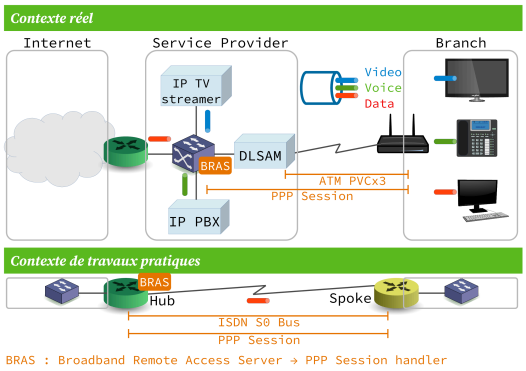
Topologie Hub & Spoke avec le protocole PPP

Philippe Latu
philippe.latu(at)inetdoc.net

https://www.inetdoc.net

Résumé



L'objectif de ce support de travaux pratiques est l'interconnexion de réseaux locaux et de réseaux étendus. On utilise une topologie classique baptisée Hub & Spoke dans laquelle le routeur Hub est relié à plusieurs routeurs Spoke via une liaison point à point qui utilise le protocole PPP. Le support physique utilsé pour illustrer la topologie est la technologie RNIS qui permet de transmettre des trames HDLC en couche liaison.

Table des matières

1. Copyright et Licence

1.1. Méta-information

Cet article est écrit avec DocBook XML sur un système Debian GNU/Linux. Il est disponible en version imprimable au format PDF : `interco.ppp.qa.pdf`.

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 :

- iproute2 - outils de contrôle du trafic et du réseau
- ifupdown - Outils de haut niveau pour configurer les interfaces réseau
- iputils-ping - Outils pour tester l'accessibilité de noeuds réseaux
- isdnutils-base - utilitaires pour RNIS – ensemble mininmal
- 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.

2. Aide à la mise au point

Afin de résoudre les problèmes de connexion et de configuration, il existe différents canaux d'information système. Voici trois exemples de consultation de messages :

Messages système émis par le noyau Linux

L'affichage des messages système est géré par le démon `rsyslogd`. Pour consulter ces messages, il faut lire le contenu des fichiers du répertoire `/var/log/`. Dans le cas des travaux pratiques, les informations nécessaires à la mise au point des connexions réseau se trouvent 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`.

Du point de vue droits sur le système de fichiers, la commande tail peut être utilisée au niveau utilisateur normal dès lors que celui-ci appartient au groupe `adm`. Les commandes id et groups permettent de connaître les groupes auxquels l'utilisateur courant appartient.

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/isdnctrl0 >/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 ipppd

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

```
# grep ^daemon /etc/rsyslog.conf
daemon.*                        -/var/log/daemon.log
```

3. Interface RNIS & protocole PPP

La connexion directe à l'aide du mode `rawip` (Voir Configuration d'une interface RNIS en mode rawip) présente l'avantage de la simplicité : authentification basée sur les numéros de téléphone sans échange d'adresses IP. Ce mode de connexion présente cependant des 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.
- Comme la configuration réseau est effectuée manuellement à chaque extrémité, le plan d'adressage IP doit être connu de toutes les entités en communication.

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). 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.

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

Q1. 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`.

L'option recherchée dans les pages de manuels est : `syncppp`.

Q2. 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.

On peut, par exemple;, effectuer la recherche suivante.

```
$ aptitude search ppp | grep -i isdn
p   ipppd               - ISDN utilities - PPP daemon
p   pppdcapiplugin      - ISDN utilities - pppd plug-in for CAPI sup
```

C'est le paquet `ipppd` qui contient le démon du même nom qui correspond à l'utilisation du sous-système RNIS du noyau Linux.

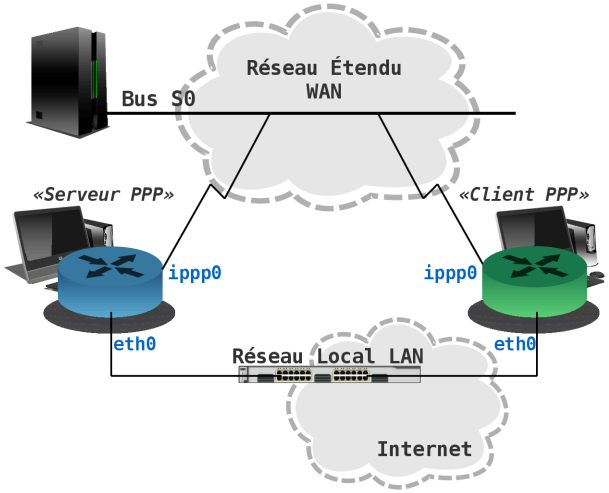
Q3. Quelles sont les noms d'interface RNIS à utiliser avec ce démon de gestion de connexion ?

