Commutateurs Juniper
EX Series

Direction Informatique

Université de Strasbourg

Sommaire

Auteurs

Nom	***Position***	***Date***
Laurence Moindrot	Ingénierie DI - Infrastructure	02/06/10
Sébastien Boggia	Ingénierie DI - Infrastructure	02/06/10
Christophe Distel	Ingénierie DI - Infrastructure	02/06/10
Guillaume Schreiner	Ingénierie DI - Infrastructure	02/06/10
Christophe Saillard	Ingénierie DI - Infrastructure	02/06/10

Historique

Version	***Date***	***Auteur***	***Raison***
1.0	16/06/10	Guillaume Schreiner, Christophe Distel, Laurence Moindrot, Christophe Saillard, Sébastien Boggia	Version initiale
1.1	18/06/10	Guillaume Schreiner, Christophe Distel, Laurence Moindrot, Christophe Saillard, Sébastien Boggia	Ajout section « Gestion des utilisateurs », diverses corrections

1. Principes de base sur les réseaux des entités reliées à Osiris

1.1. Les types de réseaux

Il existe 2 grands types de réseaux :

- **LAN** (Local Area Network) ou bien RLE (Réseaux Locaux d'entreprise). Ces réseaux sont des réseaux privés, c'est à dire faisant partie d'une même entité physique ou juridique. On les utilise essentiellement pour relier des ordinateurs entre eux et à des ressources partagées (imprimantes, serveurs de fichiers).
- **MAN** (Metropolitan Area Network) ou WAN (Wide Area Network). En français, réseaux métropolitains ou réseaux longue distance. Ces réseaux sont destinés à faire la jonction entre **plusieurs LAN** sur des distances plus ou moins longues.

Dans la pratique, on peut donc classifier **Renater** comme étant un réseau **WAN**, **Osiris** un **MAN** et les **sites** raccordés à Osiris comme des **LAN**.

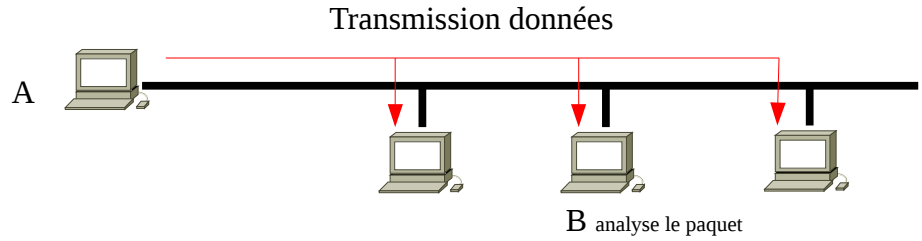
1.2. Transmission des données dans un réseau

Il y a 2 techniques de transmission des données.

- Le point à point,
- La diffusion.

Le **point à point** consiste à transmettre des données sur une connexion entre 2 machines uniquement. Un réseau formé uniquement de connexions point à point pourra faire transiter l'information d'une machine à l'autre par plusieurs intermédiaires.

Un **réseau à diffusion** (point à multipoint) n'a qu'un seul canal de communication que toutes les machines partagent (réseau de type bus). Les paquets envoyés par une machine sont reçus par toutes les autres. La machine destinataire du paquet l'analyse. Les autres l'ignorent.



D'une manière générale, **les réseau locaux des bâtiments connectés à Osiris (LAN) sont des réseaux de diffusion**. Les connexions point à point sont plutôt utilisées sur les liaisons Internet grandes distances ou parfois pour les interconnexions entre les LAN et les WAN.

1.3. Principe d'un réseau Ethernet

L'architecture des réseaux locaux des bâtiments Osiris va nous conduire naturellement à se pencher sur Ethernet. Ethernet fonctionne sur des réseaux de diffusion de type **bus,** appelés aussi **segments E**thernets. Le problème de ce type de réseau est de trouver un mécanisme d'arbitrage pour que la transmission des données ne se fasse pas simultanément entre deux machines.

Deux paquets émis en même temps par deux machines provoquent un phénomène de **collision**. C'est à dire que le signal électrique sur le câble devient incompréhensible. Heureusement, les machines qui sont à l'écoute de ce qui se passe sur le bus sont capables de détecter les collisions.

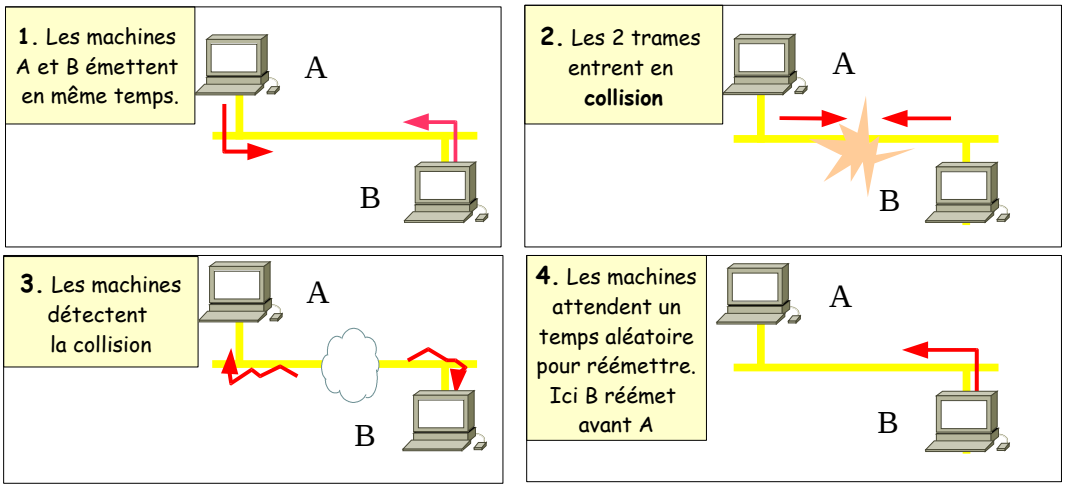
Sur Ethernet, une machine peut transmettre quand elle le désire. C'est le protocole **CSMA/CD** qui permet de gérer le moment où une machine peut émettre sur le bus, de détecter les collisions et d'y remédier.

- **CSMA** signifie : Carrier Sense Multiple Acces.
- **CD** signifie : Collision Detection.

1.3.1. Principe de base de CSMA/CD

Une machine qui souhaite transmettre sur le réseau écoute le câble. Si la voie n'est pas libre, elle attend jusqu'à ce que l'autre machine ait fini de transmettre.

Si deux machines commencent à émettre en même temps et qu'il y a collision, elles arrêtent d'émettre, attendent toutes deux un temps aléatoire pour réémettre de manière à ne plus entrer en collision.



Le protocole Ethernet est inclut dans la sous-couche liaison de données **MAC** (Medium Acces Control) du modèle **OSI**. Il s'agit de la sous-couche de Contrôle d'accès au Canal.

Chaque trame Ethernet contient une en-tête MAC avec les informations nécessaires pour acheminer le trafic.

Il y a plusieurs versions d'Ethernet : Ethernet v2, Ethernet IEEE 802.3 ... Ces versions présentent quelques différences au niveau des trames. Voici la représentation d'une trame Ethernet v2, utilisée dans plus de 90% des cas.

7 octets	1	6 octets	6 octets	2 octets	46–1500 octets	4 octets
Préambule	SD	Adresse MAC Dst	Adresse MAC Src	Type	Information couche supérieure	FCS

Trame Ethernet v2

Description des champs

- **Préambule** : Ce champ permet à l'émetteur de la trame et au récepteur de se synchroniser.
- **SD** : Ce champ de 1 octet permet de délimiter le début réel de la trame.
- **MAC Dst Address** : Adresse MAC de la machine de destination.
- **MAC Src Address** : Adresse MAC de la machine source.
- **Type** : Protocole réseau encapsulé dans la trame Ethernet. 0X800 = IPv4
- **Information** : Données transportées, 1500 octets maximum.
- **FCS** : Contrôle de l'intégrité de la trame.

La longueur d'une trame Ethernet v2 valide se situe entre 60 et 1514 octets (MAC Src + MAC Dst + Type + Information).

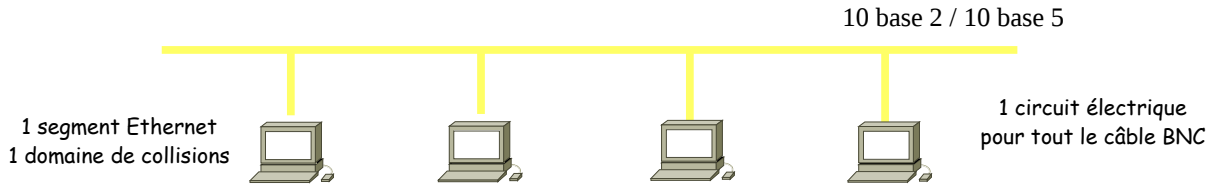
Chaque machine émettant sur un réseau Ethernet possède une **carte réseau avec un identifiant unique** sur 6 octets, c'est l'**adresse MAC** de la carte.

