

Routage inter-VLAN et protocole PPPoE dans un contexte cloud

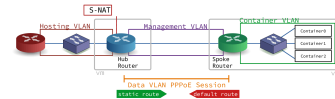
Philippe Latu

philippe.latu(at)inetdoc.net

<https://www.inetdoc.net>

Résumé

L'évolution des réseaux étendus (WAN vers la fibre optique a entraîné un changement radical au niveau de la couche liaison. Le format de trame historique HDLC est remplacé par Ethernet qui devient universel. Le hic, c'est que par définition, Ethernet est un réseau de diffusion. C'est là que le protocole PPPoE intervient. Il permet de passer d'un réseau de diffusion à un fonctionnement point à point caractéristique des réseaux étendus.



Les manipulations présentées dans ces travaux pratiques illustrent l'interconnexion entre réseaux locaux et réseaux étendus dans un contexte de type Cloud IAAS (Infrastructure As A Service).

Table des matières

1. Copyright et Licence	1
1.1. Méta-information	2
1.2. Conventions typographiques	2
2. Interface Ethernet & protocole PPP	3
3. Topologies logiques et virtuelles	4
4. Plan d'adressage	5
5. Raccordement au commutateur de distribution	11
6. Routeur Hub (bleu)	12
6.1. Configuration des interfaces du routeur	12
6.2. Activation de la fonction routage	12
6.3. Activation de la traduction d'adresses	12
6.4. Activation du protocole PPPoE côté réseau étendu	13
6.5. Ajout des routes statiques vers le réseau des conteneurs	14
7. Routeur Spoke (vert)	14
7.1. Configuration des interfaces du routeur	14
7.2. Activation de la fonction routage	15
7.3. Activation du protocole PPP dans le VLAN orange	15
7.4. Activation du commutateur virtuel asw-host	16
7.5. Activation de la configuration IPv6 automatique pour le réseau de conteneurs	16
7.6. Ajout des routes par défaut vers le réseau opérateur	16
7.7. Installation du gestionnaire de conteneurs LXD	17
7.8. Configuration du gestionnaire de conteneurs LXD	17

1. Copyright et Licence

Copyright (c) 2000,2020 Philippe Latu.
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 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) 2000,2020 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 1.3 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

Ce document est écrit avec [DocBook XML](#) sur un système [Debian GNU/Linux](#). Il est disponible en version imprimable au format PDF : [interco.pppoe-cloud.q.pdf](#).

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. 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 ainsi une référence universelle.

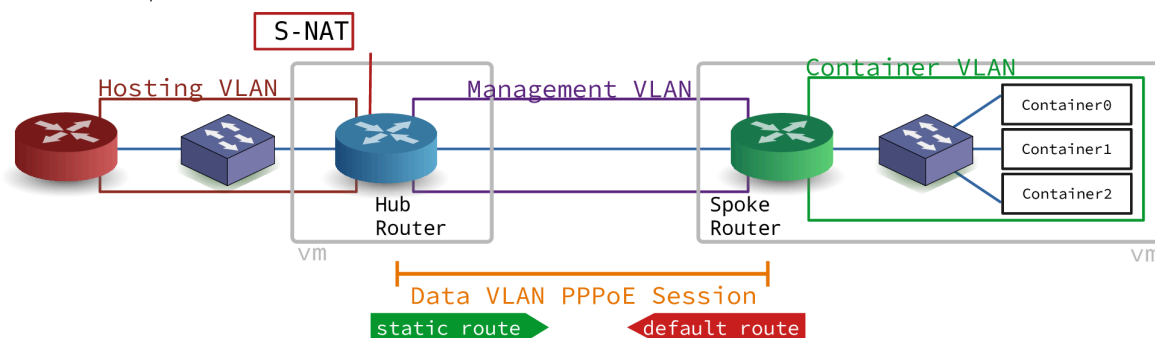
Le protocole PPP offre depuis l'origine une configuration indépendante de la technologie du réseau étendu.

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](#).
- 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](#).
- Q3. Quels sont les autres mécanismes de découverte de voisins connus dans un réseau local Ethernet ?

