

Résumé

L'objectif de cette étude de cas est de faire la synthèse sur l'ensemble du cycle de travaux pratiques sur le thème de l'interconnexion réseau LAN/WAN. Côté réseaux étendus, on retrouve la configuration des accès via PPP sur trames «HDLC synchrones» (RNIS) et le filtrage avec et sans traduction d'adresses. Côté réseaux locaux, on reprend le routage inter-VLAN avec le protocole de routage dynamique OSPF.

Table des matières

1. Copyright et Licence	1
2. Topologies réseaux	2
3. Plan d'adressage WAN	3
4. Plan d'adressage LAN	6
5. Interconnexion avec deux routeurs de bordure OSPF	9

1. Copyright et Licence

Copyright (c) 2000,2021 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".

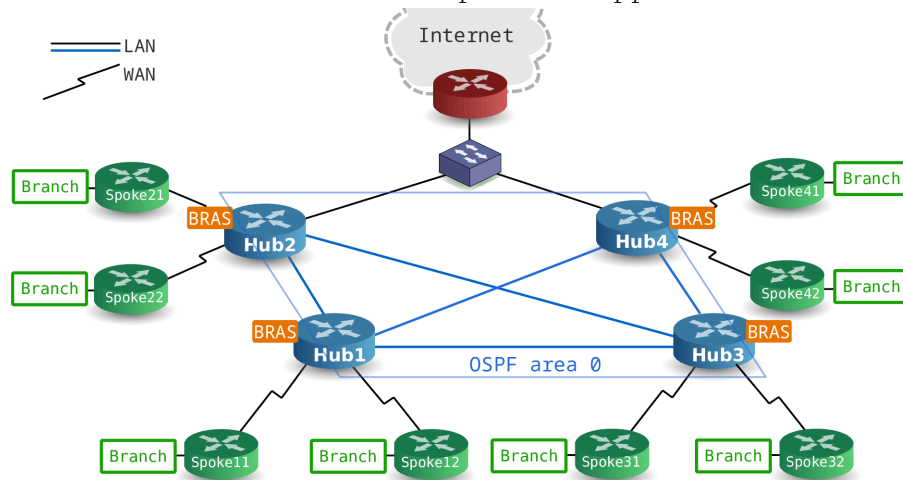
Copyright (c) 2000,2021 Philippe Latu.
Permission est accordée de copier, distribuer et/ou modifier ce document selon les termes de la Licence de Documentation Libre GNU (GNU Free Documentation License), version 1.3 ou toute version ultérieure publiée par la Free Software Foundation ; sans Sections Invariables ; 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 ».

Méta-information

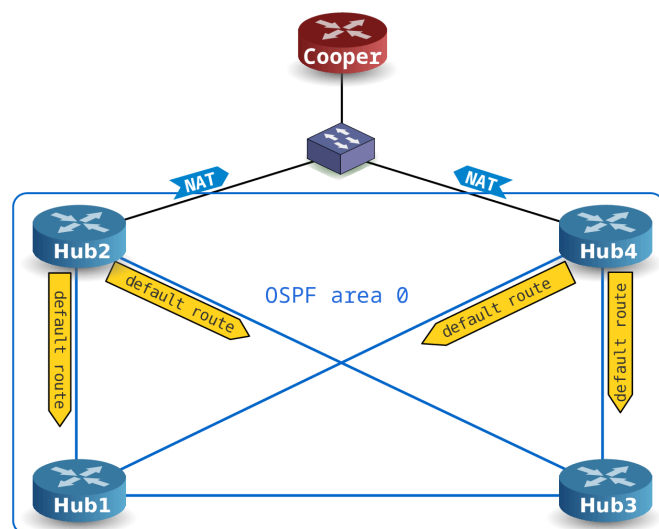
Ce document est écrit avec [DocBook XML](#) sur un système [Debian GNU/Linux](#). Il est disponible en version imprimable au format PDF : [interco-dsl.cs.pdf](#).