Cette adresse est divisée en 2 parties :

- Trois premiers octets : **Numéro du constructeur** (exemple: 00-08-20 : Sun, 00:05:85 : Juniper).
- Trois derniers octets : **Numéro de série de la carte**.

Une adresse MAC est réservée pour l'envoie en broadcast c'est à dire à destination de toutes les machines du réseau. C'est l'adresse FF-FF-FF-FF-FF-FF.

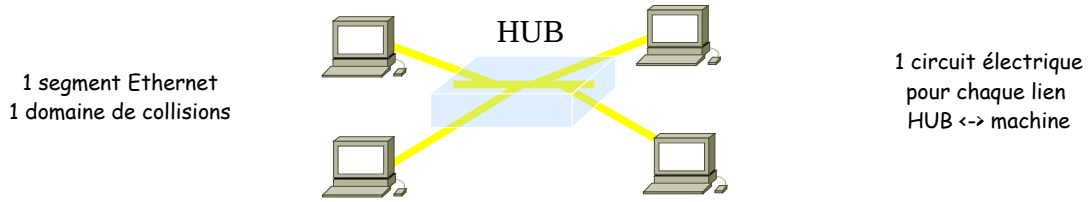
Nous venons de présenter Ethernet de manière à bien mettre en évidence ses principes de base et comme il a été pensé lors de sa conception. A l'époque, un réseau était souvent composé d'un câble coaxial (BNC) 10Base5 sur lequel étaient connectées les machines. Celles-ci émettaient donc toutes sur le même lien physique.



Cette architecture apporte vite des limitations en cas de rupture de lien (le réseau est coupé pour toutes les machines) ou lorsque le débit de transmission et le nombre de machines sur le bus augmentent (on se trouve rapidement en présence de nombreuses collisions).Le problème de la coupure de lien a été résolu par l'utilisation d'un répéteur (HUB) et de câbles RJ45. On est passé à une architecture en **étoile**. Tout le trafic transite vers le point central qui est le répéteur.

L'architecture en étoile apporte 2 avantages :

- Une coupure sur l'un des liens « répéteur <-> machine » n'affecte pas les autres machines.
- Le câblage est plus souple, peut utiliser des paires téléphonique déjà existantes et n'affecte qu'une machine.



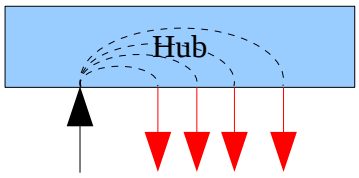
Le problème des collisions de plus en plus fréquentes par l'ajout de machines et l'augmentation de trafic peut être réglé par la **diminution de la taille du domaine de collisions**.

1.4. Concepts de base de la commutation de niveau 2

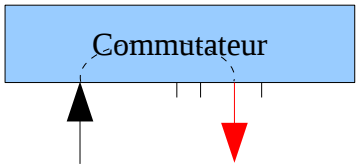
Afin de limiter les problèmes de collisions Ethernet, il faut **limiter le nombre de machines connectées sur un même segment** et n'y envoyer que les trames destinées à des machines s'y trouvant. Pour cela on se sert de commutateurs (switches). Voici un bref comparatif entre un répéteur (hub) et un commutateur.

Un **hub** est un équipement « bête » :

- Il sert à ré-amplifier le signal d'un lien,
- Il renvoie toutes les trames reçues sur tous les ports immédiatement,
- Il peut permettre de passer d'un média à un autre. Par exemple du cuivre vers de la fibre.



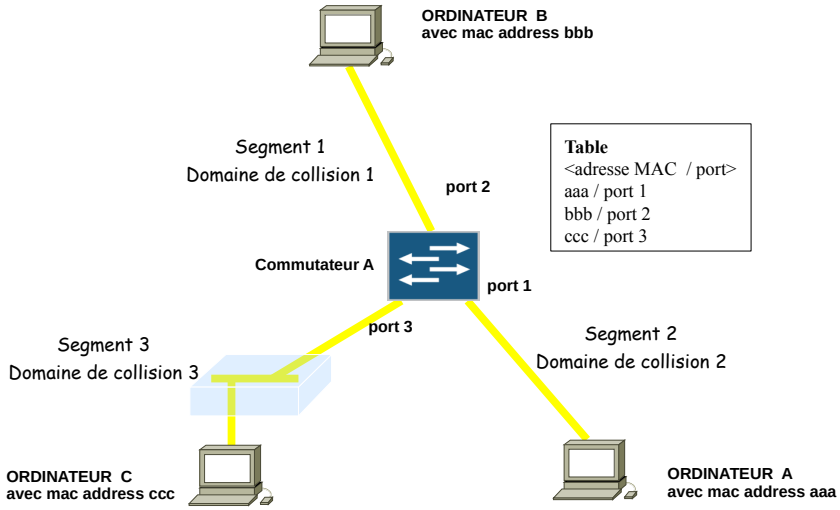
Un **commutateur** est un équipement « intelligent ». Le commutateur est le centre de la topologie en étoile. A la différence du répéteur (hub), qui ne fait que répéter sur tous les ports les données qu'il reçoit, les commutateurs ont la capacité d'analyser le trafic, et ainsi de posséder une connaissance des adresses MAC (Medium Access Control) et de construire des tables de commutation.



Le commutateur possède les particularités suivantes :

- Apprendre les adresses MAC des matériels attachés à ses ports.
- N'envoie le trafic d'une adresse MAC que sur le port concerné,
- Possède une table de commutation <adresse MAC <-> port>.
- La grande majorité des commutateurs apporte des fonctionnalités supplémentaires comme éviter la formation de boucles (Spanning Tree) ou créer des réseaux virtuels (VLAN). Attention! Ces fonctionnalités ne sont pas natives aux commutateurs et peuvent ne pas exister sur les bas de gamme.

Avec un commutateur, le domaine de collision est limité à un seul port, rendant les collisions impossibles. De plus la bande passante disponible sur une interface ne sert que pour la machine connectée dessus.



L'apprentissage des adresses MAC :

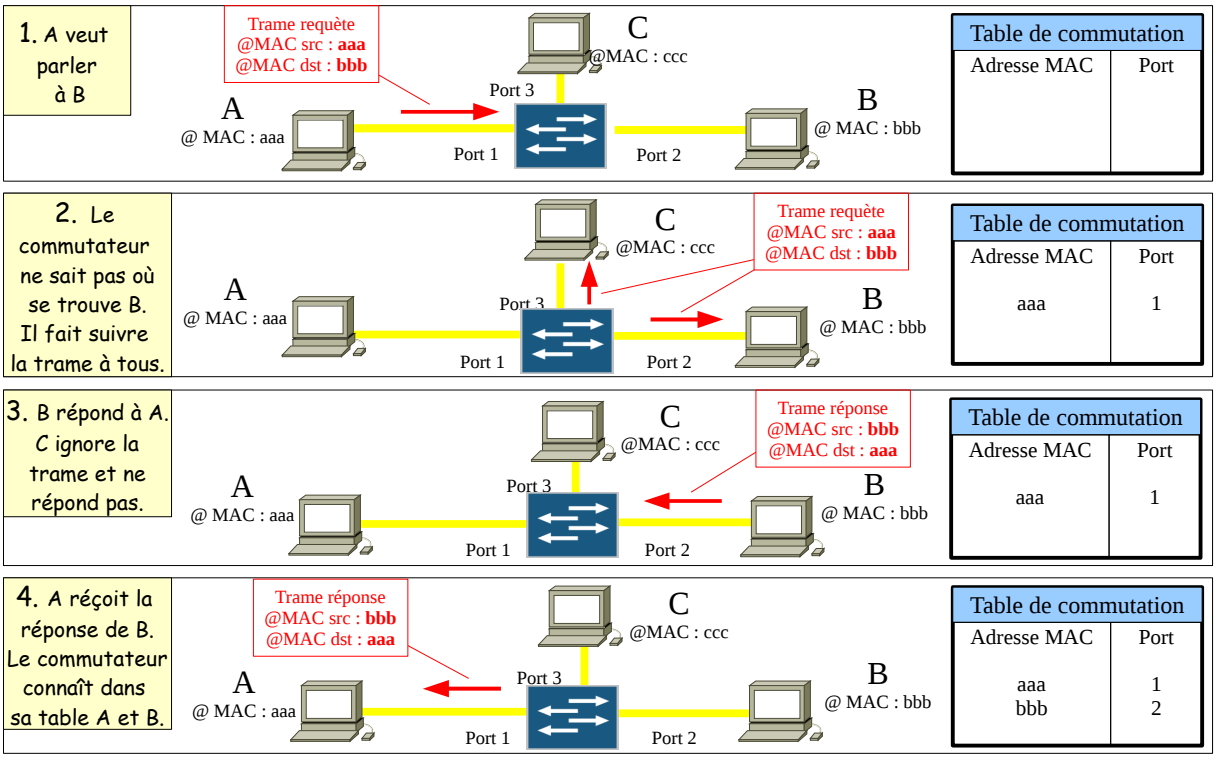
Au démarrage du commutateur, la table est vide **(1).**

Lorsque le commutateur doit envoyer une trame, s'il ne trouve pas l'adresse MAC de destination dans sa table la correspondance <adresse MAC, port>, il envoie la trame sur tous les ports **(2)**, sauf le port entrant (d'où provient la trame).

