

## Connexion réseau & analyse

### Configurer une interface réseau Ethernet

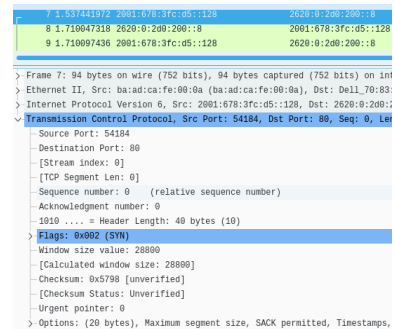
L'objectif de ces travaux pratiques est d'analyser et configurer une interface réseau Ethernet sur un système GNU/Linux. Les manipulations présentées suivent la modélisation réseau en remontant du niveau physique jusqu'à la couche application. Les questions illustrent les relations entre les différents formats d'adressage utilisés à chaque niveau ainsi que les protocoles utilisés pour les correspondances entre les différentes couches.

### Dessine moi une interconnexion réseau

Le défi proposé dans cet exercice est de construire une représentation graphique de l'interconnexion entre plusieurs routeurs reliés entre eux par des réseaux locaux IPv4 & IPv6. En ouvrant une console SSH successivement sur chaque routeur on doit collecter les informations d'adressage des interfaces, les adresses réseaux et la liste des voisins connus. Ainsi, on peut identifier les liaisons directes entre routeurs. Pour relever le défi, il suffit d'utiliser les options de la commande **ip** du paquet `iproute2`.

### Introduction à l'analyse réseau

L'analyseur de trafic est un outil pédagogique essentiel pour comprendre les mécanismes de fonctionnement des protocoles de communication sur les réseaux contemporains. Ce document comprend deux parties. Dans un premier temps, on trouve une introduction à l'utilisation de l'analyseur *Wireshark*. Dans un deuxième temps, les travaux pratiques permettent de découvrir l'organisation des informations fournies par cet analyseur.



```
7 1.53741972 2001:678:3fc:d5:128 2020:0:200::1
8 1.710047318 2020:0:200::18 2001:678:3fc:d5:128
9 1.710097436 2001:678:3fc:d5:128 2020:0:200::18

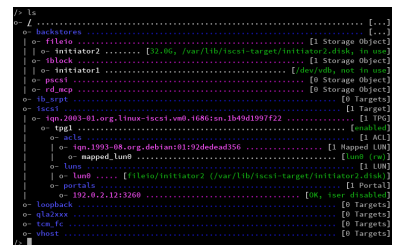
> Frame 7: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on int
> Ethernet II, Src: ba:ad:ca:fe:00:0a (ba:ad:ca:fe:00:0a), Dst: Dell_70:83
> Internet Protocol Version 6, Src: 2001:678:3fc:d5:128, Dst: 2020:0:200::18
> Transmission Control Protocol, Src Port: 54184, Dst Port: 80, Seq: 0, Len: 40
  - Source Port: 54184
  - Destination Port: 80
  - [Stream index: 0]
  - [TCP Segment Len: 0]
  - [TCP Segment Len: 0]
  - Sequence number: 0 (relative sequence number)
  - Acknowledgment number: 0
  - 1010 ... = Header Length: 40 bytes (10)
  - Flags: 0x002 (SYN)
  - Window size value: 28800
  - [Calculated window size: 28800]
  - Checksum: 0x5798 [unverified]
  - [Checksum Status: Unverified]
  - Urgent pointer: 0
  - Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps,
```

## Administration système en réseau

Le module « Administration système en réseau », enseigné en première année du *master Réseaux et télécommunications* de l'université de Toulouse, se concentre sur deux aspects principaux : le stockage réseau avec SAN / iSCSI et NAS / NFS, ainsi que la gestion d'identité avec LDAP. Les manipulations pratiques comprennent la configuration de serveurs et de clients pour ces technologies, ainsi que leur intégration. L'objectif est de fournir aux étudiants une expérience pratique approfondie des concepts clés de l'administration système distribuée combinant stockage et gestion des identités dans un environnement réseau distribué. Le manuel complet regroupant l'ensemble des manipulations est disponible à l'adresse suivante : [Manuel de Travaux Pratiques - Module « Administration système en réseau »](#) ou au format [PDF](#).