2. Topologies réseaux

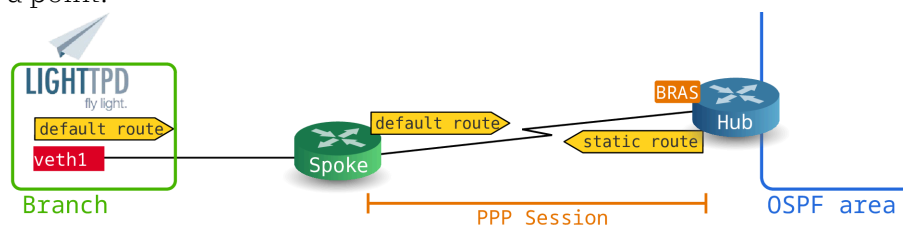
La topologie logique globale se présente comme une associations de topologies triangulaires LAN et WAN. L'ensemble des routeurs présentés appartient à une seule aire OSPF.



Les deux sous topologies LAN reprennent l'architecture étudiée dans le support **Routage dynamique avec OSPF (Bird)**. La seule particularité ici réside dans la redondance de deux VLANs entre les routeurs Hub2 et Hub3.



Les quatre sous topologies WAN reprennent l'architecture étudiée dans les supports **Topologie Hub & Spoke avec le protocole PPP** ou **Topologie Hub & Spoke avec le protocole PPPoE**. La différence ici réside dans l'utilisation du protocole de routage dynamique OSPF sur des les liens WAN point à point.



L'objectif de cette séance de travaux pratiques est d'aboutir à un accès aux services Web hébergés sur les réseaux fictifs depuis un routeur Spoke vers n'importe quel autre routeur Spoke sans recourir une seule fois à la traduction d'adresses.

3. Plan d'adressage WAN

Les connexions RNIS des routeurs Hubs se font directement sur les ports de l'autocommutateur RNIS sachant que ces connexions utilisent les deux canaux B d'un port de type BRI.

Un routeur Spoke doit s'authentifier auprès d'un routeur Hub via le protocole PPP avec la méthode CHAP.

Un routeur Spoke doit aussi mettre en place un réseau fictif qui héberge un service Web dans un espace de noms réseau dédié.

Tableau 1. Salle 211 - Affectation des rôles, des numéros de VLANs et des adresses IP

Groupe	Poste	Rôle	VLAN	Flux	Réseau/Authentification
1	christophsis	Hub1	400	Management	fe80:190::1/64
			401	Data	192.168.1.141:192.168.1.142
			402	Data	192.168.1.145:192.168.1.146
	coreellia	Spoke11	400	Management	fe80:190::11/64
			401	Data	etu_s1 / Sp0k3.1
				Branch	10.4.0.1/26
					2001:678:3fc:191::1/64
	delaya	Spoke12	400	Management	fe80:190::12/64
			402	Data	etu_s2 / Sp0k3.2
				Branch	10.4.0.65/26
					2001:678:3fc:192::1/64
	2	kashyyyk	Hub2	405	Management
406				Data	192.168.1.149:192.168.1.150
407				Data	192.168.1.153:192.168.1.154
korriban		Spoke21	405	Management	fe80:195::21/64
			406	Data	etu_s1 / Sp0k3.1
				Branch	10.4.0.129/26
					2001:678:3fc:196::1/64
kessel		Spoke22	405	Management	fe80:195::22/64
			407	Data	etu_s2 / Sp0k3.2
				Branch	10.4.0.193/26
					2001:678:3fc:197::1/64
3		mygeeto	Hub3	410	Management
	411			Data	192.168.1.157:192.168.1.158
	412			Data	192.168.1.161:192.168.1.162
	nelvaan	Spoke31	410	Management	fe80:19a::31/64
			411	Data	etu_s1 / Sp0k3.1