3. Topologies logiques et virtuelles

La représentation de la topologie logique ci-dessous montre que le routeur de couleur bleue assure l'interconnexion entre un réseau d'infrastructure opérateur appelé Hosting VLAN et un réseau étendu qui dessert un site distant. Ce site distant est représenté par le routeur de couleur verte. Les services hébergés sur le site distant appartiennent au réseau appelé Container VLAN. Sur le réseau étendu on distingue deux autres VLANs : le VLAN violet appelé Management VLAN est utilisé pour la supervision et le VLAN orange Data VLAN est utilisé pour l'acheminement des données du site distant. Ce dernier réseau à la particularité d'utiliser une session PPPoE entre les routeurs bleu et vert. Les deux rectangles en gris "matérialisent" les machines virtuelles qui sont utilisées pour les manipulations.

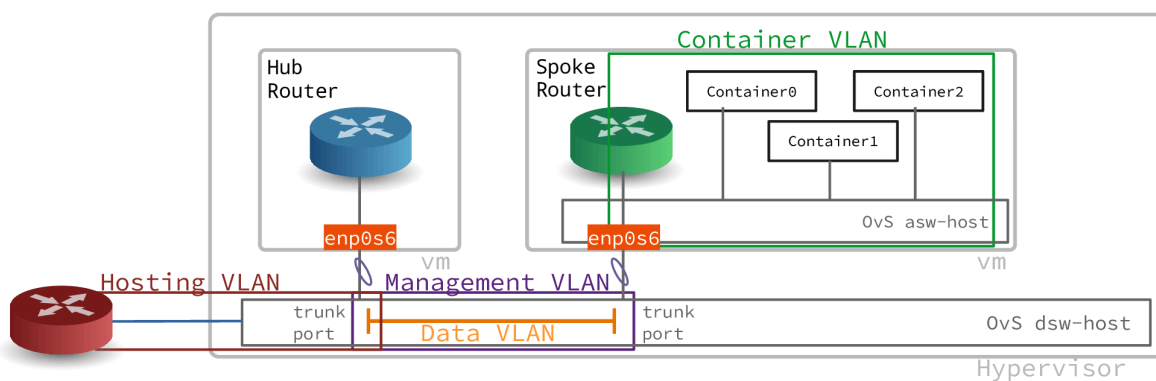


Topologie logique

La représentation de la topologie vue sous l'angle de l'hébergement sur un système hôte hyperviseur montre que le VLAN de couleur verte appelé Container VLAN n'est visible qu'à l'intérieur de la machine virtuelle qui représente le site distant. Ce VLAN est isolé et ses préfixes réseau IPv4 et IPv6 doivent être routés. C'est la raison pour laquelle la machine virtuelle du site distant dispose de son propre commutateur : `asw-host`.

Tous les autres VLANs sont présents sur le commutateur virtuel de couche distribution appelé `dsw-host`. Ce commutateur appartient au système hôte. Il assure le raccordement entre les réseaux physiques et virtualisés. Chacun des routeurs bleu et vert est raccordé avec un lien unique (port en mode trunk) sur lequel le trafic des VLANs doit transiter.

Côté conteneurs, le raccordement au commutateur `asw-host` sera assuré automatiquement par le gestionnaire LXI.



Topologie hébergée

4. Plan d'adressage

Attention ! Les adresses de passerelle côté opérateur (Hosting VLAN de couleur rouge) sont déjà implantées dans l'infrastructure de travaux pratiques tandis que toutes les autres adresses de passerelle sont à implanter sur les routeurs bleu et vert.

Tableau 1. Affectation des numéros de VLANs, des adresses de passerelle et des authentifiants - Groupe 1

Planète	VLAN	Numéro	Type	Adresse
Christophsis	Rouge	-	Passerelle	192.168.37.9/29 2001:678:3fc:133::1/64
	Violet	400	Adresse	fe80:190::1
				fe80:190::2
	Orange	401	Point à point	10.4.1.1:10.4.1.2
			Authentifiants	green_s1 / 5p0k3.1
Vert	10	Passerelle	203.0.113.1/24 fda0:7a62:a::1/64	
Corellia	Rouge	-	Passerelle	172.22.9.33/29 2001:678:3fc:151::1/64
	Violet	402	Adresse	fe80:192::1
				fe80:192::2
	Orange	403	Point à point	10.4.3.1:10.4.3.2
			Authentifiants	green_s2 / 5p0k3.2
Vert	11	Passerelle	203.0.113.1/24 fda0:7a62:b::1/64	
Delaya	Rouge	-	Passerelle	10.31.0.193/26 2001:678:3fc:136::1/64
	Violet	404	Adresse	fe80:194::1
				fe80:194::2
	Orange	405	Point à point	10.4.5.1:10.4.5.2
			Authentifiants	green_s3 / 5p0k3.3
Vert	12	Passerelle	203.0.113.1/24 fda0:7a62:c::1/64	
Kashyyyk	Rouge	-	Passerelle	10.30.5.129/26 2001:678:3fc:131::1/64
	Violet	406	Adresse	fe80:196::1
				fe80:196::2
	Orange	407	Point à point	10.4.7.1:10.4.7.2
			Authentifiants	green_s4 / 5p0k3.4
Vert	13	Passerelle	203.0.113.1/24	