Le commutateur va mettre à jour, en mémoire, sa table de couples <adresse MAC, port> **(2) (4)** à chaque passage d'une trame entrante : il récupère l'adresse MAC source (et non l'adresse MAC destination) puis ajoute ou met à jour une entrée dans la table (port entrant/adresse MAC source).

Il existe une durée maximale de présence dans la table d'une association <adresse MAC, port>. Cette durée est appelée « time-age ». Le commutateur ne se souvient donc que des matériels les plus actifs. Le « time-age » est paramétrable. Il est par défaut de 5 minutes sur les Cisco Catalyst.

On dit que lors de l'émission d'une trame, il y a commutation vers le bon port si l'adresse MAC destinatrice est connue dans la table. Il y a en même temps régénération de l'entrée associée à l'adresse MAC source dans cette table.



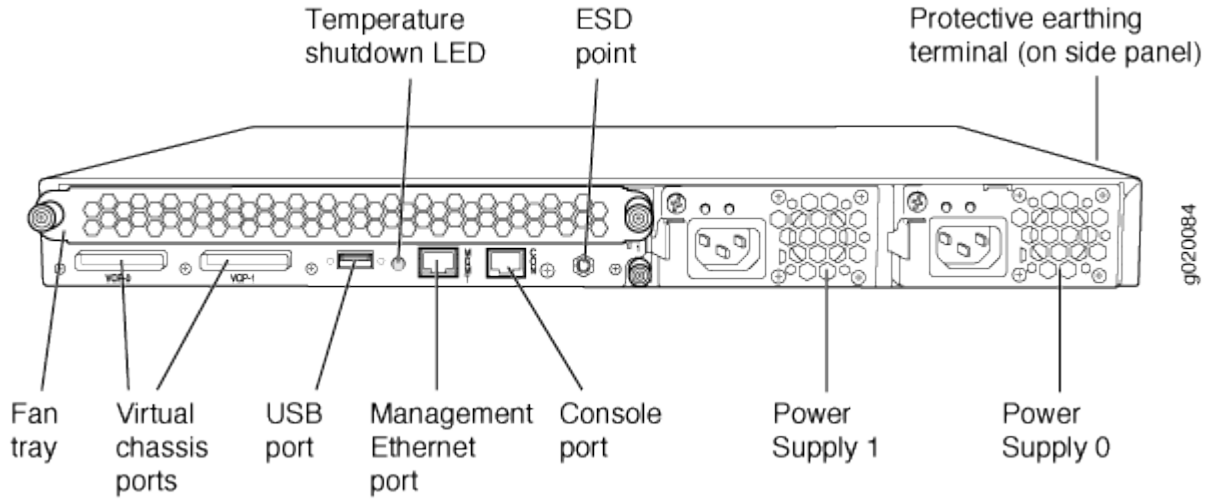
2. Généralités sur les commutateurs Juniper EX

2.1. Architecture fonctionnelle

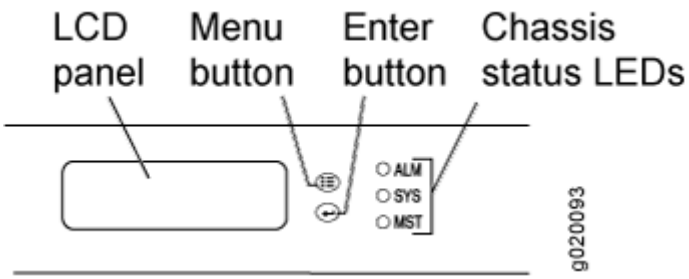
Les commutateurs Juniper sont tous dotés :

- d'un **port console** (port série compatible avec celui de votre PC) prévu pour un accès administratif local à partir d'un terminal ASCII ou d'un ordinateur avec émulation de terminal (Hyperterminal pour Windows ou minicom pour Linux)
- d'un **port de management** (port Ethernet permettant un accès hors bande au commutateur si le réseau local le permet)
- d'un **port USB** (port permettant de démarrer l'équipement sur une clef USB externe en cas de problème sur le disque interne).

Ces ports sont situés au dos du commutateur :



Les commutateurs Juniper EX 3200 et EX 4200 sont tous dotés d'un **panneau LCD** qui permet d'afficher des informations sur le statut du commutateur et permet également d'effectuer des opérations basiques comme la configuration initiale ou le redémarrage de l'équipement.



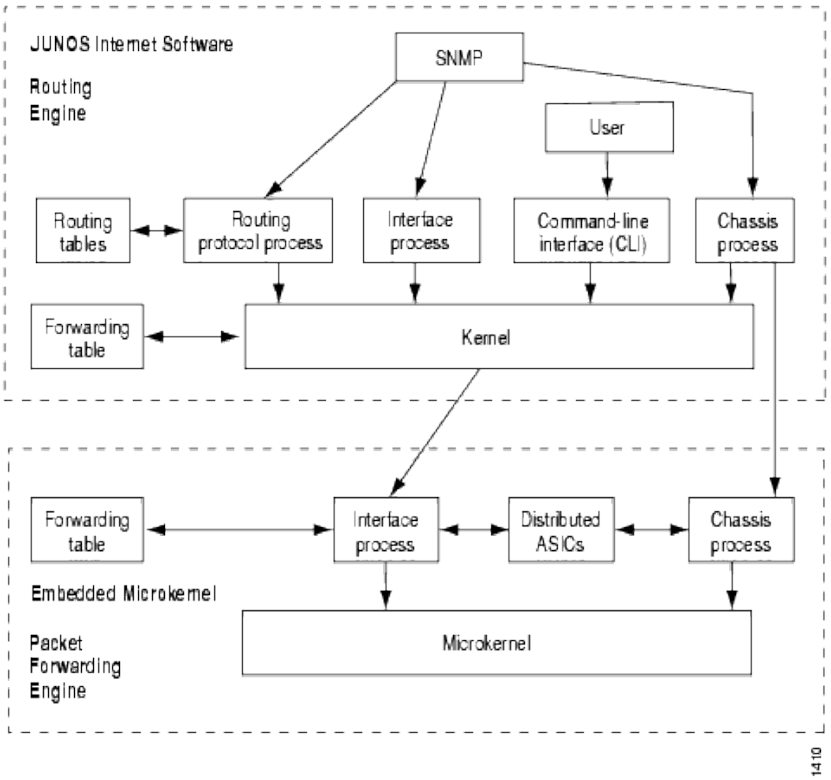
- **JUNOS** (Juniper Operating System) est le nom du système d'exploitation exécuté sur les commutateurs Juniper.
- **CLI** (Command Line Interface) est le sigle utilisé pour désigner l'interface en ligne de commande du terminal pour le système JUNOS.
- **J-Web** (Interface Web de configuration) est l'interface graphique permettant de configurer les équipements Juniper via un navigateur Web (Safari, Internet explorer, Firefox, ...).

L'architecture fonctionnelle des commutateurs Juniper s'appuie sur 2 principaux composants :

- **la Routing Engine** (RE)
- **la Packet Forwarding Engine** (PFE)

La RE est composée d'un processeur, d'une mémoire SDRAM pour le stockage des tables de routage, d'une mémoire compact flash pour le stockage primaire des images JUNOS, des fichiers de configuration et du microcode. Le logiciel JUNOS est exécuté sur la RE et est composé de plusieurs processus comme « chassisd », « eswd » ou « dcd » qui gèrent respectivement les composants hardware, les fonctionnalités de commutation ou les interfaces réseaux.

La PFE commute les paquets.