### Introduction au réseau de stockage iSCSI

Ce support de travaux pratiques est consacré à l'étude des technologies de stockage DAS (*Direct Attached Storage*), SAN (*Storage Area Network*) et de la redondance RAID 1. Le protocole iSCSI est utilisé comme exemple d'accès «mode bloc» aux unités de stockage réseau pour la partie SAN. La redondance RAID 1 utilise les fonctions intégrées au noyau Linux. L'infrastructure proposée montre comment les différentes technologies élémentaires peuvent être combinées pour atteindre les objectifs de haute disponibilité et de sauvegarde.



```
backstores ..... [ ... ]
o filerep ..... [ ... ]
  o initiator2 ..... [ ... ]
  o block ..... [ ... ]
  o initiator1 ..... [ ... ]
  o pxcsi ..... [ ... ]
  o fdisk ..... [ ... ]
  o hprt ..... [ ... ]
  o iqn.2003-01.org.linuxtarget:iscsi.vml.1686.on.1b49d197f22 ..... [ ... ]
  o tgt ..... [ ... ]
  o mapped_lun0 ..... [ ... ]
  o lun0 ..... [ ... ]
  o lun1 ..... [ ... ]
  o initiator2 (/var/lib/iscsi-target/initiator-dfba1) ..... [ ... ]
  o pvc1 ..... [ ... ]
  o 192.0.2.121:3260 ..... [ ... ]
  o target ..... [ ... ]
  o target ..... [ ... ]
  o target ..... [ ... ]
  o target ..... [ ... ]
  o target ..... [ ... ]
  o target ..... [ ... ]
```

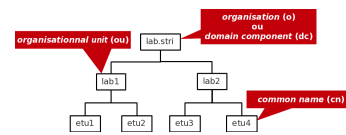
### Introduction au système de fichiers réseau NFSv4

L'objectif de ce support de travaux pratiques est d'étudier le système de fichiers réseau NFS. Il illustre les accès en « mode fichier » à une unité de stockage réseau. Ce mode d'accès correspond à un stockage de type NAS (*Network Attached Storage*). Le document commence par l'étude du principe de fonctionnement des appels de fonctions RPC (*Remote Procedure Call*), puis se poursuit avec la configuration d'un serveur NFS

qui exporte une arborescence de comptes utilisateurs. Côté client, les accès au système de fichiers réseau NFS sont étudiés selon deux modes distincts : le montage manuel, puis l'automontage.

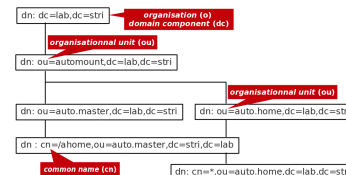
### Introduction aux annuaires LDAP avec OpenLDAP

Dans ce support de travaux pratiques, on explore le service d'annuaire LDAP. On présente succinctement les éléments constitutifs d'un annuaire puis on étudie la configuration d'un service d'annuaire basé sur le logiciel OpenLDAP. Ensuite, on étudie la configuration de l'accès aux entrées de l'annuaire depuis un poste client. Les informations délivrées par l'annuaire sont les propriétés de comptes utilisateurs stockées dans la classe d'objet `posixAccount`.



### Association LDAP, NFSv4 et autofs

Ce support reprend les deux précédents sur NFSv4 et LDAP en associant les services. Le système de fichiers réseau NFSv4 sert au partage des répertoires utilisateur tandis que l'annuaire LDAP sert au partage des attributs des comptes utilisateur et de la configuration du service d'automontage. Une fois que les deux services associés sont en place, les comptes utilisateurs peuvent être utilisés de façon transparente depuis n'importe quel poste client faisant appel à ces services.



## Interconnexion réseaux LAN/WAN

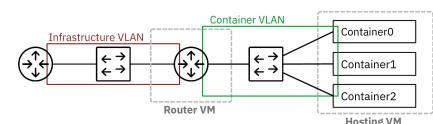
Le module « Interconnexion de réseaux LAN/WAN », enseigné en première année de *Master Réseaux et télécommunication à l'Université Paul Sabatier*, met l'accent sur les aspects opérationnels du paradigme *DevOps* dans le contexte du « cloud privé » de la formation.