Planète	VLAN	Numéro	Type	Adresse
				fda0:7a62:d::1/64
Korriban	Rouge	-	Passerelle	10.9.10.129/26 2001:678:3fc:14f::1/64
	Violet	408	Adresse	fe80:198::1
				fe80:198::2
	Orange	409	Point à point	10.4.9.1:10.4.9.2
			Authentifiants	green_s5 / 5p0k3.5
Vert	14	Passerelle	203.0.113.1/24 fda0:7a62:e::1/64	
Kessel	Rouge	-	Passerelle	10.30.6.65/28 2001:678:3fc:132::1/64
	Violet	410	Adresse	fe80:19a::1
				fe80:19a::2
	Orange	411	Point à point	10.4.11.1:10.4.11.2
			Authentifiants	green_s6 / 5p0k3.6
Vert	15	Passerelle	203.0.113.1/24 fda0:7a62:f::1/64	
Mygeeto	Rouge	-	Passerelle	10.9.15.17/29 2001:678:3fc:150::1/64
	Violet	412	Adresse	fe80:19c::1
				fe80:19c::2
	Orange	413	Point à point	10.4.13.1:10.4.13.2
			Authentifiants	green_s7 / 5p0k3.7
Vert	16	Passerelle	203.0.113.1/24 fda0:7a62:10::1/64	
Nelvaan	Rouge	-	Passerelle	10.31.1.145/28 2001:678:3fc:137::1/64
	Violet	414	Adresse	fe80:19e::1
				fe80:19e::2
	Orange	415	Point à point	10.4.15.1:10.4.15.2
			Authentifiants	green_s8 / 5p0k3.8
Vert	17	Passerelle	203.0.113.1/24 fda0:7a62:11::1/64	
Rattatak	Rouge	-	Passerelle	192.168.10.81/28 2001:678:3fc:145::1/64

Planète	VLAN	Numéro	Type	Adresse
	Violet	416	Adresse	fe80:1a0::1
				fe80:1a0::2
	Orange	417	Point à point	10.4.17.1:10.4.17.2
			Authentifiants	green_s9 / 5p0k3.9
Vert	18	Passerelle	203.0.113.1/24 fda0:7a62:12::1/64	
Saleucami	Rouge	-	Passerelle	192.168.12.17/29 2001:678:3fc:138::1/64
	Violet	418	Adresse	fe80:1a2::1
				fe80:1a2::2
	Orange	419	Point à point	10.4.19.1:10.4.19.2
Authentifiants			green_s10 / 5p0k3.10	
Vert	19	Passerelle	203.0.113.1/24 fda0:7a62:13::1/64	
Taris	Rouge	-	Passerelle	10.8.11.9/29 2001:678:3fc:14b::1/64
	Violet	420	Adresse	fe80:1a4::1
				fe80:1a4::2
	Orange	421	Point à point	10.4.21.1:10.4.21.2
Authentifiants			green_s11 / 5p0k3.11	
Vert	20	Passerelle	203.0.113.1/24 fda0:7a62:14::1/64	
Teth	Rouge	-	Passerelle	10.0.10.33/27 2001:678:3fc:13c::1/64
	Violet	422	Adresse	fe80:1a6::1
				fe80:1a6::2
	Orange	423	Point à point	10.4.23.1:10.4.23.2
Authentifiants			green_s12 / 5p0k3.12	
Vert	21	Passerelle	203.0.113.1/24 fda0:7a62:15::1/64	
Utapau	Rouge	-	Passerelle	172.21.12.17/29 2001:678:3fc:14c::1/64
	Violet	424	Adresse	fe80:1a8::1
				fe80:1a8::2
Orange	425	Point à point	10.4.25.1:10.4.25.2	