Groupe	Poste	Rôle	VLAN	Flux	Réseau/Authentification	
	rattatak	Spoke32		Branch	10.4.1.1/26	
					2001:678:3fc:19b::1/64	
			410	Management	fe80:19a::32/64	
			412	Data	etu_s2 / Sp0k3.2	
				Branch	10.4.1.65/26	
					2001:678:3fc:19c::1/64	
	4	saleucami	Hub4	415	Management	fe80:19f::4/64
				416	Data	192.168.1.165:192.168.1.166
417				Data	192.168.1.169:192.168.1.170	
taris		Spoke41	415	Management	fe80:19f::41/64	
			416	Data	etu_s1 / Sp0k3.1	
				Branch	10.4.1.129/26	
					2001:678:3fc:1a0::1/64	
teth		Spoke42	415	Management	fe80:19f::42/64	
			417	Data	etu_s2 / Sp0k3.2	
				Branch	10.4.1.193/26	
					2001:678:3fc:1a1::1/64	

Tableau 2. Salle 213 - Affectation des rôles, des numéros de bus S0 et des adresses IP

Group	Poste	Rôle	Bus S0	N° Tél.	Interface	Réseau/Authentification
1	alderaan	Hub1	S0.1	104	ipp0	192.168.104.1:192.168.104.2
			S0.1	105	ipp01	192.168.105.1:192.168.105.2
	bespin	Spoke11	S0.2	106	ipp0	etu_s11 / Sp0k3.11
					veth0:veth1	10.106.0.1/30:10.106.0.2/30
centares	Spoke12	S0.2	107	ipp0	etu_s12 / Sp0k3.12	
				veth0:veth1	10.107.0.1/30:10.107.0.2/30	
2	coruscant	Hub2	S0.3	108	ipp0	192.168.107.1:192.168.107.2
			S0.3	109	ipp01	192.168.108.1:192.168.108.2
	dagobah	Spoke21	S0.4	110	ipp0	etu_s21 / Sp0k3.21
					veth0:veth1	10.110.0.1/30:10.110.0.2/30
	endor	Spoke22	S0.4	111	ipp0	etu_s22 / Sp0k3.22
					veth0:veth1	10.111.0.1/30:10.111.0.2/30
3	felucia	Hub3	S0.5	112	ipp0	192.168.111.1:192.168.111.2

Group	Poste	Rôle	Bus SO	N° Tél.	Interface	Réseau/Authentification
			S0.5	113	ipp1	192.168.112.1:192.168.112.2
	geonosis	Spoke31	S0.6	114	ipp0	etu_s31 / Sp0k3.31
					veth0:veth1	10.114.0.1/30:10.114.0.2/30
	hoth	Spoke32	S0.6	115	ipp0	etu_s32 / Sp0k3.32
					veth0:veth1	10.115.0.1/30:10.115.0.2/30
	4	mustafar	Hub4	S0.7	116	ipp0
S0.7				117	ipp1	192.168.116.1:192.168.116.2
naboo		Spoke41	S0.8	118	ipp0	etu_s41 / Sp0k3.41
					veth0:veth1	10.118.0.1/30:10.118.0.2/30
tatooine		Spoke42	S0.8	119	ipp0	etu_s42 / Sp0k3.42
					veth0:veth1	10.119.0.1/30:10.119.0.2/30

4. Plan d'adressage LAN

La section «Plan d'adressage» du document [Architecture réseau des travaux pratiques](#) donne les adresses, dans le VLAN numéro 4, des deux routeurs ayant accès au réseau du campus.

- Routeur cooper.stri : 172.16.16.1/20 et 2001:678:3fc:4::1/64
- Routeur casper.stri : 172.16.16.2/20 et 2001:678:3fc:4::2/64

Tous les ports utilisés pour raccorder les routeurs ayant le rôle Hub doivent être configurés en mode trunk puisqu'ils servent à véhiculer le trafic de plusieurs domaines de diffusion. On conserve le VLAN natif numéro 1.

