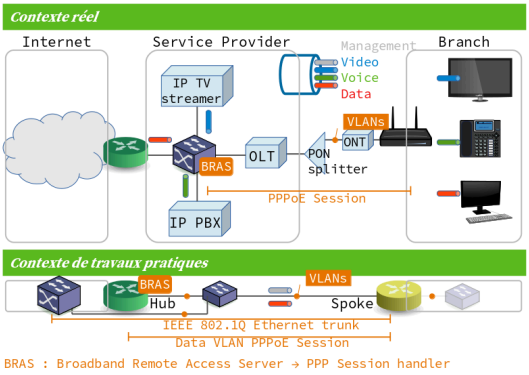
Topologie Hub & Spoke avec le protocole PPPoE

Philippe Latu
philippe.latu(at)inetdoc.net

https://www.inetdoc.net

Résumé



Ce support de travaux pratiques est une illustration d'une topologie réseau classique baptisée Hub & Spoke. Le Hub est un routeur qui concentre tous les flux des routeurs d'extrémités appelés Spoke. Les liaisons entre le Hub et les routeurs Spoke sont point à point et utilisent le protocole PPP. Avec la généralisation de la fibre optique dans les réseaux étendus (WAN), on doit encapsuler les trames PPP dans un VLAN Ethernet à l'aide de la technologie PPPoE.

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.pppoe.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 - High level tools to configure network interfaces
- iputils-ping - Tools to test the reachability of network hosts
- iputils-tracepath - Tools to trace the network path to a remote host
- ppp - Point-to-Point Protocol (PPP) - daemon
- pppoe - PPP over Ethernet driver

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.

1.3. Aide à la mise au point

Afin de résoudre les problèmes de connexion et de configuration, la journalisation système constitue le principal canal d'information.