Voir les pages de manuels de l'outil de configuration d'interface isdnctrl.

Le sous-système RNIS du noyau Linux dispose d'entrées spécifiques par type de communication. L'utilisation du démon `ipppd` impose une communication via un descripteur de périphérique nommé `/dev/ipppX` où X désigne un numéro d'interface.

4. Connexion avec le protocole PPP

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.



Topologie équivalente entre serveur et client PPP

C'est le serveur qui doit fournir les adresses données dans le tableau ci-dessous.

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

Bus	Serveur PPP	N° tél.	Adresses IP serveur:client	N° tél.	Client PPP
S0.1	alderaan	104	`192.168.104.1:192.168.105.2`	105	bespin
S0.2	centares	106	`192.168.106.1:192.168.107.2`	107	coruscant
S0.3	dagobah	108	`192.168.108.1:192.168.109.2`	109	endor
S0.4	felucia	110	`192.168.110.1:192.168.111.2`	111	geonosis
S0.5	hoth	112	`192.168.112.1:192.168.113.2`	113	mustafar
S0.6	naboo	114	`192.168.114.1:192.168.115.2`	115	tatooine

Attention, les adresses données dans ce tableau étant utilisées par des liens point à point, le masque réseau occupe les 32 bits de l'espace d'adressage.

Saisie des options du démon 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/ioptions*` 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.

4.1. Sans authentification

Q4. 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.

Le protocole PPP n'a pas été conçu suivant le modèle Client/Serveur. Il suppose que deux processus pairs échangent des informations. Pour cette question c'est l'option `auth` qui définit

si un hôte requiert une authentification de l'hôte pair. Cette authentification peut être requise par chacune des extrémités en communication. Pour désactiver l'authentification à chaque extrémité, on ajoute le préfixe `no` à l'option `auth`.

Q5. 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 la réponse se trouve.

C'est l'option `debug` qui permet l'affichage des informations relatives aux différentes étapes de l'établissement de la connexion PPP.

Q6. Quels sont les noms des deux sous-couches du protocole PPP qui apparaissent dans les journaux systèmes ? Quels sont les rôles respectifs de ces deux sous-couches ?

Consulter la page Point-to-Point Protocol.

La consultation des journaux système fait apparaître les informations suivantes.

```
pppd[3262]: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0x46010ac>]
kernel: [  895.700115] NET: Registered protocol family 24
pppd[3262]: rcvd [LCP ConfReq id=0x1 <magic 0xcab9fecc>] ❶
pppd[3262]: sent [LCP ConfAck id=0x1 <magic 0xcab9fecc>]
pppd[3262]: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0x46010ac>]
pppd[3262]: rcvd [LCP ConfAck id=0x1 <mru 1492> <magic 0x46010ac>]
pppd[3262]: sent [LCP EchoReq id=0x0 magic=0x46010ac]
pppd[3262]: peer from calling number 52:54:00:12:34:05 authorized
pppd[3262]: sent [IPCP ConfReq id=0x1 <addr 0.0.0.0>] ❷
pppd[3262]: rcvd [LCP EchoReq id=0x0 magic=0xcab9fecc]
pppd[3262]: sent [LCP EchoRep id=0x0 magic=0x46010ac]
pppd[3262]: rcvd [IPCP ConfReq id=0x1 <addr 10.0.0.1>]
pppd[3262]: sent [IPCP ConfAck id=0x1 <addr 10.0.0.1>]
pppd[3262]: rcvd [LCP EchoRep id=0x0 magic=0xcab9fecc]
pppd[3262]: rcvd [IPCP ConfNak id=0x1 <addr 10.67.15.1>]
pppd[3262]: sent [IPCP ConfReq id=0x2 <addr 10.67.15.1>]
pppd[3262]: rcvd [IPCP ConfAck id=0x2 <addr 10.67.15.1>]
pppd[3262]: local  IP address 10.67.15.1
pppd[3262]: remote IP address 10.0.0.1
```

❶ La sous-couche Link Control Protocol (LCP) assure la configuration automatique des interfaces à chaque extrémité. Les paramètres négociés entre les deux hôtes en communication sont multiples : l'adaptation de la taille de datagramme, les caractères d'échappement, les numéros magiques et la sélection des options d'authentification.