Planète	VLAN	Numéro	Type	Adresse
			Authentifiants	green_s13 / 5p0k3.13
	Vert	22	Passerelle	203.0.113.1/24 fda0:7a62:16::1/64
Yavin	Rouge	-	Passerelle	172.19.9.65/26 2001:678:3fc:13b::1/64
	Violet	426	Adresse	fe80:1aa::1
				fe80:1aa::2
	Orange	427	Point à point	10.4.27.1:10.4.27.2
			Authentifiants	green_s14 / 5p0k3.14
Vert	23	Passerelle	203.0.113.1/24 fda0:7a62:17::1/64	

Tableau 2. Affectation des numéros de VLANs, des adresses de passerelle et des authentifiants - Groupe 2

Planète	VLAN	Numéro	Type	Adresse
Alderaan	Rouge	-	Passerelle	172.17.64.129/25 2001:678:3fc:64::1/64
	Violet	220	Adresse	fe80:dc::1
				fe80:dc::2
	Orange	221	Point à point	10.2.21.1:10.2.21.2
			Authentifiants	green_s20 / 5p0k3.20
Vert	24	Passerelle	203.0.113.1/24 fda0:7a62:18::1/64	
Bespín	Rouge	-	Passerelle	172.20.135.65/28 2001:678:3fc:87::1/64
	Violet	222	Adresse	fe80:de::1
				fe80:de::2
	Orange	223	Point à point	10.2.23.1:10.2.23.2
			Authentifiants	green_s21 / 5p0k3.21
Vert	25	Passerelle	203.0.113.1/24 fda0:7a62:19::1/64	
Centares	Rouge	-	Passerelle	172.18.4.1/22 2001:678:3fc:65::1/64
	Violet	224	Adresse	fe80:e0::1
				fe80:e0::2
	Orange	225	Point à point	10.2.25.1:10.2.25.2
Authentifiants			green_s22 / 5p0k3.22	

Planète	VLAN	Numéro	Type	Adresse
	Vert	26	Passerelle	203.0.113.1/24 fda0:7a62:1a::1/64
Coruscant	Rouge	-	Passerelle	172.20.136.81/28 2001:678:3fc:88::1/64
	Violet	226	Adresse	fe80:e2::1
				fe80:e2::2
	Orange	227	Point à point	10.2.27.1:10.2.27.2
Authentifiants			green_s23 / 5p0k3.23	
	Vert	27	Passerelle	203.0.113.1/24 fda0:7a62:1b::1/64
Dagobah	Rouge	-	Passerelle	10.3.2.1/23 2001:678:3fc:66::1/64
	Violet	228	Adresse	fe80:e4::1
				fe80:e4::2
	Orange	229	Point à point	10.2.29.1:10.2.29.2
Authentifiants			green_s24 / 5p0k3.24	
	Vert	28	Passerelle	203.0.113.1/24 fda0:7a62:1c::1/64
Endor	Rouge	-	Passerelle	172.24.132.17/28 2001:678:3fc:84::1/64
	Violet	230	Adresse	fe80:e6::1
				fe80:e6::2
	Orange	231	Point à point	10.2.31.1:10.2.31.2
Authentifiants			green_s25 / 5p0k3.25	
	Vert	29	Passerelle	203.0.113.1/24 fda0:7a62:1d::1/64
Felucia	Rouge	-	Passerelle	10.6.8.1/23 2001:678:3fc:69::1/64
	Violet	232	Adresse	fe80:e8::1
				fe80:e8::2
	Orange	233	Point à point	10.2.33.1:10.2.33.2
Authentifiants			green_s26 / 5p0k3.26	
	Vert	30	Passerelle	203.0.113.1/24 fda0:7a62:1e::1/64
Geonosis	Rouge	-	Passerelle	172.20.131.33/29 2001:678:3fc:83::1/64