Tableau 3. Salle 211 - Affectation d'un commutateur par groupe

Groupe	Commutateur
1	asw05-211.infra.stri
2	asw06-211.infra.stri
3	asw07-211.infra.stri
4	asw08-211.infra.stri

Tableau 4. Salle 211 - Affectation des rôles, des numéros de VLANs et des adresses IP

Group	Poste	Rôle	OSPF router-id	VLAN	Interface	Réseau
1	christophsis	Hub1	OSPFv2 : 0.211.4.1 OSPFv3 : 0.211.6.1	421	eth0.421	10.4.21.1/28 2001:678:3fc:1a5::1
				431	eth0.431	10.4.31.1/28 2001:678:3fc:1af::1
				441	eth0.441	10.4.41.1/28 2001:678:3fc:1b9::1
2	kashyyyk	Hub2	OSPFv2 : 0.211.4.2 OSPFv3 : 0.211.6.2	4	eth0.4	172.16.18.2/20 2001:678:3fc:4::70a
				421	eth0.421	10.4.21.2/28 2001:678:3fc:1a5::2
				432	eth0.432	10.4.32.2/28 2001:678:3fc:1b0::2
3	mygeeto	Hub3	OSPFv2 : 0.211.4.3 OSPFv3 : 0.211.6.3	431	eth0.431	10.4.31.3/28 2001:678:3fc:1af::3
				432	eth0.432	10.4.32.3/28 2001:678:3fc:1b0::3
				443	eth0.443	10.4.43.3/28 2001:678:3fc:1bb::3

Group	Poste	Rôle	OSPF router-id	VLAN	Interface	Réseau
4	saleucami	Hub4	OSPFv2 : 0.211.4.4 OSPFv3 : 0.211.6.4	4	eth0.4	172.16.18.4/20
						2001:678:3fc:4::70c
				441	eth0.441	10.4.41.4/28
						2001:678:3fc:1b9::4
				443	eth0.443	10.4.43.4/28
						2001:678:3fc:1bb::4

Tableau 5. Salle 213 - Affectation d'un commutateur par groupe

Groupe	Commutateur
1	asw05-213.infra.stri
2	asw06-213.infra.stri
3	asw07-213.infra.stri
4	asw08-213.infra.stri

Tableau 6. Salle 213 - Affectation des rôles, des numéros de VLANs et des adresses IP

Group	Poste	Rôle	OSPF router-id	VLAN	Interface	Réseau
1	alderaan	Hub1	OSPFv2 : 0.213.4.1 OSPFv3 : 0.213.6.1	221	eth0.221	10.2.21.1/28
						2001:678:3fc:dd::1
				231	eth0.231	10.2.31.1/28
						2001:678:3fc:e7::1
				241	eth0.241	10.2.41.1/28
						2001:678:3fc:f1::1
2	coruscant	Hub2	OSPFv2 : 0.213.4.2 OSPFv3 : 0.213.6.2	4	eth0.4	172.16.17.2/20
						2001:678:3fc:4::6a6
				221	eth0.221	10.2.21.2/28
						2001:678:3fc:dd::2
				232	eth0.232	10.2.32.2/28
						2001:678:3fc:e8::2
3	felucia	Hub3	OSPFv2 : 0.213.4.3 OSPFv3 : 0.213.6.3	231	eth0.231	10.2.31.3/28
						2001:678:3fc:e7::3
				232	eth0.232	10.2.32.3/28
						2001:678:3fc:e8::3
				243	eth0.243	10.2.43.3/28
						2001:678:3fc:f3::3