Le module aborde des concepts clés tels que le routage interVLAN, la conteneurisation, la sécurité réseau et l'automatisation, et se concentre sur la configuration et la gestion d'une infrastructure réseau virtualisée. Les travaux pratiques incluent la configuration des interfaces réseau et des commutateurs virtuels en mode déclaratif avec *Netplan*, ainsi que la configuration de pare-feu avec *nftables*.

On aborde aussi un sujet important pour les réseaux évolutifs et agiles : le protocole de routage dynamique OSPF pour IPv4 et IPv6 avec *FRRouting*. Le manuel complet regroupant toutes les manipulations de la série est disponible à l'adresse [Manuel de Travaux Pratiques - Module « Interconnexion LAN/WAN »](#) ou au format [PDF](#).

### Routage inter-VLAN dans un contexte IaaS

Ce support de travaux pratiques détaille la mise en œuvre du routage inter-VLAN dans une infrastructure IaaS avec deux machines virtuelles, dont l'une héberge des conteneurs Incus. Il guide l'utilisateur pas à pas dans la configuration d'un réseau comportant plusieurs VLAN. Il commence par montrer comment connecter les deux machines virtuelles via un commutateur de distribution Open vSwitch, puis comment mettre en place le routage entre les réseaux de l'hyperviseur et les réseaux de conteneurs utilisant la technologie *macvlan*.

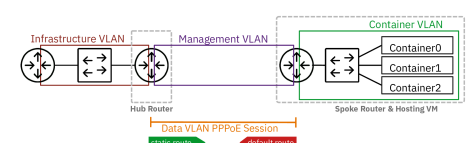


Le document couvre l'ensemble du cycle : configuration du réseau (IPv4/IPv6) et du routage sur GNU/Linux, activation de la traduction d'adresses (NAT avec *nftables*), gestion de l'adressage automatique (*dnsmasq*), installation et le paramétrage du gestionnaire de conteneurs Incus, ainsi que l'automatisation de tâches courantes avec des scripts Bash.

### Routage inter-VLAN et protocole PPPoE

La généralisation de l'utilisation de la fibre optique dans les réseaux étendus (WAN) jusqu'au raccordement domestique s'est accompagnée d'un changement important au niveau des liaisons de données. La technologie Ethernet est devenue universelle et couvre tous les besoins de commutation de circuits.

Cependant, pour raccorder les sites d'entreprises via des réseaux d'opérateurs, les fonctions historiques du protocole PPP (*Point-to-Point Protocol*) sont toujours utiles. C'est là que le protocole PPPoE



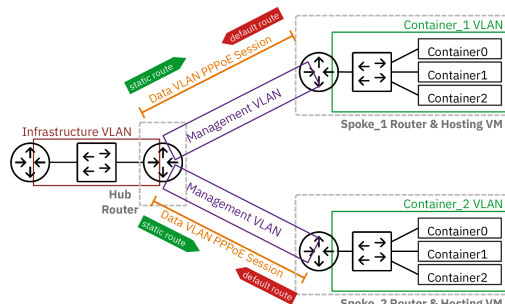
intervient. Il permet d'associer un réseau de diffusion Ethernet avec un fonctionnement point à point typique des réseaux étendus.

Le but des manipulations présentées dans ce document est d'illustrer la mise en œuvre d'une session PPPoE entre un routeur virtuel central et un site distant factice (une autre machine virtuelle) qui héberge quelques services.

### Topologie Hub and Spoke et protocole PPPoE

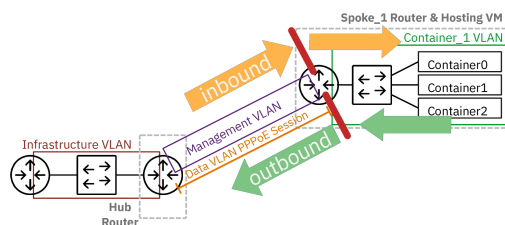
Ce support de travaux pratiques illustre une topologie réseau classique appelée « *Hub & Spoke* ». Le « *hub* » est un routeur qui concentre tous les flux des routeurs d'extrémité, appelés « *spoke* ». Les liaisons entre le *hub* et les routeurs *spoke* sont point à point et utilisent le protocole PPP. Avec la généralisation de la fibre optique dans les réseaux étendus (WAN), les trames PPP doivent être encapsulées dans un VLAN Ethernet à l'aide de la technologie PPPoE.