Planète	VLAN	Numéro	Type	Adresse
	Violet	234	Adresse	fe80:ea::1
				fe80:ea::2
	Orange	235	Point à point	10.2.35.1:10.2.35.2
			Authentifiants	green_s27 / 5p0k3.27
Vert	31	Passerelle	203.0.113.1/24 fda0:7a62:1f::1/64	
Hoth	Rouge	-	Passerelle	10.7.10.1/23 2001:678:3fc:6a::1/64
	Violet	236	Adresse	fe80:ec::1
				fe80:ec::2
	Orange	237	Point à point	10.2.37.1:10.2.37.2
Authentifiants			green_s28 / 5p0k3.28	
Vert	32	Passerelle	203.0.113.1/24 fda0:7a62:20::1/64	
Jakku	Rouge	-	Passerelle	172.20.130.25/29 2001:678:3fc:82::1/64
	Violet	238	Adresse	fe80:ee::1
				fe80:ee::2
	Orange	239	Point à point	10.2.39.1:10.2.39.2
Authentifiants			green_s29 / 5p0k3.29	
Vert	33	Passerelle	203.0.113.1/24 fda0:7a62:21::1/64	
Kamino	Rouge	-	Passerelle	192.168.107.1/25 2001:678:3fc:6b::1/64
	Violet	240	Adresse	fe80:f0::1
				fe80:f0::2
	Orange	241	Point à point	10.2.41.1:10.2.41.2
Authentifiants			green_s30 / 5p0k3.30	
Vert	34	Passerelle	203.0.113.1/24 fda0:7a62:22::1/64	
Mustafar	Rouge	-	Passerelle	192.168.110.129/25 2001:678:3fc:6e::1/64
	Violet	242	Adresse	fe80:f2::1
				fe80:f2::2
Orange	243	Point à point	10.2.43.1:10.2.43.2	

Planète	VLAN	Numéro	Type	Adresse
			Authentifiants	green_s31 / 5p0k3.31
	Vert	35	Passerelle	203.0.113.1/24 fda0:7a62:25::1/64
Naboo	Rouge	-	Passerelle	192.168.122.1/28 2001:678:3fc:7a::1/64
	Violet	244	Adresse	fe80:f4::1
				fe80:f4::2
	Orange	245	Point à point	10.2.45.1:10.2.45.2
Authentifiants			green_s32 / 5p0k3.32	
Vert	36	Passerelle	203.0.113.1/24 fda0:7a62:26::1/64	
Tatooine	Rouge	-	Passerelle	172.19.115.193/26 2001:678:3fc:73::1/64
	Violet	246	Adresse	fe80:f6::1
				fe80:f6::2
	Orange	247	Point à point	10.2.47.1:10.2.47.2
Authentifiants			green_s33 / 5p0k3.33	
Vert	37	Passerelle	203.0.113.1/24 fda0:7a62:27::1/64	

Voici le plan d'adressage utilisé pour la maquette qui sert à la rédaction de ce support de travaux pratiques.

Tableau 3. Affectation des numéros de VLANs, des adresses de passerelle et des authentifiants

Planète	VLAN	Numéro	Type	Adresse
Maquette	Rouge	300	Passerelle	10.141.0.161/27 2001:678:3fc:12c::1/64
	Violet	430	Adresse	fe80:1ae::1
				fe80:1ae::2
	Orange	431	Point à point	10.4.31.1:10.4.31.2
Authentifiants			etu / 5p0k3	
Vert	40	Passerelle	203.0.113.1/24 fda0:7a62:28::1/64	

5. Raccordement au commutateur de distribution

Dans cette section, on étudie le raccordement des deux machines virtuelles au commutateur de distribution sur le système hôte.

- Q4. Comment contrôler la configuration des ports du commutateur de distribution sur le système hôte ?
- Q5. Comment contrôler le numéro de VLAN attribué au port en mode accès du commutateur de distribution sur le système hôte ?

- Q6. Comment affecter le numéro de VLAN attribué au port en mode accès du commutateur de distribution sur le système hôte ?
- Q7. Comment s'assurer que le port du commutateur est bien configuré à chaque nouveau lancement de machine virtuelle ?

6. Routeur Hub (bleu)

Dans cette section, on étudie la machine virtuelle qui joue le rôle de routeur entre le réseau opérateur et le réseau étendu qui dessert le site distant.

6.1. Configuration des interfaces du routeur

Une fois la machine virtuelle routeur lancée, les premières étapes consistent à lui attribuer un nouveau nom et à configurer les interfaces réseau pour joindre les hôtes voisins.

- Q8. Comment changer le nom de la machine virtuelle ?
- Q9. Comment appliquer les configurations réseau IPv4 et IPv6 à partir de l'unique interface du routeur ?
Consulter les pages de manuels du fichier de configuration système à l'aide de la commande `man interfaces`.
- Q10. Quels sont les tests de connectivité réalisables après application de la nouvelle configuration des interfaces réseau ?
Relever l'état des trois interfaces et procédez aux tests en respectant les couches de la modélisation.

6.2. Activation de la fonction routage

Sans modification de la configuration par défaut, un système GNU/Linux n'assure pas la fonction de routage du trafic d'une interface réseau à une autre.