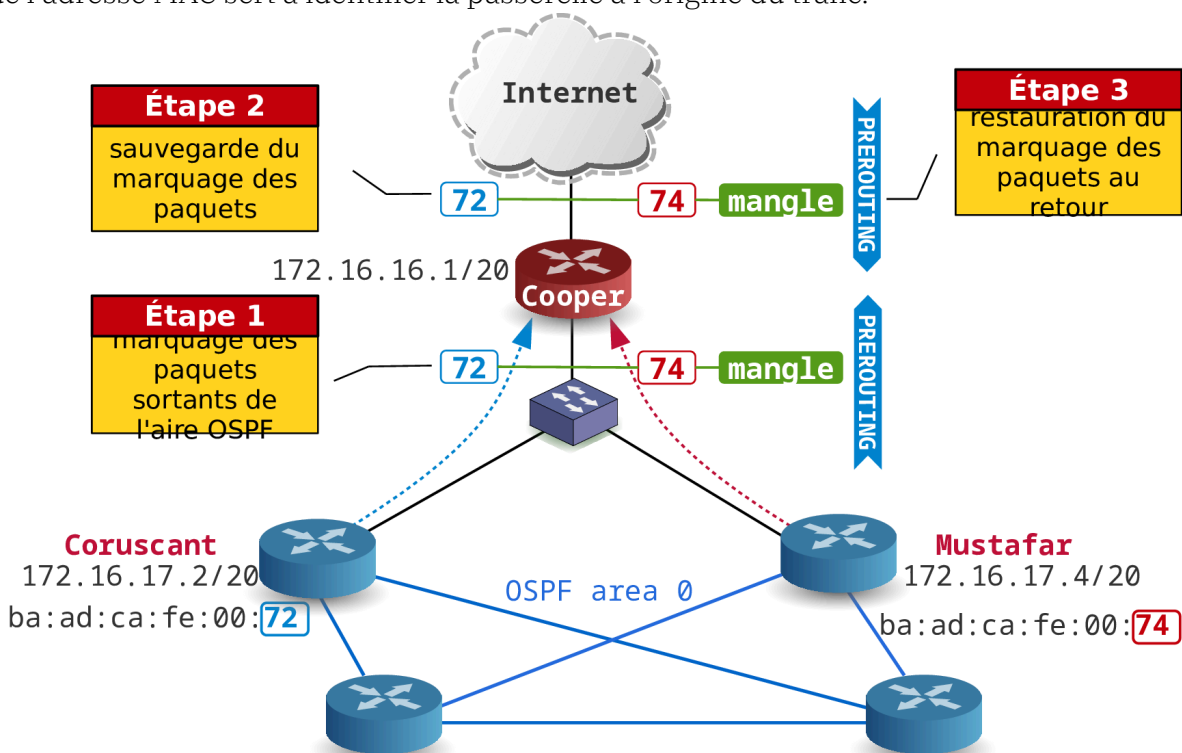
Group	Poste	Rôle	OSPF router-id	VLAN	Interface	Réseau
4	mustafar	Hub4	OSPFv2 : 0.213.4.4 OSPFv3 : 0.213.6.4	4	eth0.4	172.16.17.4/20
						2001:678:3fc:4::4
				241	eth0.241	10.2.41.4/28
						2001:678:3fc:f1::4
				243	eth0.243	10.2.43.4/28
						2001:678:3fc:f3::4

5. Interconnexion avec deux routeurs de bordure OSPF

Une fois que tous les routeurs (postes de travaux pratiques) sont actifs et que toutes les instances de routage OSPF ont convergé, les Spokes disposent de deux passerelles de sortie vers l'Internet. Les deux routeurs de bordure qui assurent cette fonction de passerelle sont Centares et Naboo. Du point de vue de l'aire OSPF, on dispose ainsi d'une tolérance aux pannes puisque les instances de routage OSPF effectuent automatiquement un recalcul de topologie dans le cas où l'une des deux passerelles viendrait à «tomber».