Les manipulations proposées reprennent en grande partie celles du support précédent « *Routage inter-VLAN et protocole PPPoE* », en les adaptant à la topologie en triangle.



### Filtrage réseau avec netfilter/nftables

Ce support de travaux pratiques introduit le filtrage réseau avec Netfilter/Nftables sur une topologie « *Hub & Spoke* ». Il commence par identifier les outils et services (nftables, contrack et fail2ban), puis aborde la mise en œuvre de règles de filtrage sans suivi d'état (*stateless*) et avec suivi d'état (*stateful*). Les activités abordent la protection de base des routeurs (anti-spoofing, limitation ICMP, défense contre les robots SSH), la traduction d'adresses source et de destination (SNAT, DNAT) ainsi que le contrôle des flux traversants. À l'issue de ces manipulations, l'étudiant est capable de concevoir, d'appliquer et de valider une première politique de sécurité réseau cohérente.

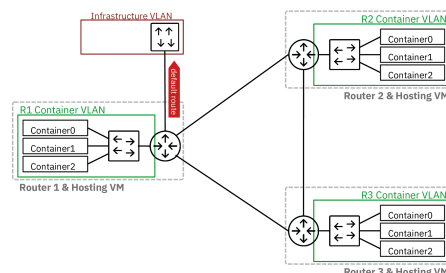


### Introduction au routage dynamique OSPF

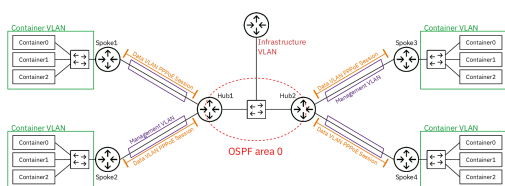
Le protocole OSPF (*Open Shortest Path First*) permet un routage dynamique efficace et évolutif dans les grands réseaux IP, en calculant automatiquement les meilleures routes en fonction de l'état des liens.

Ce support de travaux pratiques est une introduction au protocole de routage dynamique OSPF. Il détaille la mise en place d'une topologie en triangle utilisant des VLANs, ainsi que la configuration des routeurs avec la suite logicielle FRRouting pour activer et paramétrer OSPF dans une aire unique.

Les manipulations présentées expliquent comment préparer les systèmes, valider les communications entre routeurs et configurer les démons OSPFv2 et OSPFv3 étape par étape.



### Synthèse sur l'interconnexion LAN/WAN



L'objectif de ce dernier document de la série de travaux pratiques est de faire la synthèse sur l'interconnexion de réseaux locaux (LAN) et de réseaux étendus (WAN). Côté réseaux étendus, on retrouve les sessions PPPoE vers chaque site distant avec son réseau d'extrémité avec un l'hébergement de services représentés par les conteneurs Incus.

Côté réseaux locaux, les routeurs *Hub* échangent leurs routes avec le protocole de routage dynamique OSPF. Ces routeurs constituent ainsi un réseau de "collecte". Que l'on soit dans le domaine LAN ou WAN, on fait un usage massif des VLANs.

## Archives des anciens supports de travaux pratiques

---

### Introduction au service DNS

Ce support de travaux pratiques sur le service *Domain Name System* s'appuie sur le logiciel BIND. Côté client ou *resolver*, il illustre les différents tests de fonctionnement du service à l'aide de la *dig*. Côté serveur, il présente l'utilisation du service suivant 3 modes : cache seulement (*cache-only*), maître (*primary|master*) et esclave (*secondary|slave*).

### Introduction au routage dynamique OSPF avec Bird

L'objectif de ce support de travaux pratiques est d'étudier le protocole de routage dynamique OSPF. Cette illustration s'appuie sur une topologie minimale très classique : le triangle. L'originalité consiste à utiliser les VLANs pour distinguer la topologie physique (l'étoile) de la topologie logique (le triangle). Cette version du support utilise le logiciel Bird.