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 d'un journal système à la console on peut utiliser la commande tail.

```
$ tail -n 50 -f /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.

2. Interface Ethernet & protocole PPP

Avec la généralisation de l'utilisation de la fibre optique dans les réseaux étendus, le format de trame historique HDLC est progressivement abandonné. Il faut dire que ce format de trame date du développement des liaisons séries asynchrones. Aujourd'hui, les liaisons sur fibres optiques sont Full-Duplex et on ne se préoccupe plus de synchronisation au niveau de la couche liaison de données. Le format de trame Ethernet devient donc une référence universelle.

Le protocole PPP offre depuis l'origine une configuration indépendante de la technologie du réseau étendu.

L'association entre trame Ethernet et PPP se fait grâce à un autre protocole baptisé PPPoE. Ce dernier permet d'encapsuler des trames PPP dans des trames Ethernet. Il est décrit à la page Point-to-point protocol over Ethernet qui permet de traiter les questions ci-après.

Q1. Quelle est la raison de l'ajout d'un nouveau protocole entre Ethernet et PPP ?

Consulter la page Point-to-point protocol over Ethernet.

Le protocole PPP a été conçu pour fonctionner sur des liaisons point-à-point alors qu'un réseau local Ethernet est par définition un réseau de diffusion.

Sur un réseau de diffusion, le canal de transmission est partagé entre tous les hôtes qui accèdent au canal. Il a donc été nécessaire d'introduire un mécanisme de découverte des deux extrémités en communication avant de lancer les opérations du protocole PPP.

Q2. Donner la liste des messages de découverte et de session PPPoE en précisant qui est l'initiative de cette découverte.

Consulter la page Point-to-point protocol over Ethernet.

- Client to server: Initiation (PADI)
- Server to client: Offer (PADO)
- Client to server: request (PADR)
- Server to client: session-confirmation (PADS)
- Either end to other end: termination (PADT)

Q3. Quels sont les autres mécanismes de découverte de voisins connus dans un réseau local Ethernet ?

Voici la liste des «grands classiques».

- Address Resolution Protocol (ARP).

  Quelle est l'adresse MAC d'un hôte dont on connaît l'adresse IPv4 ?

- Neighbor Discovery Protocol (NDP).

  Ce protocole est associé à IPv6. Il définit 5 messages ICMPv6 qui couvrent les opérations réalisées par ARP et qui ajoutent de nouvelles fonctions.

- Multicast DNS (mDNS) ou Bonjour.

  Ce protocole entre dans la famille zeroconf qui a pour but d'annoncer et de fournir des éléments de configuration aux hôtes du réseau sans faire appel à une infrastructure de services tels que DNS et DHCP.

3. Topologie Hub & Spoke - Protocole PPPoE

Le Protocole Point à Point (PPP) est utilisé pour établir une communication directe entre deux hôtes. Il relie deux routeurs de façon logique au dessus d'une topologie de réseau physique qui peut comprendre divers composants et différentes technologies. Il permet aux deux extrémités en communication de négocier des paramètres de transmission tels que l'authentification, la compression et l'attribution d'adresses de couche réseau. Dans ce document, on utilise le protocole PPP au dessus d'un réseau Ethernet qui représente la technologie mise en œuvre par un opérateur Internet.

Pour valider le fonctionnement du protocole PPPoE, on utilise les postes de travaux pratiques par groupes de deux routeurs Spoke et un routeur Hub. Les rôles sont définis ci-dessous.

Hub

Traduit mot à mot, le rôle Hub correspond à un concentrateur.

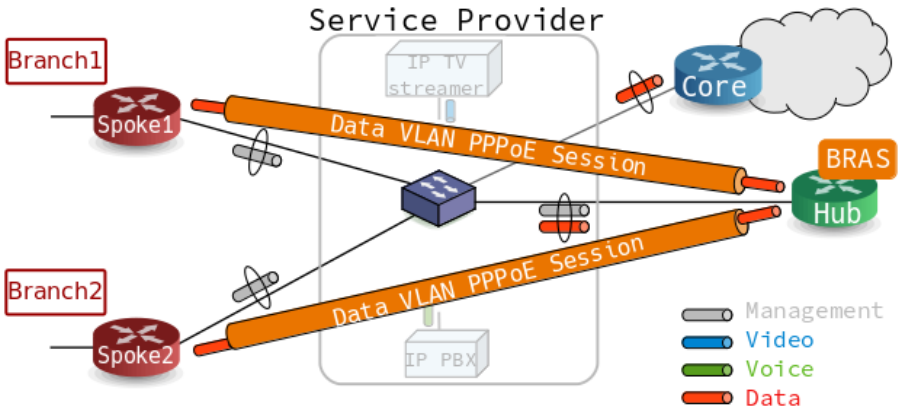
Il concentre tous les flux réseau des routeurs qui ont le rôle Spoke. En effet, les échanges entre deux routeurs Spoke doivent passer par le routeur Hub.

On lui attribue aussi la fonction de Broadband Remote Access Server ou BRAS. Dans notre contexte, cette fonction se caractérise par le fait que ce routeur détient le plan d'adressage. C'est lui qui a la responsabilité de délivrer les adresses IP lors de l'initiation de la session PPP.

Spoke

Contrairement au cas précédent, il n'y a pas de traduction mot à mot pour le rôle Spoke. Le routeur Spoke doit s'adresser au routeur Hub dès qu'il veut acheminer un flux réseau. Il s'agit d'un routeur d'extrémité qui ne dispose d'aucun chemin alternatif pour joindre l'Internet.

Dans les réseaux domestiques, la «box» correspond bien au rôle Spoke dans la mesure où elle se voit attribuer une adresse IPv4 publique par le fournisseur d'accès. Les seules informations qu'elle détient sont les authentifiants du client de l'opérateur.



Topologie entre deux routeurs Hub et Spoke avec PPPoE

Comme le montre le graphique ci-dessus, l'opérateur distingue 4 types de flux réseau. Dans les manipulations qui suivent, on ne s'intéresse qu'au VLANs Management et Data. La gestion des flux de téléphonie et de vidéo suppose que l'on mette en œuvre des services qui sortent du cadre de l'étude du protocole PPP.

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 les tableaux ci-dessous en fonction de la salle de travaux pratiques.

Plusieurs remarques sont à prendre en considération pour la suite du document.

- Les adresses IPv4 données dans les tableaux sont utilisées par des liens point à point. Le masque réseau est donc complet : `255.255.255.255`. Pour autant, les adresses ont été choisies de façon à pouvoir publier des réseaux avec un masque sur 30 bits via des routes statiques et/ou des protocoles de routage dynamique.
- Tous les exemples de commandes donnés dans la suite du document utilisent la numérotation suivante pour les VLANs.

Flux réseau	VLAN
Internet	4
Management	25
Data	26
Voice	27
Video	28

- Pour les accès à l'Internet, le routeur de cœur de réseau à utiliser est Casper. Les adresses de passerelle par défaut des routeurs Hub dans le VLAN `4` sont :
  - `172.16.16.2/20`
  - `2001:678:3fc:4::2/64`
- Pour l'adressage du réseau local d'extrémité du routeur Spoke, on utilise les préfixes suivants :
  - `10.2.6.1/28`
  - `2001:678:3fc:1a::1/64`

3.1. Plan d'adressage pour les groupes de 3 routeurs

Tableau 1. Affectation des rôles, des numéros de VLANs et des adresses pour la salle 211

Groupe	Poste	Rôle	VLAN	Flux	Réseau/Authentification
1	christophsis	Hub	4	Internet	`172.16.17.10/20`
					`2001:678:3fc:4::3a/64`
			400	Management	`fe80:190::3/64`
			401	Data	`192.168.1.141:192.168.1.142`
			402	Data	`192.168.1.145:192.168.1.146`
	corellia	Spoke 1	400	Management	`fe80:190::1/64`
			401	Data	`etu_s1 / Sp0k3.1`
				Branch	`10.4.0.1/26`
					`2001:678:3fc:191::1/64`
	delaya	Spoke 2	400	Management	`fe80:190::2/64`
			402	Data	`etu_s2 / Sp0k3.2`
				Branch	`10.4.0.65/26`
					`2001:678:3fc:192::1/64`
2	kashyyyk	Hub	4	Internet	`172.16.17.13/20`
					`2001:678:3fc:4::3d/64`
			405	Management	`fe80:195::3/64`
			406	Data	`192.168.1.149:192.168.1.150`
			407	Data	`192.168.1.153:192.168.1.154`
	korriban	Spoke 1	405	Management	`fe80:195::1/64`
			406	Data	`etu_s1 / Sp0k3.1`
				Branch	`10.4.0.129/26`
					`2001:678:3fc:196::1/64`
	kessel	Spoke 2	405	Management	`fe80:195::2/64`
			407	Data	`etu_s2 / Sp0k3.2`
				Branch	`10.4.0.193/26`
					`2001:678:3fc:197::1/64`
3	mygeeto	Hub	4	Internet	`172.16.17.16/20`
					`2001:678:3fc:4::40/64`
			410	Management	`fe80:19a::3/64`
			411	Data	`192.168.1.157:192.168.1.158`
			412	Data	`192.168.1.161:192.168.1.162`

Groupe	Poste	Rôle	VLAN	Flux	Réseau/Authentification
	nelvaan	Spoke 1	410	Management	`fe80:19a::1/64`
			411	Data	`etu_s1 / Sp0k3.1`
				Branch	`10.4.1.1/26`
					`2001:678:3fc:19b::1/64`
	rattatak	Spoke 2	410	Management	`fe80:19a::2/64`
			412	Data	`etu_s2 / Sp0k3.2`
				Branch	`10.4.1.65/26`
					`2001:678:3fc:19c::1/64`
4	saleucami	Hub	4	Internet	`172.16.17.19/20`
					`2001:678:3fc:4::43/64`
			415	Management	`fe80:19f::3/64`
			416	Data	`192.168.1.165:192.168.1.166`
			417	Data	`192.168.1.169:192.168.1.170`
	taris	Spoke 1	415	Management	`fe80:19f::1/64`
			416	Data	`etu_s1 / Sp0k3.1`
				Branch	`10.4.1.129/26`
					`2001:678:3fc:1a0::1/64`
	teth	Spoke 2	415	Management	`fe80:19f::2/64`
			417	Data	`etu_s2 / Sp0k3.2`
				Branch	`10.4.1.193/26`
					`2001:678:3fc:1a1::1/64`

3.2. Communications dans le VLAN Management

Sachant que les routeurs sont reliés entre eux par des trunks, il faut commencer par s'assurer que les échanges réseau sont possible au sein du VLAN de gestion opérateur : `Management`.

Q4. Comment créer et configurer une sous-interface dédiée au VLAN `Management` sur chaque routeur ?

Consulter les pages de manuels man ip-link et rechercher les options du type `vlan`.

Il est aussi possible de consulter l' Antisèche réseau.

La syntaxe de création d'une sous-interface de l'interface physique `eth0` est la suivante :

```
$ sudo ip link add link eth0 name eth0.25 type vlan id 25
```

La syntaxe d'activation de l'interface est la suivante :

```
$ sudo ip link set dev eth0.25 up
```

Dès cette étape il est possible de faire un recensement du voisinage réseau IPv6.