Le routeur de niveau supérieur, Cooper, ne dispose pas du même niveau d'information puisqu'il n'y a aucun échange de protocole de routage entre lui et les deux routeurs de bordure de l'aire OSPF. Pour associer ce routeur au mécanisme de tolérance aux pannes, on utilise le marquage de paquets. L'idée est que pour tout flux issu d'une passerelle, le flux retour soit renvoyé à cette même passerelle. On identifie ainsi la source du trafic. Si une des deux passerelles «tombe», elle n'émet plus aucun flux et le routeur Cooper ne verra plus de nouveau flux provenant de son interface.

Comme les interfaces des trois routeurs appartiennent au même VLAN ou domaine de diffusion, on utilise les adresses MAC comme identifiant de marquage. Dans cet exemple, l'octet le plus à droite de l'adresse MAC sert à identifier la passerelle à l'origine du trafic.



Note

Les manipulations présentées ci-dessous sont réalisées par l'enseignant sur le routeur Cooper en début de séance. Compte tenu des «alés de configuration» dans l'aire OSPF, le mécanisme de tolérance aux pannes est très utile dans le contexte des travaux pratiques.

Le processus de traitement suit les étapes suivantes pour un flux sortant de l'aire OSPF.

1. Nouveau flux entrant sur l'interface de Cooper en provenance de l'une des deux passerelles
2. Marquage du premier paquet en fonction de l'adresse MAC source dans la chaîne PREROUTING de la table `mangle`.
3. Mémoire du marquage de paquet dans le mécanisme suivi d'état du système de filtrage (`connmark`)

4. Entrée dans la table de routage dédiée au routeur de bordure à l'origine du flux.

Le processus de traitement suit les étapes suivante pour un flux retour vers l'aire OSPF.

1. Restauration du marquage de paquet en fonction des enregistrements effectués via le mécanisme suivi d'état du système de filtrage (connmark)
2. Entrée dans la table de routage dédiée au routeur de bordure à l'origine du flux.

Les opérations de configuration correspondantes sont données ci-après.

Création des tables de routage dédiées à chaque passerelle

- Édition du fichier `/etc/iproute2/rt_tables`.

```
# cat /etc/iproute2/rt_tables
#
# reserved values
#
255    local
254    main
253    default
0      unspec
#
# local
#
#1     inr.ruhep
72     centares
79     naboo
```

- Ajout des entrées dans les deux nouvelles tables de routage.

```
# ip route add 10.0.16.0/20 via 172.16.17.10 table centares
# ip route add 10.0.32.0/20 via 172.16.17.10 table centares
# ip route add default dev bond0 table centares
```

```
# ip route add 10.0.16.0/20 via 172.16.17.40 table naboo
# ip route add 10.0.32.0/20 via 172.16.17.40 table naboo
# ip route add default dev bond0 table naboo
```

Dans les deux copies d'écran ci-dessus on a agrégé tous les réseaux de l'aire OSPF en deux entrées.

Création des règles de marquage des flux

La table `mangle` est dédiée à l'altération des paquets. Ici, on s'intéresse uniquement à l'ajout d'un marquage de chaque paquet transitant par les interfaces réseau.

```
# iptables -t mangle -A PREROUTING -i bond0.4 \
-m mac --mac-source 00:1f:c6:01:26:72 -j MARK --set-mark 72
# iptables -t mangle -A PREROUTING -i bond0.4 \
-m mac --mac-source 00:1f:c6:01:26:79 -j MARK --set-mark 79
# iptables -t mangle -A PREROUTING -i bond0.4 -j CONNMARK --save-mark
# iptables -t mangle -A PREROUTING -i bond0 -j CONNMARK --restore-mark
```

Création des règles d'entrée dans les tables de routage

C'est le marquage qui détermine le choix de la table de routage à utiliser.

```
# ip rule add fwmark 72 table centares
# ip rule add fwmark 79 table naboo
```

Et voilà ! Il ne reste plus qu'à consulter les entrées `conntrack` à l'aide de la commande `# conntrack -t` pour voir apparaître les marquages.