❷ La sous-couche Network Control Protocol (NCP) assure l'encapsulation de multiples protocoles de la couche réseau. Dans l'exemple donné, c'est le protocole IP qui est utilisé ; d'où l'acronyme IPCP.

Q7. Quels sont les en-têtes du dialogue qui identifient les requêtes (émises|reçues), les rejets et les acquittements ?

Consulter les journaux système contenant les traces d'une connexion PPP.

La copie d'écran donnée ci-dessus fait apparaître les directives `Conf*` pour chaque paramètre négocié.

- `ConfReq` indique une requête.
- `ConfAck` indique un acquittement.
- `ConfNak` indique un rejet.

4.2. Avec authentification PAP

Relativement à la section précédente, on ajoute ici le volet authentification au dialogue PPP en utilisant le protocole PAP.

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

> 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.

Q8. Quelles sont les options de configuration spécifiques à l'authentification PAP à fournir au démon PPP ?

Consulter les pages de manuels du démon ipppd.

C'est l'option `pap` qui permet de spécifier ce type d'authentification.

Q9. Dans quel fichier sont stockés les paramètres d'authentification login/password utilisés par le protocole PAP ?

Consulter les pages de manuels du démon ipppd.

C'est le fichier `/etc/ppp/pap-secrets` qui contient les couples login/password utilisés lors de l'authentification.

Q10. Quels sont les en-têtes du dialogue de la couche LCP qui identifient les requêtes d'authentification échangées entre les deux processus pairs ?

Voici une copie d'écran de connexion qui fait apparaître les directives `Conf*` relatives à la partie authentification.

```
pppd[5259]: sent [LCP ConfReq id=0x1 <auth pap> <magic 0x53c04a36>]
pppd[5259]: rcvd [LCP ConfAck id=0x1 <auth pap> <magic 0x53c04a36>]
pppd[5259]: rcvd [LCP ConfReq id=0x1 <mru 1492> <magic 0x3f810ce9>]
pppd[5259]: sent [LCP ConfAck id=0x1 <mru 1492> <magic 0x3f810ce9>]
pppd[5259]: sent [LCP EchoReq id=0x0 magic=0x53c04a36]
pppd[5259]: rcvd [LCP EchoReq id=0x0 magic=0x3f810ce9]
pppd[5259]: sent [LCP EchoRep id=0x0 magic=0x53c04a36]
pppd[5259]: rcvd [PAP AuthReq id=0x1 user="etu" password=<hidden>]
```

Q11. 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 ?

L'utilisation de la méthode d'authentification PAP implique que le mot de passe circule en clair. Une simple capture du trafic permet de «relever» le mot de passe.

Voici un extrait de capture réseau effectué avec le démon `pppd` à l'aide de la commande `# tshark -V -i eth0 -R "ppp" > grepMyPassword.txt`.

```
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Session Data (0x00)
    Session ID: 0x0003
    Payload Length: 16
Point-to-Point Protocol
    Protocol: Password Authentication Protocol (0xc023)
PPP Password Authentication Protocol
    Code: Authenticate-Request (1)
    Identifier: 1
    Length: 14
    Data
        Peer-ID-Length: 3
        Peer-ID: etu
        Password-Length: 5
        Password: stri
```

4.3. Avec authentification CHAP

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

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

Q12. Quelles sont les options de configuration spécifiques à l'authentification CHAP à fournir au démon PPP ?

Consulter les pages de manuels du démon ipppd.

C'est l'option `chap` qui permet de spécifier ce type d'authentification.

Q13. Dans quel fichier sont stockés les paramètres d'authentification login/password utilisés par le protocole CHAP ?

Consulter les pages de manuels du démon ipppd.

C'est le fichier `/etc/ppp/chap-secrets` qui contient les couples login/password utilisés lors de l'authentification.

Q14. Quels sont les en-têtes du dialogue de la couche LCP qui identifient les requêtes d'authentification échangées entre les deux processus pairs ?

Voici une copie d'écran de connexion qui fait apparaître les directives `Conf*` relatives à la partie authentification.