```
$ ping -c2 ff02::1%eth0.25
PING ff02::1%eth0.25(ff02::1%eth0.25) 56 data bytes
64 bytes from fe80::baca:3aff:fe9e:8556%eth0.25: icmp_seq=1 ttl=64 time=0.055 ms
64 bytes from fe80::c0da:e2ff:feec:6ac0%eth0.25: icmp_seq=1 ttl=64 time=2.83 ms (DUP!)
64 bytes from fe80::baca:3aff:fe9e:8556%eth0.25: icmp_seq=2 ttl=64 time=0.069 ms

--- ff02::1%eth0.25 ping statistics ---
2 packets transmitted, 2 received, +1 duplicates, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 0.055/0.985/2.831/1.305 ms

$ ip neigh ls dev eth0.25
fe80::c0da:e2ff:feec:6ac0 lladdr c2:da:e2:ec:6a:c0 REACHABLE
```

La dernière commande de la copie d'écran ci-dessus indique qu'au moins un voisin est joignable dans le domaine de diffusion correspondant au VLAN `Management`.

La syntaxe d'affectation d'une nouvelle adresse IPv6 à l'interface est la suivante :

```
$ sudo ip -6 addr add fe80:19::3/64 dev eth0.25

$ ip addr ls dev eth0.25
3: eth0.25@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 \
   qdisc noqueue state UP group default qlen 1000
    link/ether b8:ca:3a:9e:85:56 brd ff:ff:ff:ff:ff:ff
    inet6 fe80:19::3/64 scope link
       valid_lft forever preferred_lft forever
    inet6 fe80::baca:3aff:fe9e:8556/64 scope link
       valid_lft forever preferred_lft forever
```

Q5. Comment qualifier les échanges réseau dans le VLAN `Management` ?

Il faut, au minimum, que le routeur Hub et les deux routeurs Spoke puissent se contacter via le protocole ICMP. Cette opération sert à valider le raccordement physique entre les 3 routeurs ainsi que la configuration des ports de commutation Ethernet.

Voici un exemple de commande ping dans le VLAN `Management`.

```
$ ping -c2 fe80:19::1%eth0.25
PING fe80:19::1%eth0.25(fe80:19::1%eth0.25) 56 data bytes
64 bytes from fe80:19::1%eth0.25: icmp_seq=1 ttl=64 time=1.42 ms
64 bytes from fe80:19::1%eth0.25: icmp_seq=2 ttl=64 time=0.827 ms

--- fe80:19::1%eth0.25 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 0.827/1.124/1.422/0.299 ms
```

3.3. Activation du routage dans le noyau Linux

Quel que soit le rôle joué par le routeur, il est essentiel que la fonction de routage des paquets IPv4 et IPv6 soit activée dans le noyau Linux.

Q6. Quel est l'outil qui permet de modifier dynamiquement les paramètres de fonctionnement du noyau Linux ?

Les paramètres du noyau Linux apparaissent dans l'arborescence du système de fichiers virtuel `/proc`. Il faut rechercher le paquet contenant les outils qui travaillent avec cette arborescence.

Le paquet qui fournit les outils de manipulation des paramètres du noyau Linux est procps. Il contient l'outil sysctl qui nous permet de configurer la fonction de routage dans le noyau Linux.

Q7. Quels sont les fichiers ou répertoires qui contiennent les paramètres de configuration et leurs valeurs dans l'arborescence de configuration du système ?

Rechercher dans l'arborescence les références à l'outil de la question précédente.

```
$ sudo find /etc/ -name "*sysctl*"
/etc/sysctl.conf
/etc/sysctl.d
/etc/sysctl.d/README.sysctl
/etc/sysctl.d/99-sysctl.conf
```

C'est le fichier `/etc/sysctl.conf` qui contient les paramètres intéressants dans le contexte de ces travaux pratiques.

Q8. Quels sont les paramètres à modifier pour que le routage des paquets IPv4 et IPv6 soit effectif ?

La consultation du fichier fait apparaître directement les paramètres de routage. Il suffit alors de décommenter les lignes intéressantes.

Voici le contenu du fichier `/etc/sysctl.conf` après modification des paramètres et après filtrage des lignes de commentaires et des lignes vides.

```
$ egrep -v '(^#|^$)' /etc/sysctl.conf
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1
net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=1
net.ipv4.conf.all.secure_redirects = 1
net.ipv4.conf.all.log_martians = 1
```

Q9. Comment activer les paramètres définis dans les fichiers de configuration des paramètres du noyau Linux ?

Consulter les pages de manuels de la commande sysctl.

L'option `--system` de la commande sysctl permet de (re)parcourir tous les paramètres de tous les fichiers et répertoires de l'arborescence de configuration.

```
$ sudo sysctl --system
* Applying /etc/sysctl.d/99-sysctl.conf ...
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.all.secure_redirects = 1
net.ipv4.conf.all.log_martians = 1
* Applying /etc/sysctl.d/bindv6only.conf ...
net.ipv6.bindv6only = 1
* Applying /etc/sysctl.d/protect-links.conf ...
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
* Applying /etc/sysctl.conf ...
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.all.secure_redirects = 1
net.ipv4.conf.all.log_martians = 1
```

4. Configuration PPPoE d'un routeur Hub

Le rôle du routeur Hub, tel qu'il été défini dans la section précédente, est d'interconnecter un réseau local (LAN) qui donne accès à l'Internet et plusieurs réseaux étendus (WAN) d'extrémité. Dans le contexte de ces travaux pratiques, le routeur Hub assure aussi la fonction Broadband Remote Access Server (BRAS). C'est la raison pour laquelle il détient les adresses IPv4 et IPv6 à attribuer aux routeurs Spoke.

Ce routeur doit aussi gérer l'encapsulation des trames PPP dans Ethernet. Voir Section 2, « Interface Ethernet & protocole PPP ».

4.1. Côté réseaux étendus - WAN

Le protocole PPP n'a pas été conçu suivant le modèle Client/Serveur. Il suppose que deux processus pairs échangent des informations. Dans les questions qui suivent, le routeur Hub doit exiger que le routeur Spoke s'authentifie auprès de lui avant de délivrer les adresses de couche réseau.

Q10. Quel paquet spécifique à la gestion du dialogue PPPoE à installer sur le routeur Hub ?

Rechercher dans le catalogue des paquets, la référence pppoe.