L'activation du routage correspond à un réglage de paramètres du sous-système réseau du noyau Linux. L'outil qui permet de consulter et modifier les réglages de paramètre sur le noyau est appelé `sysctl`. Son fichier de configuration principal est `/etc/sysctl.conf`.

- Q11. Comment activer le routage dans le sous-système réseau du noyau Linux ?
Utiliser la commande `sysctl` pour effectuer des recherches et identifier les paramètres utiles. Par exemple :

```
$ sudo sysctl -a -r ".*forward.*"
```


Le fichier `/etc/sysctl.conf` contient des commentaires qui guident facilement vers les bons paramètres.
Attention ! Il ne faut pas oublier d'appliquer les nouvelles valeurs des paramètres de configuration.
- Q12. Quelles sont les conditions à réunir pour tester le fonctionnement du routage ?
Rechercher comment utiliser l'analyseur réseau `tshark` pour caractériser l'acheminement du trafic d'un réseau à l'autre.

6.3. Activation de la traduction d'adresses

Le résultat de la question ci-dessus montre que les hôtes situés dans le réseau des conteneurs ne peuvent pas joindre l'Internet puisque les préfixes réseau utilisés ont une portée limitée.

- Q13. Quels sont les paquets qui fournissent les outils de gestion de la traduction d'adresses ?
Rechercher les paquets relatifs au filtrage et à la gestion des règles de pare-feux.
- Q14. Quelles sont les règles à appliquer pour assurer une traduction des adresses sources en sortie sur le réseau hébergement ?
Rechercher dans les pages de manuel de la commande `iptables`.
- Q15. Comment caractériser le fonctionnement de la traduction d'adresses sources ?

Rechercher dans les pages de manuel de la commande iptables les options d'affichage du décompte du trafic traité.

6.4. Activation du protocole PPPoE côté réseau étendu

Pour acheminer le trafic depuis et vers le site distant, il est nécessaire de passer par une authentification. Cette fonction est assurée à l'aide du protocole PPPoE.

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 bleu doit exiger que le routeur vert s'authentifie auprès de lui avant de délivrer les adresses de couche réseau.

Q16. Quel paquet spécifique à la gestion du dialogue PPPoE à installer sur le routeur Hub ?

Rechercher dans le catalogue des paquets, la référence pppoe.

Q17. 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.

Q18. 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](#).

Q19. 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.

Q20. 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.

Q21. 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.

Q22. 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 vert. 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 vert une authentification via le protocole CHAP (Challenge Handshake Authentication Protocol).
- Préserver la route par défaut, et donc l'accès Internet, du routeur bleu.
- Publier l'adresse IP du serveur DNS à utiliser pour la résolution des noms de domaines.
- Activer l'utilisation des protocoles IPv6CP et IPv6.

Q23. Comment créer le compte utilisateur local sur le routeur bleu sachant qu'il n'est autorisé ni à se connecter ni à avoir un répertoire personnel ?

Consulter les options de la commande `adduser`.

- Q24. Quels sont les paramètres à donner au lancement de l'outil `pppoe-server` pour qu'il délivre les adresses au routeur vert après authentification de celui-ci ?

Consulter les options de la commande `pppoe-server`.

- Q25. 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 processus, l'état des interfaces réseau et de la table de routage.

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

- Q26. Quelles sont les modifications à apporter au fichier de configuration système des interfaces réseau pour que l'ouverture de session PPP soit disponible après chaque réinitialisation ?

Consulter les pages de manuel du fichier `/etc/network/interfaces` : `man interfaces`.

6.5. Ajout des routes statiques vers le réseau des conteneurs

Pour joindre le réseau des conteneurs situé au delà du routeur vert, il est nécessaire d'ajouter une route statique pour chaque protocole de la couche réseau IPv4 et IPv6. Le choix du routage statique est justifié par le fait que l'on adresse un site distant d'extrémité via un lien unique.