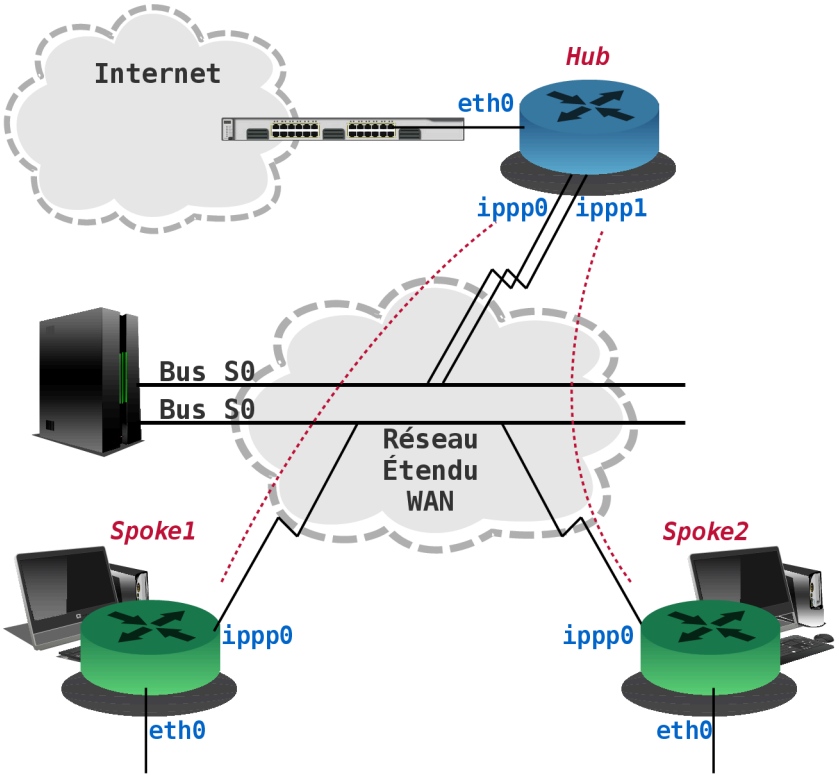
```
pppd[6037]: pppd 2.4.5 started by root, uid 0
pppd[6037]: using channel 28
pppd[6037]: Using interface ppp0
pppd[6037]: Connect: ppp0 < /dev/pts/1
pppd[6037]: sent [LCP ConfReq id=0x1 <auth chap MD5> <magic 0x46c97184>]
pppd[6037]: rcvd [LCP ConfAck id=0x1 <auth chap MD5> <magic 0x46c97184>]
pppd[6037]: rcvd [LCP ConfReq id=0x1 <mru 1492> <auth chap MD5> <magic 0x1f157ebf>]
pppd[6037]: sent [LCP ConfAck id=0x1 <mru 1492> <auth chap MD5> <magic 0x1f157ebf>]
pppd[6037]: sent [LCP EchoReq id=0x0 magic=0x46c97184]
pppd[6037]: sent [CHAP Challenge id=0x86 <ed6d9c0c022dbe008b2d3332fb275f5af1ca499393>,\
     name = "ppp-hub"]
pppd[6037]: rcvd [LCP EchoReq id=0x0 magic=0x1f157ebf]
pppd[6037]: sent [LCP EchoRep id=0x0 magic=0x46c97184]
pppd[6037]: rcvd [CHAP Challenge id=0x4f <29b6227da7da53d7ee2b4f6f7ec9a1900d5c9ac33f14>,\
     name = "etu"]
pppd[6037]: sent [CHAP Response id=0x4f <cb5bf4fbb0f9afd98a477f1f8a2e4c1f>,\
     name = "etu"]
pppd[6037]: rcvd [LCP EchoRep id=0x0 magic=0x1f157ebf]
pppd[6037]: rcvd [CHAP Response id=0x86 <de265c472d38a441fdbd2228314e0d86>,\
     name = "etu"]
pppd[6037]: sent [CHAP Success id=0x86 "Access granted"]
pppd[6037]: rcvd [CHAP Success id=0x4f "Access granted"]
pppd[6037]: CHAP authentication succeeded: Access granted
pppd[6037]: CHAP authentication succeeded
```

Q15. 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 ?

Les éléments donnés dans le copie d'écran ci-dessus montrent qu'il n'y a pas d'échange de mot de passe entre les deux systèmes en communication. Seuls des Challenges sont échangés.

5. Topologie Hub & Spoke

La topologie dite Hub & Spoke est une forme de topologie étoile dans laquelle tous les liens sont de type point à point. Le rôle du Hub est de concentrer tous les accès depuis les sites distants ou les Spokes. Du point de vue routage le Hub détient la totalité du plan d'adressage alors que les Spokes ne disposent que d'un accès unique vers les autres réseaux.