```
$ aptitude search pppoe
i   pppoe      - Pilote PPP sur Ethernet
p   pppoeconf - configures PPPoE/ADSL connections
```

Le résultat de la commande aptitude show pppoe montre que c'est bien ce paquet qui répond au besoin.

Q11. Quel est le rôle de l'outil contenu dans le paquet demandé à la question précédente relativement au démon pppd fourni avec le paquet ppp ?

Rechercher dans les pages de manuels de l'outil demandé à la question précédente.

L'outil pppoe-server gère directement l'encapsulation des trames PPP dans les trames Ethernet. Il communique ensuite les paramètres utiles au démon pppd qui fonctionne de façon totalement transparente vis-à-vis de la technologie du réseau sous-jacent.

Q12. 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 lors du dialogue PPP fait apparaître des informations du type suivant.

```
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 IPv4 qui est utilisé ; d'où l'acronyme IPCP.

Q13. 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.

Q14. Dans quel fichier sont stockés les paramètres d'identité et d'authentification utilisés par le protocole CHAP ?

Consulter les pages de manuels du démon pppd à la section AUTHENTICATION.

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

Voici un exmple du contenu de ce fichier.

```
# Secrets for authentication using CHAP
# client        server  secret                  IP addresses
"spoke1"        *       "5p0k3-1-53cr3t"        *
"spoke2"        *       "5p0k3-2-53cr3t"        *
```

Q15. Dans quel fichier sont stockés les paramètres passés au démon pppd lors du lancement du serveur PPPoE ?

Consulter les pages de manuels de l'outil pppoe-server.

C'est le fichier `/etc/ppp/pppoe-server-options` qui contient la liste des paramètres utilisés lors du dialogue PPP.

Q16. Quelles sont les options du protocole PPP qui doivent être implantées dans le fichier demandé à la question précédente ?

Consulter les pages de manuels du démon pppd et rechercher les paramètres correspondant à la liste suivante.

- Afficher en détail toutes les étapes d'établissement de session dans les journaux système.
- Référencer l'identifiant du compte utilisateur à utiliser lors de l'authentification du routeur Spoke. Cette option implique que le compte utilisateur existe sur le système et qu'il soit présent dans le fichier `/etc/ppp/chap-secrets`.
- Imposer au routeur Spoke une authentification via le protocole CHAP (Challenge Handshake Authentication Protocol).
- Préserver la route par défaut, et donc l'accès Internet, du routeur Hub.
- Publier l'adresse IP du serveur DNS à utiliser pour la résolution des noms de domaines.
- Activer l'utilisation des protocoles IPv6CP et IPv6.

Voici une copie du fichier `/etc/ppp/pppoe-server-options` qui contient la liste des paramètres demandés.

```
debug
login
require-chap
nodefaultroute
ms-dns 172.16.16.2
+ipv6
```

Q17. Comment créer les comptes utilisateurs locaux sur le routeur Hub sachant qu'ils ne sont autorisés ni à se connecter ni à avoir un répertoire personnel ?

Consulter les options de la commande adduser.

Voici un exemple de commande adduser.

```
# adduser --disabled-login --no-create-home spoke1
```

Q18. Quels sont les paramètres à donner au lancement de l'outil pppoe-server pour qu'il délivre les adresses aux routeurs Spoke après authentification de ceux-ci ?

Consulter les options de la commande pppoe-server.

Voici un exemple de commande pppoe-server.

```
# pppoe-server -I eth0.26 -C BRAS -L 192.168.1.29 -R 192.168.1.30
```

Q19. Quels sont les résultats obtenus une fois que la session PPP est établie et que les adresses de couche réseau ont été délivrées ?

Consulter les journaux système, la liste des procsessus, l'état des interfaces réseau et de la table de routage.

Attention ! Les résultats ne sont pertinents que si le dialogue avec un routeur Spoke est effectif.

- Consultation des journaux système.

```
pppoe-server[7]: Session 1 created for client e6:92:9d:7a:9a:98 (192.168.1.30) on eth0.26 using Service-Name
pppd[7]: pppd 2.4.7 started by etu, uid 0
pppd[7]: using channel 2
pppd[7]: Using interface ppp0
pppd[7]: Connect: ppp0 <--> /dev/pts/1
pppd[7]: sent [LCP ConfReq id=0x1 <mru 1492> <auth chap MD5> <magic 0x7da53eb6>]
pppd[7]: rcvd [LCP ConfAck id=0x1 <mru 1492> <auth chap MD5> <magic 0x7da53eb6>]
pppd[7]: rcvd [LCP ConfReq id=0x1 <mru 1492> <magic 0xeea2b21a>]
pppd[7]: sent [LCP ConfAck id=0x1 <mru 1492> <magic 0xeea2b21a>]
pppd[7]: sent [LCP EchoReq id=0x0 magic=0x7da53eb6]
pppd[7]: sent [CHAP Challenge id=0xdf <a67ec17d7f16afda88af52b81a1357b506b2260d7f754e>, name = "corellia"]
pppd[7]: rcvd [LCP EchoReq id=0x0 magic=0xeea2b21a]
pppd[7]: sent [LCP EchoRep id=0x0 magic=0x7da53eb6]
pppd[7]: rcvd [LCP EchoRep id=0x0 magic=0xeea2b21a]
pppd[7]: rcvd [CHAP Response id=0xdf <8d36d92d4559ee32aec3383bd725eb4f>, name = "spoke1"]
pppd[7]: sent [CHAP Success id=0xdf "Access granted"]
pppd[7]: Initializing PAM (2) for user spoke1
pppd[7]: ---> PAM INIT Result = 0
pppd[7]: Attempting PAM account checks
pppd[7]: PAM Account OK for spoke1
pppd[7]: PAM Session opened for user spoke1
pppd[7]: user spoke1 logged in on tty  intf ppp0
pppd[7]: local  LL address fe80::85c9:885e:3a4e:02ad
pppd[7]: remote LL address fe80::399d:24c8:9deb:a7b7
pppd[7]: local  IP address 192.168.1.29
pppd[7]: remote IP address 192.168.1.30
```