Architecture matérielle des commutateurs Juniper

2.2. Gammes de commutateurs Juniper

5 gammes de commutateurs Juniper sont disponibles :

- **EX2200** : 24 ou 48 ports 10/100/1000 + 4 SFP (1G), PoE ou non
  - Pas de ports 10G
  - Non stackable
  - Pas évolutif
- **EX3200** : 24 ou 48 ports 10/100/1000, 8 ports PoE ou full PoE
  - Non stackable
  - Évolutif, possibilité d'insertion de modules
    - Pour avoir 4 ports SFP 10/100/1000 ou 2 ports SFP 10G
- **EX4200** : 24 ou 48 ports 10/100/1000, 8 ports PoE ou full PoE ; 24 ports SF
  - Équivalent EX 3200 + fonctionnalité de virtual-chassis (stackable)
- **EX4500** : 40ports 1G/10G
  - Stackable, orientés datacenters
- **EX8208** : châssis pour densité de port importante (densité possible de 384 ports
  - Possibilité d'ajouter 8 cartes d'extension :
    - 48 ports ethernet 10/100/1000
    - 48 ports SFP (100M ou 1G)
    - 8 ports SFP 10G
    - 40 ports SFP 10G (bloquants)
  - A venir : carte d'extension virtual-chassis (stackable) pour la fin de l'année

2.3. Arborescence de la configuration

La configuration sur les commutateurs Juniper est décomposée en plusieurs **contextes**. Chaque contexte peut comporter des **sous-contextes** ou des **attributs**. La configuration est représentée comme une arborescence dont les contextes sont des branches et les attributs sont des feuilles. Voici un aperçu non exhaustif de l'arborescence :

- **system**
  - **host-name** (attribut) : nom de l'équipement
  - **login** (contexte) : identifiants de connexion
  - **syslog** (contexte) : paramétrage des options de log
  - **domain-name** (attribut) : nom de domaine
  - **name-server** (contexte) : IP des serveurs DNS
  - **ntp** (contexte) : IP ds serveurs NTP
  - **services** (contexte) : types d'accès autorisés, par exemple ssh, web
- **chassis** :
  - **aggregated-devices** (contexte) : liens agrégés 802.3ad
  - **alarm** (contexte) : configuration des alarmes remontées
  - **lcd** (contexte) : activation ou non du menu de maintenance du panneau LCD
- **interfaces** :
  - **ge-X/X/X** (contexte) : configuration des ports cuivres Giga
  - **xe-X/X/X** (contexte) : configuration des ports optiques 10Giga
  - **vlan** (contexte) : configuration des ports logiques
  - **aeX** (contexte) : configuration des agrégats
- **routing-options**
  - **static** (contexte) : configuration des routes statiques, par exemple la passerelle par défaut
- **protocols**
  - **vstp** (contexte) : configuration du protocole de spanning tree recommandé par la DI
  - **lldp** (contexte) : configuration du protocole LLDP
  - **igmp-snooping** (contexte) : configuration du protocole IGMP snooping
- **ethernet-switching-options**
  - **voip** (contexte) : configuration du vlan natif pour la VOIP
  - **storm-control** (contexte) : activation de la protection contre les tempêtes de broadcast
  - **bpdu-block** (contexte) : blocage du spanning tree
  - **redundant-trunk-group** (contexte) : configuration du protocole RTG (équivalent FlexLinks Cisco)
- **vlans** (contexte) : configuration des VLANs
- **poe** (contexte) : gestion de l'activation ou non des ports PoE

3. Les interfaces de configuration

3.1. CLI via port console et SSH

3.1.1. Connexion au port console

Se connecter avec un PC sur le port console du commutateur Juniper via un terminal vt100 ou bien une émulation (Hyperterminal Windows ou minicom pour Linux).

Paramétrage :

- vitesse : 9600 bps,
- taille : 8 bits,
- parité : non,
- bit d'arrêt : 1,
- contrôle de flux : non.

Une fois le câble connecté, appuyer sur « **Entrée** ». Pour un commutateur non configuré sorti d'usine, voici le prompt affiché :

```
Amnesiac (ttyu0)
login:
```

Pour se connecter sur un équipement non configuré sorti d'usine, il faut utiliser le login « **root** » :

```
Amnesiac (ttyu0)
login: root
--- JUNOS 9.2R3.5 built 2009-01-15 04:19:40 UTC
root@%
```

Par défaut, l'utilisateur « **root** » n'a pas de mot de passe. L'utilisateur root est l'administrateur par défaut du commutateur. En se connectant en root sur le port console, le mode shell est proposé par défaut. Il faut utiliser la commande « **cli »** pour accéder au mode opérationnel.

3.1.2. Connexion SSH

Pour se connecter en SSH, il faut que l'équipement possède une adresse IP de management et que le service SSH soit activé.

En se connectant en SSH, l'utilisateur est directement dans le mode opérationnel:

```
$ ssh admin@form-o3-cg1
admin@form-o3-cg1's password:
--- JUNOS 10.1S1.3 built 2010-03-31 20:03:32 UTC
{master:0}
admin@form-o3-cg1>
```

3.1.3. Navigation et changement de mode

Pour découvrir les commandes disponibles, taper : **?**

Le listing avec la description des commandes disponibles apparaît.

« ? » permet aussi de lister les paramètres d'une commande.

Exemple :

```
{master:0}
admin@form-o3-cg1> ping ?
Possible completions:
  <host>               Hostname or IP address of remote host
  bypass-routing       Bypass routing table, use specified interface
  count                Number of ping requests to send (1..2000000000 packets)
  detail               Display incoming interface of received packet
  do-not-fragment      Don't fragment echo request packets (IPv4)
  inet                 Force ping to IPv4 destination
  inet6                Force ping to IPv6 destination
```

La « complétion » des commandes se fait avec le touche **<TAB>**. Il est possible également de taper qu'une partie des commandes pour qu'elles soient reconnues à partir du moment où il n'y a plus d'ambiguité entre plusieurs commandes.

3.1.4. Modes de fonctionnement

Il y a différents modes de fonctionnement que l'on reconnaît grâce au prompt :

- **Mode opérationnel**

```
{master:0}
admin@form-o3-cg1>
```

Dans le mode opérationnel, vous pouvez entrer des commandes pour contrôler l'état matériel et logiciel du commutateur ainsi que que l'état réseau.

- **Mode configuration**

```
{master:0}[edit]
admin@form-o3-cg1#
```

Dans le mode configuration, vous pouvez définir toutes les propriétés JUNOS, comme la configuration réseau, l'administration du commutateur ou les paramètres matériels.

Pour entrer en mode configuration depuis le mode opérationnel, taper la commande «**configure**».

```
{master:0}
admin@form-o3-cg1> configure
Entering configuration mode
{master:0}[edit]
admin@form-o3-cg1#
```

Le **mode configuration possède plusieurs niveaux** et définit le **contexte** de configuration**.** Pour changer de contexte, il faut taper la commande **edit** suivie du contexte qu'on souhaite atteindre. Par exemple, pour configurer une interface :

```
{master:0}[edit]
admin@form-o3-cg1# edit interfaces
{master:0}[edit interfaces]
admin@form-o3-cg1# edit ge-0/0/13
{master:0}[edit interfaces ge-0/0/13]
```

Une fois dans le contexte de configuration `[edit interfaces ge-0/0/13]`, les commandes ne s'appliquent qu'à l'interface ge-0/0/13.

Pour appliquer un paramètre ou activer une fonctionnalité, il suffit alors d'utiliser la commande **set** suivie des arguments souhaités :

```
{master:0}[edit interfaces ge-0/0/13]
admin@form-o3-cg1# set description "lien serveur"
```

Pour sortir du contexte de l'interface ge-0/0/13 et remonter d'un cran au contexte des interfaces, il faut taper la commande **exit** ou **up** :

```
{master:0}[edit interfaces ge-0/0/13]
admin@form-o3-cg1# exit
{master:0}[edit interfaces]
admin@form-o3-cg1#
```

Pour remonter directement à la racine du contexte de configuration, taper la commande **top :**

```
{master:0}[edit interfaces ge-0/0/13]
admin@form-o3-cg1# top
{master:0}[edit]
admin@form-o3-cg1#
```

Pour quitter le mode configuration et revenir au mode opérationnel, taper à la racine du contexte la commande **exit** :

```
{master:0}[edit]
admin@form-o3-cg1# exit

Exiting configuration mode

{master:0}
admin@form-o3-cg1>
```

Pour quitter le mode opérationnel, taper la commande **exit** .

Si vous êtes connecté en SSH sur le commutateur, vous terminerez votre session SSH. Si vous êtes connecté depuis le port console, vous serez ramené au prompt d'identification ou vous basculerez en mode SHELL selon la configuration du commutateur.

- **Mode shell**

Le mode shell permet d'accéder au système d'exploitation du commutateur.

Attention : dans le mode shell vous aurez la possibilité de taper de nombreuses commande UNIX en mode administrateur. Ce mode ne fournit aucune protection en cas de mauvaise commande. Il est donc à utiliser avec extrême précaution. Nous déconseillons son utilisation sauf pour certaines commande de maintenance.