Topologie Hub & Spoke

Dans le contexte de ces travaux pratiques, le routeur Hub dispose d'un accès au réseau local (LAN) via son interface Ethernet et doit fournir un accès à Internet par ses interfaces d'accès au réseau étendu (WAN). Ce réseau étendu est modélisé par les deux canaux B de l'interface RNIS du Hub. Côté Spokes, les interfaces Ethernet sont provisoirement inutilisées et le seul accès aux autres réseau se fait par un canal B de l'interface RNIS.

5.1. 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/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
 ippp0)  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.

5.2. Plan d'adressage

Pour mettre en œuvre la topologie voulue, on distingue 4 groupes de 3 postes de travaux pratiques. Le rôle de chaque poste est défini dans le tableau ci-dessous.

Tableau 2. Affectation des rôles, des numéros de bus S0 et des adresses IP

Groupe	Poste	Rôle	Bus S0	N° Tél.	Interface	Réseau/Authentification
1	centares	Hub	S0.1	104	ippp0	192.168.104.1:192.168.104.2
			S0.1	105	ippp1	192.168.105.1:192.168.105.2
	bespin	Spoke 1	S0.2	106	ippp0	etu_s1 / Sp0k3.1
			-	-	dummy0	10.106.0.1/29
	alderaan	Spoke 2	S0.2	107	ippp0	etu_s2 / Sp0k3.2
			-	-	dummy0	10.107.0.1/29
2	endor	Hub	S0.3	108	ippp0	192.168.107.1:192.168.107.2
			S0.3	109	ippp1	192.168.108.1:192.168.108.2
	dagobah	Spoke 1	S0.4	110	ippp0	etu_s1 / Sp0k3.1
			-	-	dummy0	10.109.0.1/29
	coruscant	Spoke 2	S0.4	111	ippp0	etu_s2 / Sp0k3.2
			-	-	dummy0	10.110.0.1/29
3	hoth	Hub	S0.5	112	ippp0	192.168.111.1:192.168.111.2
			S0.5	113	ippp1	192.168.112.1:192.168.112.2
	geonosis	Spoke 1	S0.6	114	ippp0	etu_s1 / Sp0k3.1
			-	-	dummy0	10.113.0.1/29
	felucia	Spoke 2	S0.6	115	ippp0	etu_s2 / Sp0k3.2
			-	-	dummy0	10.114.0.1/29
4	naboo	Hub	S0.7	116	ippp0	192.168.115.1:192.168.115.2
			S0.7	117	ippp1	192.168.116.1:192.168.116.2
	mustafar	Spoke 1	S0.8	118	ippp0	etu_s1 / Sp0k3.1
			-	-	dummy0	10.117.0.1/29
	tatooine	Spoke 2	S0.8	119	ippp0	etu_s2 / Sp0k3.2
			-	-	dummy0	10.118.0.1/29

Comme dans le tableau d'adressage précédent, les adresses données ci-dessus étant utilisées par des liens point à point, le masque réseau occupe les 32 bits de l'espace d'adressage.

> Avertissement
>
> Les connexions RNIS des routeurs (Hubs doivent se faire directement sur les ports de l'autocommutateur RNIS. En effet, ces connexions utilisent les deux canaux B du port BRI.

6. Configuration d'un routeur Hub

Compte tenu de la topologie définie dans la section précédente, on doit configurer les interfaces LAN et WAN du Hub. Ce routeur doit fournir l'accès Internet via son interface LAN et attribuer les adresses IP aux Spokes via ses interfaces WAN.

6.1. Connexion au réseau local

Le routeur Hub accède à l'Internet via son interface LAN. Cet accès doit être permanent et indépendant de l'état des interfaces WAN.

Q16. Comment activer le routage au niveau dans le noyau du routeur ?

Consulter le document Configuration d'une interface de réseau local et les pages de manuels de la commande sysctl pour trouver les options d'activation du routage IPv4.

Les paramètres de réglage des fonctions réseau du noyau Linux sont situés dans l'arborescence `/proc`. L'ensemble de ces paramètres est géré par la commande sysctl. On commence par effectuer une recherche avec la chaîne de caractères `ip_forward`.

```
# sysctl -a --pattern ip_forward
net.ipv4.ip_forward = 0
net.ipv4.ip_forward_use_pmtu = 0
```

Activer le routage revient à placer l'indicateur à la valeur `1`.

```
# sysctl -w net.ipv4.ip_forward=1
```

Pour rendre ce réglage permanent, il est possible d'éditer le fichier `/etc/sysctl.conf`. De cette façon, le routage sera activé à chaque redémarrage du système.

