Linux PPP HOWTO

Linux PPP HOWTO²⁶ : Ce guide est relativement ancien. On y trouve cependant des exemples utiles sur le paramétrage de l'authentification avec la protocole PPP.

¹⁹ <http://www.faqs.org/rfcs/rfc1661.html>

²⁰ <http://www.linux-france.org/prj/inetdoc/guides/rnis/part2.chapter1.arch.html>

²¹ <http://www.linux-france.org/prj/inetdoc/cours/interco.rawip.tp/>

²² <http://www.linux-france.org/prj/inetdoc/cours/config.interface.lan/>

²³ <http://qref.sourceforge.net/Debian/reference/ch-gateway.fr.html>

²⁴ <http://www.linux-france.org/prj/inetdoc/cours/interco.noyau/>

²⁵ <http://www.linux-france.org/prj/inetdoc/guides/NAT-HOWTO/NAT-HOWTO-4.html#ss4.1>

²⁶ <http://tldp.org/HOWTO/PPP-HOWTO/>