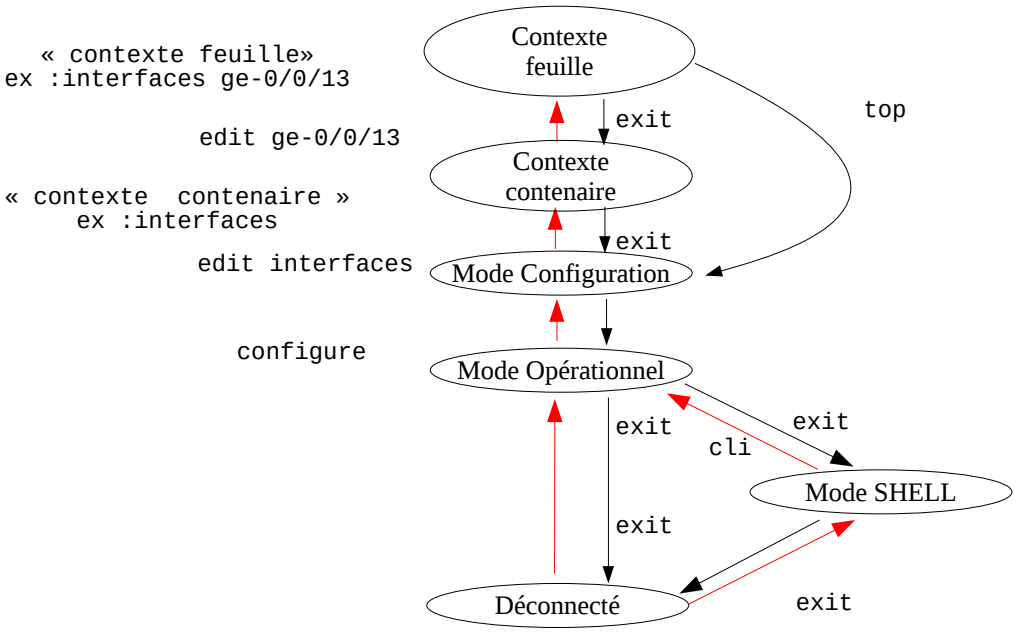
Depuis le mode opérationnel, pour accéder au mode shell, taper la commande **start shell** :

```
{master:0}
admin@form-o3-cg1> start shell
%
```

Selon la configuration du commutateur, depuis le mode déconnecté, vous pouvez arriver soit dans le mode opérationnel directement ou dans en premier temps dans le mode shell. Pour accéder au mode opérationnel de puis le mode shell, taper la commande **cli** :

```
% cli
{master:0}
admin@form-o3-cg1>
```

Le schéma ci-dessus récapitule les différents modes et les manières de passer de l'un à l'autre.



La commande «delete» :

Le «delete » permet de supprimer une ligne de configuration. Taper «delete» suivi des paramètres de configuration à supprimer. Exemple :

```
{master:0}[edit interfaces ge-0/0/13]
admin@form-o3-cg1# delete description
```

3.2. J-Web

L'interface « J-Web » est une interface graphique permettant de superviser, configurer, dépanner et gérer un commutateur Juniper via un navigateur web. J-Web autorise la configuration de quasiment tous les paramètres supportés par le commutateur, et permet donc de se passer de l'utilisation de la CLI. Toutefois il est important de maitriser et de connaître les commandes de base de la CLI lors d'un dépannage sur l'équipement via le port console.

J-Web fournit 3 méthodes pour configurer le commutateur :

- Le menu « **Configure** »
- Le menu « **CLI Terminal** »
- Le menu « **Point & Click CLI** »

3.2.1. Configuration HTTPS

Par défaut, seul le protocole HTTP est activé pour J-Web. Il convient d'activer le protocole HTTPS et désactiver HTTP pour sécuriser les communications entre le poste de travail de l'administrateur et le commutateur.

Sur votre poste de travail, générer un certificat SSL pour le serveur web HTTPS avec la commande « openssl » :

```
$ openssl req -x509 -nodes -newkey rsa:1024 -keyout filename.pem -out filename.pem
Generating a 1024 bit RSA private key
..++++++
.........................................++++++
writing new private key to 'filename.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:France
Locality Name (eg, city) []:Strasbourg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Université de Strasbourg
Organizational Unit Name (eg, section) []:Direction Informatique
Common Name (eg, YOUR name) []:Guillaume Schreiner
Email Address []:schreiner@unistra.fr
```

Copier le fichier sur commutateur avec SCP dans /var/tmp :

```
$ scp filename.pem admin@form-o3-cg1:
```

Sur le commutateur, configurer le certificat :

```
{master:0}[edit]
admin@form-o3-cg1# edit security certificates
{master:0}[edit security certificates]
admin@form-o3-cg1# set security certificates local moncertificat load-key-file
/var/tmp/filename.pem
```

Puis activer le mode HTTPS :

```
{master:0}[edit]
admin@form-o3-cg1# edit system services web-management
{master:0}[edit system services web-management]
admin@form-o3-cg1# set https local-certificate moncertificat
```

Désactiver également HTTP, l'utilisation conjointe de HTTP et HTTPS pour l'accès web peut générer des problèmes de connexion sur l'interface HTTPS.

```
{master:0}[edit system services web-management]
admin@form-o3-cg1# delete http
```

4. Gestion d'un Juniper via la CLI

4.1. Visualiser de la configuration

La configuration d'un commutateur ne peut être visualisée qu'en mode opérationnel ou configuration.

Depuis le mode opérationnel taper la commande **show configuration** :

```
{master:0}
admin@form-o3-cg1> show configuration
```

Depuis le mode configuration taper la commande **show** :

```
{master:0}
admin@form-o3-cg1# show
```

Il est possible de visualiser un contexte spécifique de la configuration. Par exemple pour visualiser directement la configuration de l'interface ge-0/0/13 :

```
{master:0}
admin@form-o3-cg1> show configuration interfaces ge-0/0/13
```

4.2. Appliquer/Annuler la configuration d'un commutateur

A la différence de l'IOS Cisco, le mode configuration de JUNOS n'applique pas directement les commandes tapées. Pour prendre en compte les nouveaux paramètres de configuration, il faut explicitement appliquer la configuration. Spécifiquement à JUNOS, des mécanismes de récupération de configuration permettent de revenir dans l'historique vers une configuration précédente stable.

Toutes les commandes suivantes s'effectuent en mode configuration.

Après avoir modifié tous les paramètres souhaités, les bonnes pratiques requièrent de lancer une commande de vérification pour vérifier l'intégrité de la configuration. Taper la commande **commit check** :

```
{master:0}[edit interfaces ge-0/0/13]
admin@form-o3-cg1# commit check
configuration check succeeds
```

Si un paramètre interfère dans la configuration, le test échoue. Tant que le mauvais paramètre n'est pas corrigé, il sera impossible d'appliquer la nouvelle configuration.

Bien que le test de vérification **commit check** ne présente aucune erreur logique, il se peut que la nouvelle configuration soit mauvaise. Notamment, l'administrateur risque de perdre la main sur son équipement. Les bonnes pratiques suggèrent de taper la commande **commit confirmed :**

```
{master:0}[edit interfaces ge-0/0/13]
admin@form-o3-cg1# commit confirmed
configuration check succeeds
commit confirmed will be automatically rolled back in 10 minutes unless confirmed
commit complete
```

Pendant 10 minutes, l'équipement va appliquer la nouvelle configuration. Si rien n'est confirmé avant, l'équipement va revenir à la configuration précédente à la fin de l'échéance. Cette commande est très pratique en cas d'erreur sur des équipements distants :

```
{master:0}[edit interfaces ge-0/0/13]
Broadcast Message from root@form-o3-cg1
        (no tty) at 12:28 CEST...
Commit was not confirmed; automatic rollback complete.
{master:0}[edit interfaces ge-0/0/13]
```

Si la configuration est bonne (vous n'avez pas perdue la main sur l'équipement distant), vous pouvez alors appliquer les changements définitivement avec la commande **commit :**

```
{master:0}[edit interfaces ge-0/0/13]
admin@form-o3-cg1# commit
configuration check succeeds commit complete
```

Dans le cas où les modifications ont été appliquées définitivement après une commande commit, il est possible de revenir en arrière dans un état d'une configuration précédente grâce à la commande **rollback**. Pour visualiser l'historique des configuration, taper **rollback ?**

```
{master:0}[edit]
admin@form-o3-cg1# rollback ?
Possible completions:
  <[Enter]>            Execute this command
  0      2010-06-03 12:28:14 CEST by root via other
  1      2010-06-03 12:17:54 CEST by admin via cli commit confirmed, rollback in 10mins
  2      2010-06-03 12:12:28 CEST by admin via cli
  3      2010-06-03 12:10:55 CEST by admin via cli
  4      2010-06-02 09:21:43 CEST by admin via cli
  5      2010-05-28 14:48:41 CEST by admin via cli
  6      2010-05-28 14:47:19 CEST by admin via cli
  7      2010-05-28 14:46:29 CEST by admin via cli
  8      2010-05-26 17:51:24 CEST by admin via junoscript
  9      2010-05-26 17:51:06 CEST by admin via junoscript
```

Pour récupérer la configuration précédente, taper **rollback** puis **commit :**

```
{master:0}[edit]
admin@form-o3-cg1# rollback
load complete
{master:0}[edit]
admin@form-o3-cg1# commit
configuration check succeeds commit complete
```

Pour récupérer la 3ème configuration précédente de l'historique, taper **rollback 3** puis **commit** :

```
{master:0}[edit]
admin@form-o3-cg1# rollback 3
load complete
{master:0}[edit]
admin@form-o3-cg1# commit
configuration check succeeds commit complete
```

4.3. Sauvegarder la configuration d'un commutateur

Il est **recommandé** de sauvegarder la configuration de votre JUNOS sur un serveur SSH. Cette méthode est beaucoup plus sûre et rapide qu'un copier/coller dans un fichier texte. Il est possible de télécharger la configuration complète du commutateur par SCP sur un serveur de sauvegarde. Pour cela, l'accès SSH sur le commutateur doit être activé.