Q17. Quelles sont les opérations nécessaires à la configuration de la traduction des adresses sources des paquets sortant par l'interface LAN ?

Consulter la documentation Guide Pratique du NAT.

On utilise ici la méthode de traduction d'adresses sources la plus simple. Elle est connue sous le nom de masquerading.

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Q18. Quels sont les tests à réaliser pour s'assurer du fonctionnement de l'accès Internet ?

Consulter la documentation Configuration d'une interface de réseau local.

Les tests peuvent se décomposer en deux parties : l'utilisation du protocole ICMP et l'analyse réseau.

Avec ICMP, il faut reprendre la séquence «rituelle» des requêtes echo en allant de la destination la plus proche à la plus éloignée. On débute avec l'interface de boucle locale (loopback), puis l'interface locale, puis la passerelle par défaut et enfin une adresse IP 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, on peut utiliser un outil du type tcptraceroute pour tester la connectivité inter réseau.

Pour la partie analyse réseau, tshark permet d'analyser à la console le trafic passant par chacune des interfaces d'un routeur. Il permet notamment de caractériser le fonctionnement de la traduction d'adresses entre les interfaces LAN et WAN.

6.2. Connexion au réseau étendu

Chaque routeur Hub utilise les deux canaux B d'un bus S0. On doit donc configurer deux interfaces `ipppX` pour établir les connexions point à point avec les deux Spokes.

Q19. Donner la liste des options de la commande isdnctrl pour la configuration des deux interfaces du Hub ?

Reprendre les instructions vues dans le support Configuration d'une interface RNIS en mode rawip et la Section 4, « Connexion avec le protocole PPP ».

Comme dans les questions précédentes du même type, on doit effectuer les opérations suivantes pour chacune des deux interfaces `/dev/ippp0` et `/dev/ippp1`.

1. Créer l'interface.
2. Attribuer le numéro de téléphone entrant.
3. Attribuer l'identifiant MSN/EAZ (Multiple Subscriber Number) à partir du numéro de téléphone entrant.
4. Attribuer le numéro de téléphone du correspondant.
5. Choisir le protocole HDLC pour la couche liaison.
6. Choisir l'encapsulation `syncppp`.
7. Fixer le mode de connexion automatique.

Q20. Quelles sont les opérations supplémentaires nécessaires à la configuration des interfaces RNIS du routeur Hub ?

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

De façon à éviter les «croisements» entre les affectations d'adresses IP des deux Spokes, il est nécessaire de lier les interfaces réseau avec le plan de numérotation téléphonique. Par exemple, sur le Hub Centares, on peut exécuter les commandes suivantes.

```
# isdnctrl pppbind ippp0 0
# isdnctrl pppbind ippp1 1
```

Q21. Quelle est l'option de la commande isdnctrl qui permet de sauvegarder/restituer la configuration de l'interface RNIS ?

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

Ce sont les options `readconf` et `writeconf` de la commande isdnctrl quit permettent respectivement de lire et d'écrire dans un fichier de configuration l'ensemble des paramètres d'une ou plusieurs interfaces RNIS.

Q22. Quelles sont les opérations à effectuer pour mettre en œuvre le protocole PPP avec une authentification CHAP ?

Reprendre les questions de la Section 4, « Connexion avec le protocole PPP » pour chacune des deux interfaces. Les couples d'authentification login/password sont donnés dans le Section 5.2, « Plan d'adressage ».

6.3. Routage statique

Pour que les réseaux desservis par les routeurs Spokes soient accessibles depuis toutes les extrémités en communication, le routeur Hub doit disposer d'une table de routage complète. Comme le nombre des réseaux de chaque Spoke est limité, on utilise des entrées statiques dans la table de routage du Hub.

Q23. Comment ajouter une entrée statique dans la table de routage du Hub ?

Rechercher les options de la commande ip dans le Manuel de référence Debian : configuration du réseau.

C'est l'instruction `# ip route add ...` qui permet l'ajout de routes statiques. Par exemple, dans le cas du routeur Hub `centares`, les deux instructions suivantes permettent d'ajouter les deux routes correspondant aux deux réseaux des routeurs Spokes `alderaan` et `bespin`.

```
# ip route add 10.106.0.0/29 dev ippp0
# ip route add 10.107.0.0/29 dev ippp1
```

Q24. Comment tester la disponibilité des différents réseaux interconnectés ?