- Liste des processus.

```
pppoe-server -I eth0.26 -C BRAS -L 192.168.1.29 -R 192.168.1.30
 \_ pppd pty /usr/sbin/pppoe -n -I eth0.26 -e 1:e6:92:9d:7a:9a:98 -S ''
  file /etc/ppp/pppoe-server-options 192.168.1.29:192.168.1.30
  nodetach noaccomp nopcomp default-asyncmap mru 1492 mtu 1492
  \_ /usr/sbin/pppoe -n -I eth0.26 -e 1:e6:92:9d:7a:9a:98 -S
```

- État des interfaces.

```
$ ip addr ls dev eth0.26
5: eth0.26@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 \
   qdisc noqueue state UP group default qlen 1000
    link/ether b8:ca:3a:9e:85:56 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::baca:3aff:fe9e:8556/64 scope link
       valid_lft forever preferred_lft forever

$ ip addr ls dev ppp0
9: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1492 \
   qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 192.168.1.29 peer 192.168.1.30/32 scope global ppp0
       valid_lft forever preferred_lft forever
    inet6 fe80::8478:a29b:3836:8f96/10 scope link
       valid_lft forever preferred_lft forever
```

- Table de routage.

```
$ ip route ls dev ppp0
192.168.1.30 proto kernel scope link src 192.168.1.29
```

4.2. Côté réseau local - LAN

Le routeur Hub doit interconnecter les routeurs Spoke entre eux et donner accès à l'Internet via son interface réseau active sur le VLAN dédié à cet usage.

Ici, on reprend les questions de la Section 3.2, « Communications dans le VLAN Management » avec un changement de numéro de VLAN.

Q20. Comment créer et configurer une sous-interface dédiée au VLAN Internet (numéro 4) ?

Consulter l' Antisèche réseau ou les pages de manuels man ip-link et rechercher les options du type `vlan`.

Voici les différentes instructions.

```
$ sudo ip link add link eth0 name eth0.4 type vlan id 4

$ sudo ip link set dev eth0.4 up

$ sudo ip addr add 172.16.16.59/20 brd + dev eth0.4

$ sudo ip -6 addr add 2001:678:3fc:4::3b/64 dev eth0.4
```

Q21. Comment valider les communciations dans le VLAN Internet (numéro 4) ?

L'hôte voisin le plus intéressant dans le VLAN Internet est le routeur. On vérifie à l'aide de requêtes ICMP que l'on peut le contacter.

Voici un exemple de résultats.

```
$ ping -qc2 172.16.16.2
PING 172.16.16.2 (172.16.16.2) 56(84) bytes of data.

--- 172.16.16.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 13ms
rtt min/avg/max/mdev = 0.634/0.643/0.653/0.027 ms

$ ping -qc2 2001:678:3fc:4::2
PING 2001:678:3fc:4::2(2001:678:3fc:4::2) 56 data bytes

--- 2001:678:3fc:4::2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 28ms
rtt min/avg/max/mdev = 0.628/0.634/0.640/0.006 ms
```

5. Configuration PPPoE d'un routeur Spoke

Dans le scénario défini dans la Section 3, « Topologie Hub & Spoke - Protocole PPPoE », ce routeur ne peut accéder aux autres réseaux que par le routeur Hub. Son interface WAN joue donc le rôle de route par défaut pour le réseau local Branch. Ce genre de routeur est aussi appelé routeur d'extrémité.

5.1. Côté réseau étendu - WAN

Cette partie vient en vis-à-vis de la Section 4.1, « Côté réseaux étendus - WAN » d'un routeur Hub. Le routeur Spoke utilise lui aussi un démon pppd sur le VLAN `Data` pour établir une session PPP avec le routeur Hub. À la différence de ce dernier, il n'est pas à l'initiative du dialogue PPPoE mais il doit être capable de gérer l'encapsulation des trames PPP sur un réseau local Ethernet.

Q22. Comment utiliser l'encapsulation des trames PPP dans Ethernet à partir du démon pppd fourni avec le paquet ppp ?

Rechercher dans le répertoire de documentation du paquet ppp.

Dans le répertoire `/usr/share/doc/ppp/`, on trouve le fichier `README.pppoe` qui indique que l'appel au module `rp-pppoe.so` permet d'encapsuler des trames PPP sur un réseau local Ethernet.

Toujours à partir du même répertoire, on trouve dans la liste des fichiers d'exemples de configuration un modèle adapté à notre contexte : `peers-pppoe`.

Q23. Dans quel fichier sont stockés les paramètres d'identité et d'authentification utilisés par le protocole CHAP ?

Consulter les pages de manuels du démon pppd à la section AUTHENTICATION.

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

Voici un exemple du contenu de ce fichier. Le nom du client ainsi que son mot de passe secret doivent être identiques à chaque extrémité de la session PPP.

```
# Secrets for authentication using CHAP
# client        server  secret                  IP addresses
"spoke1"        *       "5p0k3-1-53cr3t"        *
```

Q24. Quelles sont les options de configuration du démon pppd à placer dans le fichier `/etc/ppp/peers/pppoe-provider` pour assurer l'établissement de la session PPP entre les routeurs ?

Utiliser le fichier exemple PPPoE fourni avec la documentation du paquet ppp.

Voici une copie du fichier `/etc/ppp/peers/pppoe-provider` avec les options correspondant au contexte d'un routeur Spoke.

```
# There should be a matching entry with the password in /etc/ppp/chap-secrets.
user "spoke1"

# Load the PPPoE plugin.
plugin rp-pppoe.so

# Ethernet interface to which the modem is connected.
vlan26

# Assumes that your IP address is allocated dynamically by the ISP.
noipdefault
# Try to get the name server addresses from the ISP.
usepeerdns
# Use this connection as the default route.
defaultroute

# Makes pppd "dial again" when the connection is lost.
persist

# Do not ask the remote to authenticate.
noauth

debug
+ipv6
```

Q25. Comment lancer le démon pppd pour qu'il prenne en compte les paramètres définis dans le fichier complété à la question précédente ?