Attention ! Les tests de connectivité vers le réseau des conteneurs supposent que ces conteneurs soient actifs et correctement configurés. Voici un exemple d'information sur l'état des conteneurs sur le site distant.

```
etu@vert:~$ lxc ls
```

NAME	STATE	IPV4	IPV6	TYPE	SNAPSHOTS
container0	RUNNING	203.0.113.10 (eth0)	fda0:7a62:28:0:216:3eff:feda:e1a (eth0)	CONTAINER	0
container1	RUNNING	203.0.113.11 (eth0)	fda0:7a62:28:0:216:3eff:fec4:d325 (eth0)	CONTAINER	0
container2	RUNNING	203.0.113.12 (eth0)	fda0:7a62:28:0:216:3eff:fe66:86fb (eth0)	CONTAINER	0

On peut aussi s'assurer que les tables de routage du routeur vert désignent bien le routeur bleu comme passerelle vers tous les autres réseaux.

```
etu@bleu:~$ ssh fe80:1ae::2%enp0s6.430 "ip route ls default"
default dev ppp0 scope link
etu@bleu:~$ ssh fe80:1ae::2%enp0s6.430 "ip -6 route ls default"
default dev ppp0 metric 1024 pref medium
```

- Q27. Comment ajouter manuellement les routes IPv4 et IPv6 vers le réseau desservi par le routeur vert ?

Consulter les pages de manuel sur le routage avec la commande : `man ip-route`.

- Q28. Quels sont les tests de connectivité qui permettent valider la communication à destination des conteneurs du réseau distant ?

Collecter les adresses IPv4 et IPv6 des conteneurs avant de lancer des requêtes ICMP.

- Q29. Comment appliquer ces routes statiques dans la configuration système pour qu'elles soient activées à chaque établissement de session PPP ?

Il faut parcourir l'arborescence du répertoire `/etc/ppp/` pour repérer les scripts exécutés lors de l'ouverture de session. Créer un script pour chaque protocole de couche réseau qui ajoute la route statique voulue.

7. Routeur Spoke (vert)

7.1. Configuration des interfaces du routeur

Une fois la machine virtuelle serveur de conteneurs lancée, les premières étapes consistent à lui attribuer un nouveau nom et à configurer les interfaces réseau pour joindre le routeur voisin et l'Internet.

Q30. Comment changer le nom de la machine virtuelle ?

Q31. Comment appliquer la configuration réseau IPv4 et IPv6 de l'interface du serveur ?

Consulter les pages de manuels du fichier de configuration système à l'aide de la commande `man interfaces`.

7.2. Activation de la fonction routage

Sans modification de la configuration par défaut, un système GNU/Linux n'assure pas la fonction de routage du trafic d'une interface réseau à une autre.

L'activation du routage correspond à un réglage de paramètres du sous-système réseau du noyau Linux. L'outil qui permet de consulter et modifier les réglages de paramètre sur le noyau est appelé `sysctl`. Son fichier de configuration principal est `/etc/sysctl.conf`.

Q32. Comment activer le routage dans le sous-système réseau du noyau Linux ?

Utiliser la commande `sysctl` pour effectuer des recherches et identifier les paramètres utiles. Par exemple :

```
$ sudo sysctl -a -r ".*forward.*"
```

Le fichier `/etc/sysctl.conf` contient des commentaires qui guident facilement vers les bons paramètres.

Attention ! Il ne faut pas oublier d'appliquer les nouvelles valeurs des paramètres de configuration.

7.3. Activation du protocole PPP dans le VLAN orange

Le routeur vert utilise un démon `pppd` sur le VLAN `data` pour établir une session PPP avec le routeur bleu. 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.

Q33. Quel paquet fournit le démon de gestion des sessions du protocole PPP sur le routeur vert ?

Rechercher dans le catalogue des paquets, la référence `ppp`.

Q34. 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`.

Q35. 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.

Q36. 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`.

Q37. 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`.

Q38. 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](#).

Q39. 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.

Q40. Quelles sont les modifications à apporter au fichier système de configuration des interfaces réseau pour ouvrir la session PPP à chaque réinitialisation système ?

Consulter les pages de manuel du fichier `/etc/network/interfaces` : `man interfaces`.

7.4. Activation du commutateur virtuel `asw-host`

Dans le scénario étudié, les services sont hébergés dans un réseau de conteneurs propre au routeur vert. La mise en œuvre de cette configuration passe par l'installation d'un commutateur virtuel appelé `asw-host`. On utilise Open vSwitch pour configurer ce commutateur.

- Q41. Quel est le paquet à installer pour pouvoir ajouter un commutateur virtuel au routeur vert ?
Rechercher le mot clé `openvswitch` dans la liste des paquets.
- Q42. Quel est le fichier de documentation qui fournit les directives de configuration d'un commutateur intégré au fichier système `/etc/network/interfaces` ?
Rechercher dans la liste des fichiers des paquets installés à la question précédente.
- Q43. Quelles sont les modifications à apporter au fichier `/etc/network/interfaces` pour configurer le commutateur `asw-host` ?