Reprendre les séquences de tests ICMP entre les différents hôtes.

7. Configuration d'un routeur Spoke

Dans ce scénario, le routeur accède à Internet par son interface WAN et redistribue cet accès sur un réseau local. Ce genre de routeur est appelé «routeur d'agence».

7.1. Connexion au réseau local

Compte tenu de la topologie définie dans la Section 5, « Topologie Hub & Spoke », l'interface LAN du routeur Spoke n'est pas utilisée. Il faut donc désactiver cette interface.

Q25. Comment supprimer la configuration d'une interface réseau au niveau système ?

Rechercher les outils systèmes proposés dans le Manuel de référence Debian : configuration du réseau.

Le paquet `ifupdown` propose deux scripts baptisés ifup et ifdown qui assurent un contrôle d'état sur la configuration des interfaces listées dans le fichier de configuration système `/etc/network/interfaces`.

Dans le cas de l'interface LAN du poste de travaux pratiques, `eth0` est configurée via le protocole DHCP. Pour résilier le bail DHCP et désactiver l'interface, on utilise l'instruction suivante.

```
# ifdown eth0
```

7.2. Connexion au réseau étendu

Chaque routeur Spoke utilise un canal B d'un bus S0. On doit donc configurer une interface `ippp0` pour établir la connexion point à point avec le Hub.

Q26. Donner la liste des options de la commande isdnctrl pour la configuration de l'interface du Spoke ?

Reprendre les instructions vues dans le support Configuration d'une interface RNIS en mode rawip et la Section 4, « Connexion avec le protocole PPP ».

Comme dans les questions précédentes du même type, on doit effectuer les opérations suivantes pour l'interface `/dev/ippp0`.

1. Créer l'interface.
2. Attribuer le numéro de téléphone entrant.
3. Attribuer l'identifiant MSN/EAZ (Multiple Subscriber Number) à partir du numéro de téléphone entrant.
4. Attribuer le numéro de téléphone du correspondant.
5. Choisir le protocole HDLC pour la couche liaison.

6. Choisir l'encapsulation `syncppp`.

7. Fixer le mode de connexion automatique.

Q27. Quelle est l'option de la commande isdnctrl qui permet de sauvegarder/restituer la configuration de l'interface RNIS ?

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

Ce sont les options `readconf` et `writeconf` de la commande isdnctrl quit permettent respectivement de lire et d'écrire dans un fichier de configuration l'ensemble des paramètres d'une ou plusieurs interfaces RNIS.

Q28. Quelles sont les opérations à effectuer pour mettre en œuvre le protocole PPP avec une authentification CHAP ?

Reprendre les questions de la Section 4, « Connexion avec le protocole PPP ». Les couples d'authentification login/password sont donnés dans le Section 5.2, « Plan d'adressage ».

7.3. Ajout d'un réseau fictif

L'ajout de nouvelles entrées fictives dans les tables de routage est une pratique très répandue. Elle permet de qualifier le bon fonctionnement d'un service ou d'un filtrage sans ajouter de matériel. Dans le cas de ces travaux pratiques, c'est le service Web qui est utilisé pour valider la disponibilité d'un réseau au niveau application.

Q29. Quelles sont les opérations à effectuer pour pouvoir utiliser des interfaces réseau virtuelles de type boucle locale sur un système GNU/Linux ?

Avec le noyau Linux, il est conseillé d'utiliser des interfaces baptisées dummy pour ce genre d'usage. Rechercher le module correspondant à charger en mémoire.

On charge le module `dummy` suivi de l'option `numdummies` pour créer les interfaces. Il suffit ensuite d'appliquer une nouvelle configuration IP pour ajouter un ou plusieurs nouveaux réseaux.

```
# ip link add dummy0 type dummy
```

En prenant l'exemple du Spoke `bespin`, on ajoute le réseau `10.106.0.0/29` en configurant l'interface `dummy0`.

```
# ip link set dev dummy0 up
# ip addr add 10.106.0.1/29 brd + dev dummy0
# ip route ls
default via 192.0.2.1 dev eth0
10.106.0.0/29 dev dummy0  proto kernel  scope link  src 10.106.0.1
192.0.2.0/26 dev eth0  proto kernel  scope link  src 192.0.2.10
```

Q30. Quelles sont les opérations à effectuer pour installer un service Web en écoute exclusivement sur l'adresse IP de l'interface `dummy0` ?