Consulter les pages de manuels du démon pppd.

C'est l'option `file` qui permet de désigner le fichier de configuration à utiliser. Voici une copie d'écran du lancement de pppd.

```
# pppd file /etc/ppp/peers/pppoe-provider
```

Q26. 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 lors du dialogue PPP fait apparaître des informations suivantes.

```
pppd[18]:  dst e6:92:9d:7a:9a:98  src b8:ca:3a:9e:85:56
pppd[18]:  [service-name]
pppd[18]: PADS: Service-Name: ''
pppd[18]: PPP session is 3
pppd[18]: Connected to b8:ca:3a:9e:85:56 via interface vlan26
pppd[18]: using channel 40
pppd[18]: Using interface ppp0
pppd[18]: Connect: ppp0 <--> vlan26
pppd[18]: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xd9acc3c9>]
pppd[18]: rcvd [LCP ConfReq id=0x1 <mru 1492> <auth chap MD5> <magic 0xf7fb217b>]
pppd[18]: sent [LCP ConfAck id=0x1 <mru 1492> <auth chap MD5> <magic 0xf7fb217b>]
pppd[18]: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xd9acc3c9>]
pppd[18]: rcvd [LCP ConfAck id=0x1 <mru 1492> <magic 0xd9acc3c9>]
pppd[18]: sent [LCP EchoReq id=0x0 magic=0xd9acc3c9]
pppd[18]: rcvd [LCP EchoReq id=0x0 magic=0xf7fb217b]
pppd[18]: sent [LCP EchoRep id=0x0 magic=0xd9acc3c9]
pppd[18]: rcvd [CHAP Challenge id=0x3 <330acf7fa955f3bf549595f45a700c00fe8b7bf934198b>, name = "corellia"]
pppd[18]: sent [CHAP Response id=0x3 <4b3c887e7581087b5d97718f91d1a372>, name = "spoke1"]
pppd[18]: rcvd [LCP EchoRep id=0x0 magic=0xf7fb217b]
pppd[18]: rcvd [CHAP Success id=0x3 "Access granted"]
pppd[18]: CHAP authentication succeeded: Access granted
pppd[18]: CHAP authentication succeeded
pppd[18]: peer from calling number B8:CA:3A:9E:85:56 authorized
pppd[18]: sent [IPCP ConfReq id=0x1 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns2 0.0.0.0>]
pppd[18]: sent [IPV6CP ConfReq id=0x1 <addr fe80::bc5e:a5f6:6402:1a31>]
pppd[18]: rcvd [CCP ConfReq id=0x1 <deflate 15> <deflate(old#) 15> <bsd v1 15>]
pppd[18]: sent [CCP ConfReq id=0x1]
pppd[18]: sent [CCP ConfRej id=0x1 <deflate 15> <deflate(old#) 15> <bsd v1 15>]
pppd[18]: rcvd [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 192.168.1.29>]
pppd[18]: sent [IPCP ConfRej id=0x1 <compress VJ 0f 01>]
pppd[18]: rcvd [IPV6CP ConfReq id=0x1 <addr fe80::34a0:f09f:e323:94be>]
pppd[18]: sent [IPV6CP ConfAck id=0x1 <addr fe80::34a0:f09f:e323:94be>]
pppd[18]: rcvd [IPCP ConfNak id=0x1 <addr 192.168.1.30> <ms-dns1 172.16.16.2> <ms-dns2 172.16.16.2>]
pppd[18]: sent [IPCP ConfReq id=0x2 <addr 192.168.1.30> <ms-dns1 172.16.16.2> <ms-dns2 172.16.16.2>]
pppd[18]: rcvd [IPV6CP ConfAck id=0x1 <addr fe80::bc5e:a5f6:6402:1a31>]
pppd[18]: local  LL address fe80::bc5e:a5f6:6402:1a31
pppd[18]: remote LL address fe80::34a0:f09f:e323:94be
pppd[18]: Script /etc/ppp/ipv6-up started (pid 18817)
pppd[18]: rcvd [CCP ConfAck id=0x1]
pppd[18]: rcvd [CCP ConfReq id=0x2]
pppd[18]: sent [CCP ConfAck id=0x2]
pppd[18]: rcvd [IPCP ConfReq id=0x2 <addr 192.168.1.29>]
pppd[18]: sent [IPCP ConfAck id=0x2 <addr 192.168.1.29>]
pppd[18]: rcvd [IPCP ConfAck id=0x2 <addr 192.168.1.30> <ms-dns1 172.16.16.2> <ms-dns2 172.16.16.2>]
pppd[18]: local  IP address 192.168.1.30
pppd[18]: remote IP address 192.168.1.29
pppd[18]: primary   DNS address 172.16.16.2
pppd[18]: secondary DNS address 172.16.16.2
pppd[18]: Script /etc/ppp/ip-up started (pid 18819)
pppd[18]: Script /etc/ppp/ipv6-up finished (pid 18817), status = 0x0
pppd[18]: Script /etc/ppp/ip-up finished (pid 18819), status = 0x0
```

Q27. 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.

5.2. Côté réseau local - LAN fictif

En théorie, le réseau local d'extrémité desservi par le routeur Spoke suppose l'ajout d'un commutateur et de plusieurs hôtes pour caractériser l'interconnexion des différents réseaux de la topologie étudiée dans ces travaux pratiques. Pour éviter l'utilisation de matériel supplémentaire qui demande des étapes de configuration longues et non pertinentes, on utilise une technique très répandue : les interfaces de boucles locales. Ces interfaces viennent se substituer au réseau local d'extrémité.

L'ajout et la configuration d'une interface de boucle locale provoque l'arrivée d'une nouvelle entrée dans la table de routage du routeur Spoke. Vu des autres réseaux de la topologie, cette technique permet de qualifier le bon fonctionnement d'un service Internet 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.