7.5. Activation de la configuration IPv6 automatique pour le réseau de conteneurs

Pour que les hôtes du réseau de conteneurs obtiennent automatiquement une configuration IPv6, il faut que le routeur assure les annonces auprès de ces voisins. Un moyen simple pour assurer la configuration SLAAC des hôtes voisins du routeur consiste à utiliser le paquet `radvd`.

On débute par l'installation de ce paquet.

```
$ sudo apt install radvd
...
Préparation du dépaquetage de .../radvd_1%3a2.17-2+b1_amd64.deb ...
Dépaquetage de radvd (1:2.17-2+b1) ...
Paramétrage de radvd (1:2.17-2+b1) ...
Job for radvd.service failed because the control process exited with error code.
See "systemctl status radvd.service" and "journalctl -xe" for details.
invoke-rc.d: initscript radvd, action "start" failed.
● radvd.service - Router advertisement daemon for IPv6
   Loaded: loaded (/lib/systemd/system/radvd.service; disabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Sun 2020-09-13 22:32:10 CEST; 17ms ago
     Docs: man:radvd(8)
   Process: 2814 ExecStartPre=/usr/sbin/radvd --logmethod stderr_clean --configtest (code=exited, status=1/FAILURE)
```

On voit que le lancement du service a échoué.

- Q44. Comment configurer le service `radvd` pour publier les annonces côté conteneurs ?
Rechercher les options utiles dans les pages de manuel du service : `man radvd.conf`.

7.6. Ajout des routes par défaut vers le réseau opérateur

Pour joindre l'Internet situé au delà du routeur bleu, il est nécessaire d'ajouter une route par défaut pour chaque protocole de la couche réseau : IPv4 et IPv6.

Attention ! Les tests de connectivité vers l'Internet supposent que le routeur bleu soit fonctionnel.

- Q45. Comment ajouter manuellement les routes par défaut IPv4 et IPv6 vers le routeur bleu ?
Consulter les pages de manuel sur le routage avec la commande : `man ip-route`.
- Q46. Quels sont les tests de connectivité qui permettent valider la communication vers l'Internet en passant par le routeur bleu ?
Au niveau de la couche réseau, on lance les requêtes ICMP classques.
- Q47. Comment appliquer ces routes statiques dans la configuration système pour qu'elles soient activées à chaque établissement de session PPP ?
Il faut parcourir l'arborescence du répertoire `/etc/ppp/` pour repérer les scripts exécutés lors de l'ouverture de session. Créer un script pour chaque protocole de couche réseau qui ajoute la route statique voulue.

7.7. Installation du gestionnaire de conteneurs LXD

Sur le routeur vert, la gestion des conteneurs est confiée à LXD. Pour des raisons de rapidité de mise en œuvre, on choisit de passer par le gestionnaire de paquets snapd pour l'installation des outils.

- Q48. Comment installer le gestionnaire de paquets snap sur une distribution Debian GNU/Linux ?
Effectuer une recherche dans les paquets fournis via APT.
- Q49. Comment installer le gestionnaire de conteneurs LXD ?
Rechercher dans la liste des snaps.
- Q50. Comment faire pour que l'utilisateur normal `etu` ait la capacité à gérer les conteneurs ?
Rechercher le nom du groupe système correspondant à l'utilisation des outils LXD.

7.8. Configuration du gestionnaire de conteneurs LXD

- Q51. Quelle est l'instruction de configuration initiale du gestionnaire LXD ?
Utiliser l'aide de la commande `lxd`.
- Q52. Comment changer le type de raccordement défini par le paramètre `nictype` de `macvlan` à `bridged` ?
Rechercher dans les options d'édition des paramètres du profil avec la commande `lxc`.
- Q53. Quelle est l'instruction qui permet d'afficher le profil par défaut des conteneur ?
Rechercher dans les options de la commande `lxc`.
- Q54. Quelle est l'instruction de lancement d'un conteneur ?
Rechercher dans les options de la commande `lxc`.
Tester son exécution avec un conteneur de type `debian/bullseye`.
- Q55. Comment appliquer une configuration IPv4 statique à chaque conteneur ?
Identifier le fichier de configuration système et modifier ce fichier pour chaque conteneur