Depuis le serveur de sauvegarde, taper la commande suivante :

```
$ scp admin@form-o3-cg1:/config/juniper.conf.gz .
```

Pour restaurer une configuration sauvegardée sur le serveur, il faut d'abord la copier sur le commutateur dans un répertoire temporaire :

```
$ scp  juniper.conf.gz admin@form-o3-cg1:/var/tmp
```

Puis sur le commutateur en mode configuration (à la racine de la configuration), taper la commande **load override** <fichier> pour écraser la configuration courante :

```
{master:0}[edit]
admin@form-o3-cg1# load override /config/juniper.conf.gz
load complete
{master:0}[edit]
admin@form-o3-cg1# commit
configuration check succeeds commit complete
```

4.4. Mise à jour du système (JUNOS)

La mise à jour de JUNOS permet de faire évoluer les fonctionnalités d'un commutateur et de corriger les bugs. Il existe chez Juniper un JUNOS spécifique par famille de commutateur. Il faut mettre à jour la version de JUNOS en utilisant celle préconisée par la Direction Informatique :

- Pour les EX2200 :

https://www-crc.u-strasbg.fr/ftp-cr/juniper/junos/EX2200/jinstall-ex-2200-10.1S1.3-domestic-signed.tgz

- Pour les EX3200 :

https://www-crc.u-strasbg.fr/ftp-cr/juniper/junos/EX3200/jinstall-ex-3200-10.1S1.3-domestic-signed.tgz

- Pour les EX4200 :

https://www-crc.u-strasbg.fr/ftp-cr/juniper/junos/EX4200/jinstall-ex-4200-10.1S1.3-domestic-signed.tgz

Attention : La mise à jour d'un JUNOS avec les procédures 1 et 2 nécessite qu'une adresse IP de management et une route par défaut aient été configurées.

4.4.1. Procédure 1 : mise à jour d'un EX via l'interface web

Se connecter à l'interface web du commutateur.

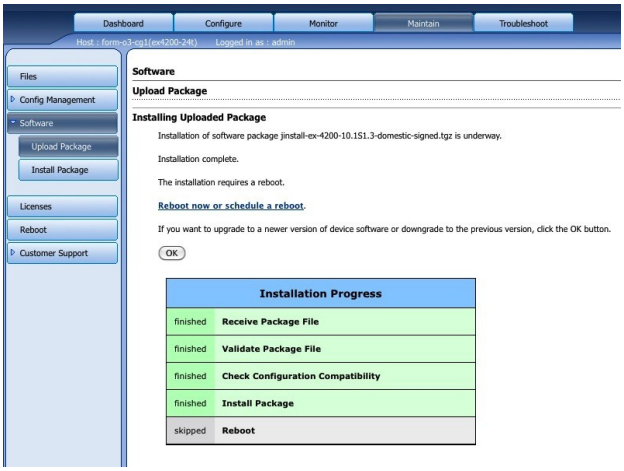
Aller dans l'onglet du haut **Maintain**.

Cliquer sur l'onglet de gauche **Software**, puis **Upload Package**.

Cliquer dans la case **File to Upload** ou sur le bouton **Parcourir...** et sélectionner dans l'arborescence de votre ordinateur l'image du commutateur à charger.

Si vous voulez automatiquement rebooter le commutateur sur la nouvelle version de JUNOS, cocher la case **Reboot If Required**.

Si vous n'avez pas cocher la case **Reboot If Required**, un écran avec les tests passés au vert devrait apparaitre :



Cliquer sur le lien **Reboot now or schedule a reboot** pour démarrer sur la nouvelle image. Après quelques minutes, le commutateur est de nouveau accessible.

4.4.2. Procédure 2 : mise à jour d'un EX en ligne de commande avec SSH/SCP

Copier l'image Juntes via SSH/SCP sur le commutateur dans le répertoire /var/tmp :

```
$ scp jinstall-ex-4200-10.1S1.3-domestic-signed.tgz admin@ip-commut:/var/tmp/
```

Se connecter en SSH sur le commutateur en mode CLI puis taper les commandes suivantes en mode opérationnel :

```
{master:0}
admin@form-o3-cg1> request system software validate /var/tmp/jinstall-ex-4200-10.1S1.3-domestic-signed.tgz
{master:0}
admin@form-o3-cg1> request system software add /var/tmp/jinstall-ex-4200-10.1S1.3-domestic-signed.tgz
{master:0}
admin@form-o3-cg1> request system reboot
```

Après quelques minutes, le commutateur est de nouveau accessible.

4.4.3. Procédure 3 : mise à jour d'un EX via le port console et une clé USB

Formater une clé en FAT et copier le nouveau firmware jinstall-ex-4200-10.1S1.3-domestic-signed.tgz sur la clé.

Brancher la clé USB à l'arrière du commutateur et se connecter sur le commutateur via le port console.

Si vous êtes en mode CLI, passer en mode SHELL :

```
{master:0}
admin@form-o3-cg1> start shell
```

Repérer le nom du volume de la clé USB grâce à la commande **dmesg**, le nom dépend de la version de JUNOS installée.

```
% dmesg
```

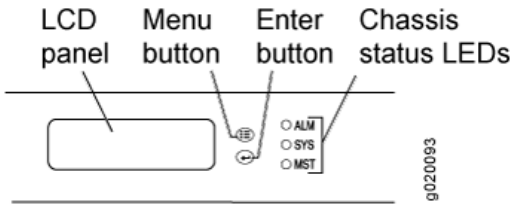
Puis monter la clé USB :

```
% mount -t msdos /dev/da1s1 /mnt/
% cd /mnt/
% cp jinstall-ex-4200-10.1S1.3-domestic-signed.tgz /var/tmp/
% cd
% umount /mnt
% cli
{master:0}
admin@form-o3-cg1> request system software validate /var/tmp/jinstall-ex-4200-10.1S1.3-domestic-signed.tgz
{master:0}
admin@form-o3-cg1> request system software add /var/tmp/jinstall-ex-4200-10.1S1.3-domestic-signed.tgz
{master:0}
admin@form-o3-cg1> request system reboot
```

Après quelques minutes, le commutateur est de nouveau accessible.

5. Configuration de base recommandée par la Direction Informatique

5.1. Démarrage d'un commutateur d'usine



Pour démarrer un commutateur de la gamme EX avec la configuration d'usine à partir du panneau LCD :

- Appuyer sur **Menu** jusqu'à **MAINTENANCE MENU**
- Appuyer sur **Enter** pour valider
- Appuyer sur **Menu** jusqu'à **FACTORY DEFAULT**
- Appuyer sur **Enter** pour valider
- Appuyer sur **Enter** pour confirmer la configuration et continuer avec **EZ Setup**

5.2. EZ Setup Juniper

EZ Setup est un assistant qui permet la configuration initiale et minimale du commutateur. Cet assistant va permettre d'attribuer un nom et une IP de management au commutateur.

Lancer l'assistant de configuration EZ Setup à partir du panneau LCD.

Branchez un PC avec un câble Ethernet sur le port 0 (ge-0/0/0) du commutateur.

Après avoir activé l'EZ Setup, le commutateur est configuré pour activer un serveur DHCP sur le l'interface ge-0/0/0. Le PC doit être configuré en client DHCP pour recevoir une IP dans la plage 192.168.1.2 – 192.168.1.253. Le commutateur prendra l'adresse IP 192.168.1.1 et activera une interface web.

Pour passer le commutateur en mode de configuration initiale :

- Appuyer sur **Menu** jusqu'à **MAINTENANCE MENU**.
- Appuyer sur **Enter** pour valider
- Appuyer sur **Menu** jusqu'à **ENTER EZ Setup**.
- Appuyer sur **Enter** pour valider
- Appuyer sur **Enter** pour confirmer le passage en mode configuration

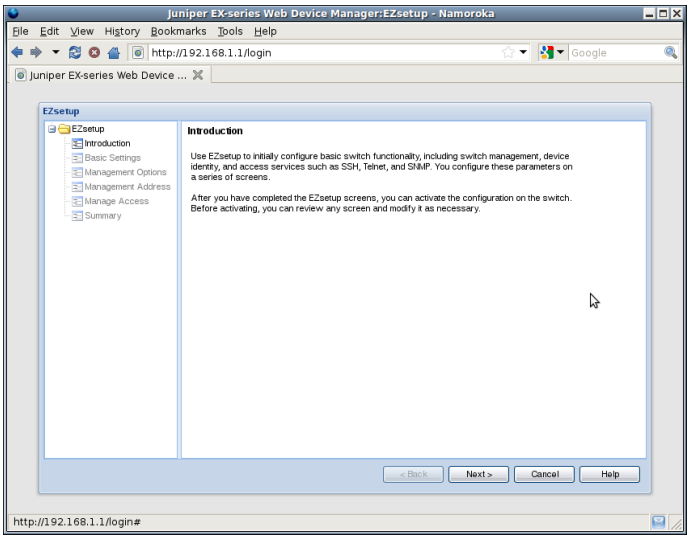
A partir de ce moment vous avez 10 minutes valider la configuration saisie via EZ Setup.