Q28. 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 de type dummy pour ce genre d'usage. Consulter les pages de manuels ma ip-link pour obtenir la syntaxe de création d'une interface de ce type.

On commence par créer une interface à l'aide de l'instruction suivante.

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

On passe ensuite à la configuration de l'interface `dummy0` comme dans l'exemple qui suit.

```
# ip link set dev dummy0 up
# ip addr add 10.2.6.1/28 brd + dev dummy0
# ip -6 addr add 2001:678:3fc:1a::1/64 dev dummy0
# ip addr ls dev dummy0
7: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 \
   qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether ce:9f:3e:c1:c5:e2 brd ff:ff:ff:ff:ff:ff
    inet 10.2.6.1/28 brd 10.2.6.15 scope global dummy0
       valid_lft forever preferred_lft forever
    inet6 2001:678:3fc:1a::1/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::cc9f:3eff:fec1:c5e2/64 scope link
       valid_lft forever preferred_lft forever
```

Q29. Quelles sont les opérations à effectuer pour installer un service Web en écoute exclusivement sur les adresses IPv4 et IPv6 de l'interface `dummy0` ?

Installer le paquet `lighttpd` et modifier sa configuration pour que le service ne soit accessible que sur les adresses de l'interface `dummy0`.

```
# aptitude install lighttpd
<snipped/>
```

On modifie ensuite le fichier de configuration `/etc/lighttpd/lighttpd.conf` de façon à limiter l'accès aux adresses voulues.

```
# cd /etc/lighttpd/
# diff -uBb lighttpd.conf.orig lighttpd.conf
--- lighttpd.conf.orig  2018-10-07 16:37:55.579183757 +0200
+++ lighttpd.conf       2018-10-07 16:33:31.093675213 +0200
@@ -22,6 +22,9 @@
 compress.filetype           = ( "application/javascript", "text/css", "text/html", "text/plain" )

 # default listening port for IPv6 falls back to the IPv4 port
-include_shell "/usr/share/lighttpd/use-ipv6.pl " + server.port
+#include_shell "/usr/share/lighttpd/use-ipv6.pl " + server.port
 include_shell "/usr/share/lighttpd/create-mime.assign.pl"
 include_shell "/usr/share/lighttpd/include-conf-enabled.pl"
+
+server.bind = "10.2.6.1"
+$SERVER["socket"] == "[2001:678:3fc:1a::1]:80" { server.use-ipv6 = "enable" }
```

On redémarre le service et on affiche la liste des prises réseau ouvertes sur le système pour confirmer que les adresses choisies sont bien prises en compte.

```
# systemctl restart lighttpd

# lsof -i tcp:80
COMMAND    PID     USER   FD   TYPE  DEVICE SIZE/OFF NODE NAME
lighttpd 25745 www-data    4u  IPv4 4990017      0t0  TCP 10.2.6.1:http (LISTEN)
lighttpd 25745 www-data    5u  IPv6 4990018      0t0  TCP [2001:678:3fc:1a::1]:http (LISTEN)
```

Q30. Comment valider l'accès à ce service Web au niveau du routeur Spoke ?

Il s'agit de faire un test au niveau de la couche application. À la console, les deux outils adaptés sont wget et curl.

Voici deux exemples de tests avec wget.

```
$ wget -O /dev/null http://10.2.6.1
--2018-10-07 16:50:16--  http://10.2.6.1/
Connexion à 10.2.6.1:80… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 3378 (3,3K) [text/html]
Sauvegarde en : « /dev/null »

/dev/null    100%[======================>]   3,30K  --.-KB/s    ds 0s

2018-10-07 16:50:16 (267 MB/s) – « /dev/null » sauvegardé [3378/3378]
```

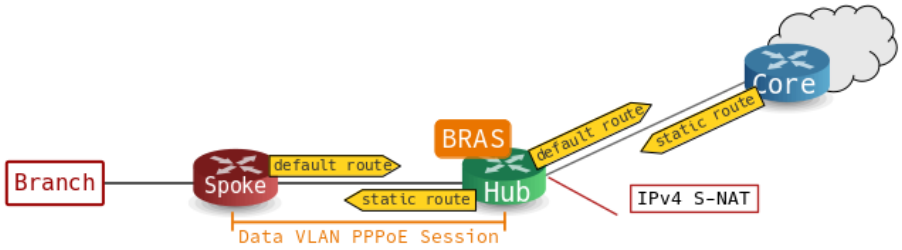
```
$ wget -O /dev/null http://[2001:678:3fc:1a::1]
--2018-10-07 16:51:38--  http://[2001:678:3fc:1a::1]/
Connexion à [2001:678:3fc:1a::1]:80… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 3378 (3,3K) [text/html]
Sauvegarde en : « /dev/null »

/dev/null    100%[======================>]   3,30K  --.-KB/s    ds 0s

2018-10-07 16:51:38 (193 MB/s) – « /dev/null » sauvegardé [3378/3378]
```

6. Interconnexion et routage

En l'absence de routage dynamique, il est nécessaire d'implanter des routes par défaut, des routes statiques et de la traduction d'adresses source sur les routeurs de la topologie étudiée. Dans cette section, on veut s'assurer que les communications entre les différents réseaux fonctionnent correctement.



Interconnexion des différents réseaux

Dans cette partie, on considère que le routage est déjà activé au niveau noyau. Voir Section 3.3, « Activation du routage dans le noyau Linux ».

6.1. Tables de routage du routeur Hub

Selon la représentation simplifiée de la topologie ci-dessus, les tables de routage routeur Hub doivent contenir les éléments suivants.

- Des routes par défaut IPv4 et IPv6 vers le cœur de réseau pour accéder à l'Internet.
- La traduction des adresses IPv4 source en sortie de l'interface de connexion au cœur de réseau.
- Des routes statiques IPv4 et IPv6 vers les réseaux d'extrémité desservis par le routeur Spoke.

Q31. Comment ajouter les routes par défaut vers le cœur de réseau ?

Consulter l' Antisèche réseau ou les pages de manuels man ip-route et rechercher la syntaxe relative aux route par défaut sachant que les adresses de passerelle sont données à la Section 3, « Topologie Hub & Spoke - Protocole PPPoE ».