Installer le paquet `apache2` et modifier sa configuration pour que le service ne soit accessible que sur une adresse IP.

```
# aptitude install apache2
<snipped/>
Paramétrage de apache2-mpm-worker (2.2.21-2) ...
Starting web server: apache2apache2: Could not reliably determine the server's
fully qualified domain name, using 127.0.1.1 for ServerName
.
Paramétrage de apache2 (2.2.21-2) ...
<snipped/>
```

On modifie ensuite le fichier de configuration `/etc/apache2/ports.conf` de façon à limiter l'accès à l'adresse IP voulue.

```
# cd /etc/apache2/
# diff -uBb ports.conf.orig ports.conf
--- ports.conf.orig     2011-10-31 20:37:09.000000000 +0100
+++ ports.conf  2011-10-31 20:37:39.000000000 +0100
@@ -6,7 +6,7 @@
 # README.Debian.gz

 NameVirtualHost *:80
-Listen 80
+Listen 10.106.0.1:80

 <IfModule mod_ssl.c>
     # If you add NameVirtualHost *:443 here, you will also have to change
```

On redémarre le service et on affiche le liste des sockets inet ouverts sur le système pour confirmer que l'adresse IP choisie est bien affectée.

```
# /etc/init.d/apache2 restart
<snipped/>
# lsof -i | grep apache2
apache2  22206        root    3u  IPv4  30721      0t0  TCP 10.106.0.1:www (LISTEN)
apache2  22211    www-data    3u  IPv4  30721      0t0  TCP 10.106.0.1:www (LISTEN)
apache2  22212    www-data    3u  IPv4  30721      0t0  TCP 10.106.0.1:www (LISTEN)
```

Q31. Comment valider l'accès à ce service Web depuis les autres routeurs ?

Si la table de routage du routeur Hub est complète, on décrit les couches de la modélisation en partant de la couche réseau vers la couche application. Les tests ICMP valident le niveau réseau. Les tests traceroute valident le fonctionnement des protocoles de la couche transport. Enfin, le navigateur web permet de tester la couche application.

Voici trois exemples de tests.

- Test ICMP.

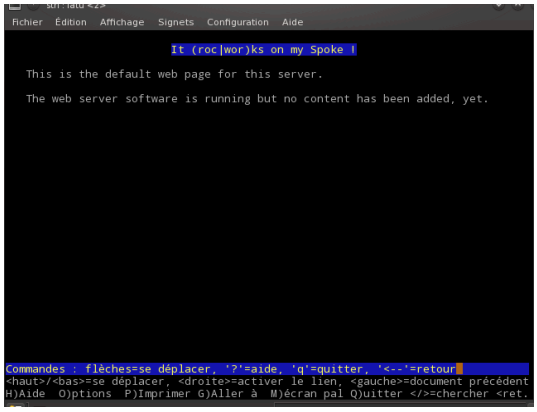
```
$ ping -c 2 10.106.0.1
PING 10.106.0.1 (10.106.0.1) 56(84) bytes of data.
64 bytes from 10.106.0.1: icmp_req=1 ttl=64 time=0.435 ms
64 bytes from 10.106.0.1: icmp_req=2 ttl=64 time=0.360 ms

--- 10.106.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.360/0.397/0.435/0.042 ms
```

- Test traceroute.

```
$ traceroute 10.106.0.1
traceroute to 10.106.0.1 (10.106.0.1), 30 hops max, 60 byte packets
 1  10.106.0.1 (10.106.0.1)  0.467 ms  0.256 ms  0.262 ms
```

- Test HTTP.



Copie d'écran navigateur Web

8. Documents de référence

The Point-to-Point Protocol (PPP)

RFC1661 The Point-to-Point Protocol (PPP) : 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.

Configuration d'une interface RNIS en mode rawip

Configuration d'une interface RNIS en mode rawip : 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 local : 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

Manuel de référence Debian : configuration du réseau : chapitre du manuel de référence Debian consacré à la configuration réseau.

Fonctions réseau du noyau Linux

Configuration des fonctions réseau & compilation du noyau Linux : présentation et configuration des fonctions réseau du noyau LINUX

Guide Pratique du NAT sous Linux 2.4

Guide Pratique du NAT : 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 HOWTO : Ce guide est relativement ancien. On y trouve cependant des exemples utiles sur le paramétrage de l'authentification avec la protocole PPP.