Passer ce délais le commutateur retourne dans sont mode de fonctionnement normale et l'interface web de configuration sera désactivé.

Depuis votre PC :

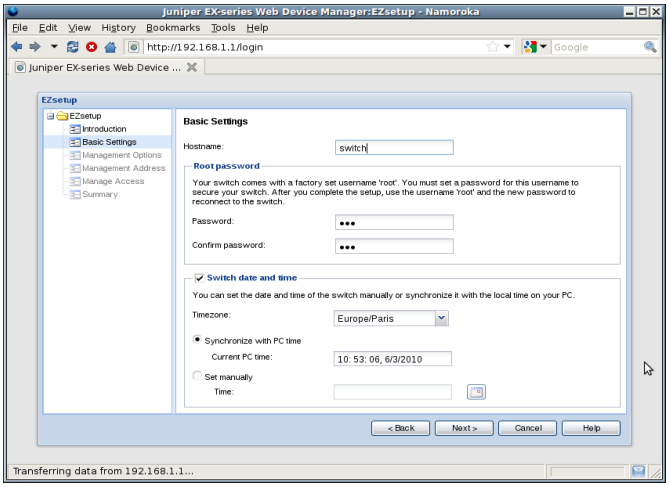
- Ouvrer un navigateur web avec l'URL http://192.168.1.1
- S'identifier avec les paramètres suivants
  - login : root
  - mot de passe : laisser vide
  - Puis valider.

Vous arrivez sur la page d'introduction de l' « EZ Setup »

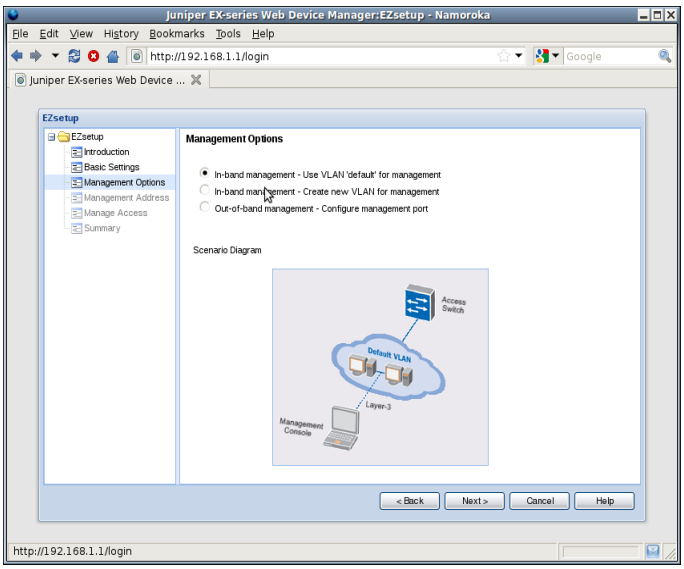


Sur la page « Basic Settings » modifier les informations suivantes :

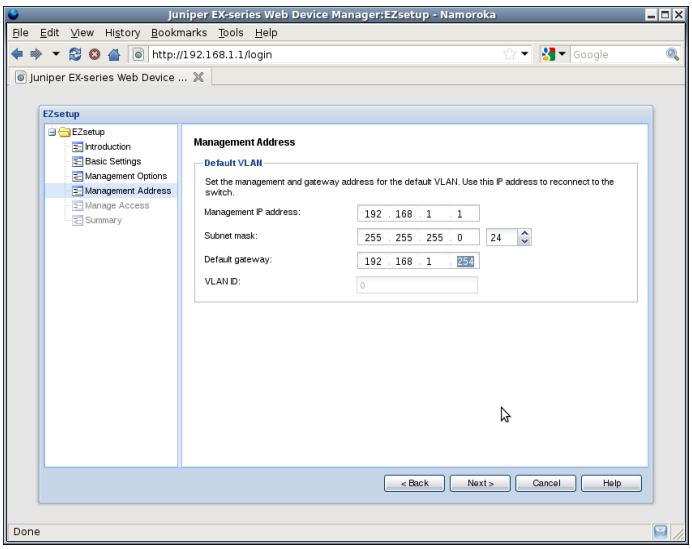
- nom du commutateur
- mot de passe root
- date et heure



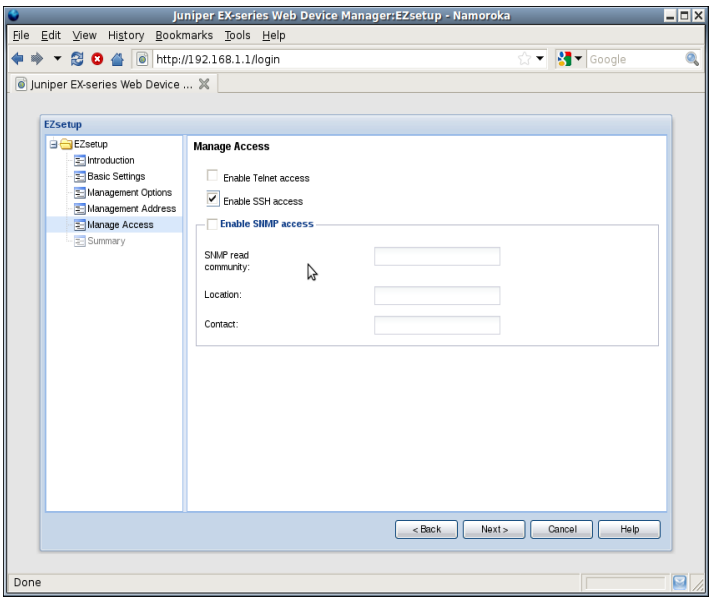
Sur la page « Management Options » sélectionner « In-band-management ».



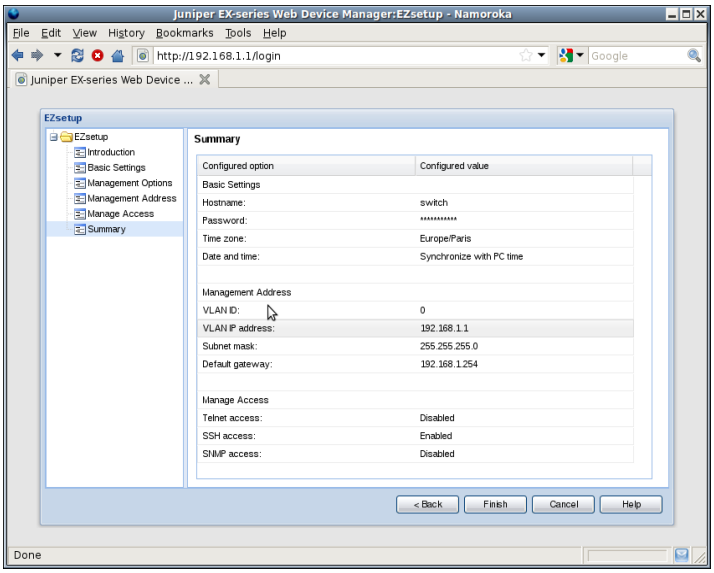
Sur la page « Management Address » compléter les informations IP de management du commutateur.



Sur la page « Manage Access » activer le protocole SSH pour l'accès au commutateur.



La page « Summary » récapitule les paramètres saisis. Après validation de cette page la configuration sera transférée sur le commutateur.



5.3. Configuration du nom de l'équipement

Depuis la CLI :

```
{master:0}[edit]
admin@form-o3-cg1# set system host-name host
```

Depuis l'interface WEB :

« Configure » → « System Properties » → « System Identity » → « Edit »

5.4. Configuration de l'heure et du fuseau horaire

Depuis la CLI :

```
{master:0}[edit]
admin@form-o3-cg1# set system time-zone Europe/Paris
```

Depuis l'interface WEB :

« Configure » → « System Properties » → « Date Time » → « Edit »

5.5. Configuration du client NTP

Pour la lecture des logs en cas de problème, il est important d'avoir l'heure exacte en synchronisant l'équipement sur un serveur NTP.

Mettre l'adresse IP du serveur ntp (ntp.u-strasbg.fr)

Depuis la CLI :

```
{master:0}[edit]
admin@form-o3-cg1# set system ntp server 130.79.14.177
```

Depuis l'interface WEB :

« Configure » → « System Properties » → « Date Time » → « Edit »

5.6. Résolution de noms DNS

L'activation de la résolution DNS sur le commutateur permettra de joindre des sites en se servant de leurs noms de domaines (ping ou traceroute).