Pour les réseaux IPv4, la syntaxe est la suivante.

```
# ip route add default via 172.16.16.2
```

```
# ip route ls dev eth0.4
default via 172.16.16.2
172.16.16.0/20 proto kernel scope link src 172.16.16.59
```

```
# ip route get 9.9.9.9
9.9.9.9 via 172.16.16.2 dev eth0.4 src 172.16.16.59 uid 1000
```

Pour les réseaux IPv6, la syntaxe est la suivante.

```
# ip -6 route add default via 2001:678:3fc:4::2
```

```
# ip -6 route ls dev eth0.4
2001:678:3fc:4::/64 proto kernel metric 256 pref medium
fe80::/64 proto kernel metric 256 pref medium
default via 2001:678:3fc:4::2 metric 1024 pref medium
```

```
# ip route get 2620:fe::fe
2620:fe::fe from :: via 2001:678:3fc:4::2 dev eth0.4 src 2001:678:3fc:4::3b metric 1024 pref medium
```

Q32. Comment activer la traduction des adresses source IPv4 des paquets sortant par l'interface située sur le VLAN d'accès au coeur de réseau ?

Consulter les pages de manuels de la commande iptables.

La traduction des adresses source IPv4 s'applique dans la chaîne `POSTROUTING` de la table `nat` et le traitement est appelé `MASQUERADE`. La syntaxe est la suivante.

```
# iptables -t nat -A POSTROUTING -o eth0.4 -j MASQUERADE
```

On vérifie la présence de la règle de traduction d'adresse à l'aide de la commande suivante.

```
# iptables -t nat -vnL POSTROUTING
Chain POSTROUTING (policy ACCEPT 50 packets, 3000 bytes)
 pkts bytes target     prot opt in     out     source               destination
  587 41926 MASQUERADE  all  --  *      eth0.4  0.0.0.0/0            0.0.0.0/0
```

On consulte la table des enregistrements de suivi d'état à l'aide de la commande conntrack fournie avec le paquet du même nom.

```
# conntrack -L | grep icmp
icmp     1 29 src=192.168.1.30 dst=9.9.9.9 type=8 code=0 id=30606 \
   src=9.9.9.9 dst=172.16.16.59 type=0 code=0 id=30606 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 36 flow entries have been shown.
```

Q33. Comment assurer le routage des paquets vers le réseau local d'extrémité Branch desservi par le routeur Spoke ?

Consulter l' Antisèche réseau ou les pages de manuels man ip-route et rechercher la syntaxe relative aux route statiques.

Comme les communications entre les routeurs Hub et Spoke se font via un lien point à point, on peut utiliser directement le nom d'interface pour la prise décision sur l'acheminement des paquets.

Pour le réseau IPv4, la syntaxe est la suivante.

```
# ip route add 10.2.6.0/28 dev ppp0
```

On valide ensuite les communications à destination de l'interface fictive `dummy0` du routeur Spoke depuis le routeur Hub.

```
# ping -qc2 10.2.6.1
PING 10.2.6.1 (10.2.6.1) 56(84) bytes of data.

--- 10.2.6.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 1.043/1.133/1.224/0.096 ms
```

Pour le réseau IPv6, la syntaxe est la suivante.

```
# ip -6 route add 2001:678:3fc:1a::/64 dev ppp0
```

On valide ensuite les communications de la même façon que pour les paquets IPv4.

```
# ping -qc2 2001:678:3fc:1a::1
PING 2001:678:3fc:1a::1(2001:678:3fc:1a::1) 56 data bytes

--- 2001:678:3fc:1a::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 1.186/1.246/1.306/0.060 ms
```

6.2. Tables de routage du routeur Spoke

Selon la représentation simplifiée de la topologie ci-dessus, les tables de routage routeur Spoke ne doivent contenir que des routes par défaut.

Q34. Comment ajouter les routes par défaut vers le routeur Hub ?

Consulter l' Antisèche réseau ou les pages de manuels man ip-route et rechercher la syntaxe relative aux route par défaut.

Comme les communications entre les routeurs Spoke et Hub se font via un lien point à point, on peut utiliser directement le nom d'interface pour la prise décision sur l'acheminement des paquets.

Pour les réseaux IPv4, la syntaxe est la suivante.

```
# ip route add default dev ppp0
```

```
# ip route ls dev ppp0
default scope link
192.168.1.29 proto kernel scope link src 192.168.1.30
```

```
# ip route get 9.9.9.9
9.9.9.9 dev ppp0 src 192.168.1.30 uid 0
```

Pour les réseaux IPv6, la syntaxe est la suivante.

```
# ip -6 route add default dev ppp0
```

```
# ip -6 route ls dev ppp0
none fe80::/10 metric 1 pref medium
fe80::/10 proto kernel metric 256 pref medium
default metric 1024 pref medium
```

```
# ip route get 2620:fe::fe
2620:fe::fe from :: dev ppp0 src 2001:678:3fc:1a::1 metric 1024 pref medium
```

Q35. Comment les routes par défaut sont attribuées vis-à-vis de l'établissement d'une session PPP ?

Consulter les pages de manuels du démon pppd et rechercher dans l'arborescence des scripts de ce même démon, les options ou les commandes de manipulation des routes par défaut.

Pour IPv4, la réponse est fournie par les options du démon pppd paramétrées dans le fichier `/etc/ppp/peers/pppoe-provider`. Ce fichier contient la directive `defaultroute` qui attribue la route par défaut lors de l'établissement de la session PPP.

Pour IPv6, il n'existe pas de paramètre qui permet d'établir la route par défaut avec la session PPP. Il faut donc créer un script qui est appelé lors de l'établissement de session. Le répertoire dédié à ces opérations est nommé `/etc/ppp/ipv6-up.d/`. Voici un exemple de script appelé `/etc/ppp/ipv6-up.d/defaultroute` qui ajoute la route par défaut à chaque nouvelle session.

```
# cat /etc/ppp/ipv6-up.d/defaultroute
#!/bin/sh -e

if [ -z "${CONNECT_TIME}" ]; then
        ip -6 route add default dev ${PPP_IFACE}
fi
```

Attention ! Ce script doit être exécutable.

```
# chmod +x /etc/ppp/ipv6-up.d/defaultroute
```

7. 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.

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.

Fonctions réseau du noyau Linux

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