Pour configurer le domaine DNS :

```
{master:0}[edit]
admin@form-o3-cg1# set system domain-name u-strasbg.fr
```

Pour configurer l'adresse IP du serveur DNS :

```
{master:0}[edit]
admin@form-o3-cg1# set system name-server 130.79.200.200
```

Pour configurer le domaine de recherche DNS :

```
{master:0}[edit]
admin@form-o3-cg1# set system domain-search u-strasbg.fr
```

5.7. Adresse IP de management commutateur

Affecter une adresse IP à un commutateur permet de se connecter à distance, de récupérer les logs sur un serveur syslog, d'interroger le commutateur en SNMP, de faire des transferts SCP et de mettre à jour JUNOS.

Dans une configuration, sans VLAN avec un seul réseau IP, nous affecterons une adresse IP au VLAN par défaut. Nous verrons par la suite dans le chapitre de gestion des VLAN d'autres méthodes.

Il n'est pas possible de le supprimer. Par défaut il est affecté à toutes les interfaces. Il faut choisir une adresse de votre réseau IP et l'appliquer au VLAN par défaut.

Déclaration de l'adresse IP de management :

Depuis la CLI :

En mode configuration, entrer dans l'unité 0 des interfaces vlans :

```
{master:0}[edit]
admin@form-o3-cg1# edit interface vlan unit 0 family inet
```

Déclarer l'adresse IP de management :

```
{master:0}[edit interface vlan unit 0 family inet]
admin@form-o3-cg1# set address X.X.X.X/Y
{master:0}[edit interface vlan unit 0 family inet]
admin@form-o3-cg1# top
```

Activer l'IP de management sur le VLAN par défaut

```
{master:0}[edit]
admin@form-o3-cg1# edit vlans default
{master:0}[edit vlans deflaut]
admin@form-o3-cg1# set l3-interface vlan.0
```

Si par la suite d'autres VLAN sont créés et que l'adresse de management doit faire partie de l'un de ces nouveaux VLAN, Créer le nouveau VLAN, appliquer l'adresse IP au nouveau VLAN :

```
{master:0}[edit]
admin@form-o3-cg1# edit interface vlan unit <vlan_tag> family inet
```

puis appliquer les commandes appliquées pour le VLAN par défaut.

Depuis l'interface WEB :

```
« Configure » → « System Properties » → « Management Access » → « Edit »
```

Le commutateur est maintenant accessible de puis le réseau.

Si les stations de gestion ne sont pas dans le même réseau IP, ou si l'on veut joindre le commutateur depuis n'importe ou sur Internet, ajouter une route par défaut comme sur n'importe quelle machine de votre réseau :

```
{master:0}[edit]
admin@form-o3-cg1# edit routing-options static
{master:0}[edit routing-options static]
admin@form-o3-cg1# set route 0.0.0.0/0 next-hop 130.79.X.Y
```

5.8. Le protocole LLDP (Logical Link Discovery Protocol)

LLDP permet de récupérer des informations sur les commutateurs voisins supportant ces protocoles. Ces options peuvent nuire à la sécurité. Des utilisateurs non autorisés peuvent récupérer des informations simplement en se connectant sur un port du commutateur si celui-ci est mal configuré. La Direction Informatique recommande de désactiver LLDP et LLDP-MED avec les commandes suivantes :

```
{master:0}[edit]
admin@form-o3-cg1# set protocols lldp disable
{master:0}[edit]
admin@form-o3-cg1# set protocols lldp-med disable
```

5.9. Configuration des logs sur le commutateur

Il y a 8 niveaux de criticité pour les logs : *emergency*, *alert*, *crtitical*, *error*, *warning*, *notice*, *info* et *debug*. *Emergency* est le niveau le plus grave (explosion du commutateur), *debug* le moins grave et le plus explicite.

La configuration par défaut est la suivante :

- log sur la console de tous les utilisateurs toutes les alertes emergency.
- log dans le fichier *message* toutes les alertes de criticité *notice* et les messages de criticité *info* pour toute ce qui concerne l'authentification.
- log dans le fichier *interactive-commands* toutes les alertes pour les messages concernant les commandes exécutées sur la CLI
- les fichiers sont archivés après avoir attend la taille de 128 Ko (ajout d'un index au nom de fichier).
- les archives conservent 10 index de fichiers.

Pour paramétrer le nombre de fichiers archives :

```
{master:0}[edit]
admin@form-o3-cg1# edit system syslog archive
{master:0}[edit system syslog archive]
admin@form-o3-cg1# set files 15
```

Pour paramétrer la taille des fichiers en octets devant être archiver, par exemple pour augmenter la taille à 512 Ko :

```
{master:0}[edit system syslog archive]
admin@form-o3-cg1# set size 524288
```

Rends les archives consultable pour tous les utilisateurs :

```
{master:0}[edit system syslog archive]
admin@form-o3-cg1# set world-readable
```

Pour envoyer tous les logs à un serveur syslog (udp/514), ajouter la ligne :

```
{master:0}[edit]
admin@form-o3-cg1# edit system syslog
{master:0}[edit system syslog ]
admin@form-o3-cg1# set host <IP_SERVEUR_SYSLOG> any any
```

5.10. Configuration de la Rescue Configuration

Si par inadvertance vous valider une configuration qui interdit tous les accès au management du commutateur, la Rescue Configuration est une alternative rapide pour restaurer rapidement une configuration que vous savez fonctionnelle.

5.10.1. Sauvegarde et suppression de la Rescue Configuration

Pour disposer de cette option il vous faudra au préalable définir la Rescue Configuration à partir d'une configuration que vous savez valide.

Créer la Rescue Configuration

Depuis la CLI :

```
{master:0}[edit]
admin@form-o3-cg1# run request system configuration rescue save
```

Depuis l'interface WEB :

« Maintain » → « Config Management » → « Rescue » → « Set rescue configuration »

Supprimer la Rescue Configuration

Depuis la CLI :

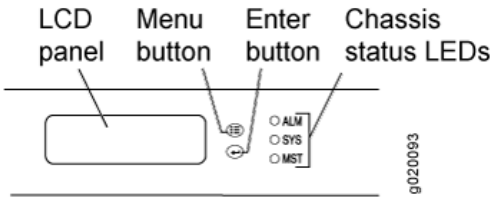
```
{master:0}[edit]
admin@form-o3-cg1# run request system configuration rescue delete
```

Depuis l'interface WEB :

« Maintain » → « Config Management » → « Rescue » → « Delete rescue configuration »

5.10.2. Restauration de la Rescue Configuration

La restauration de la Rescue Configuration se fait à partir du panneau de contrôle du commutateur.



Pour restaurer la dernière Rescue Configuration d'un commutateur (gamme EX 3200 ou supérieur) à partir du panneau LCD :

- Appuyer sur **Menu** jusqu'à **MAINTENANCE MENU**
- Appuyer sur **Enter** pour valider
- Appuyer sur **Menu** jusqu'à **LOAD RESCUE**
- Appuyer sur **Enter** pour valider
- Appuyer sur **Enter** pour confirmer la restauration de la Rescue Configuration.

5.11. Gestion des utilisateurs

5.11.1. Changer le mot de passe « root »

L'utilisateur « root » est le super utilisateur par défaut du commutateur. En configuration d'usine, « root » n'a pas de mot de passe. Lors d'un EZ Setup, le mot de passe « root » est obligatoirement défini.

Pour changer ce mot de passe, taper :

```
{master:0}[edit]
admin@form-o3-cg1# edit system root-authentication
{master:0}[edit system root-authentication]
admin@form-o3-cg1# set plain-text-password
New password:
Retype new password:
```

5.11.2. Ajouter/supprimer des utilisateurs

Les différents privilèges possibles pour les utilisateurs sont :

- **super-user** : l'utilisateur a tout les droit et peut entrer en mode configuration
- **operator** : l'utilisateur est limité au mode opérateur avec possibilité de changer l'état des tables de commutation (par ex. commande **clear**)
- **read-only** : l'utilisateur est limité au mode opérateur pour des commandes de diagnostics uniquement
- **unauthorized** : l'utilisateur n'a aucun droit mais arrive encore à se connecter à l'équipement

Pour ajouter un utilisateur sur le commutateur, taper les commandes suivantes en remplaçant «identifiant» par le nom de l'utilisateur. Remplacer <privilège> par l'une des 4 classes d'utilisateurs possibles. Enfin, taper le mot de passe souhaité :

```
{master:0}[edit]
admin@form-o3-cg1# edit system login user <identifiant>
{master:0}[edit system login user <identifiant>]
admin@form-o3-cg1# set class <privilège>
{master:0}[edit system login <identifiant>]
admin@form-o3-cg1# set authentication plain-text-password
New password:
Retype new password:
```

6. Configuration des interfaces

Toutes les interfaces sur les Juniper EX sont du type Gigabit Ethernet ou 10 Gigabit Ethernet.

Voici un aperçu des longueurs et du choix du média à utiliser en fonction de la distance :

Distance max.	***Type de connexion***
90 m	Module 1000 Base T sur cuivre
220 m	Module SX/SR sur FO multimode
550 m	Module LX/LH sur FO multimode
10 km	Module LX/LH/LR sur FO monomode
40 km	Module ER sur FO monomode

Pour les câbles cuivre, préférer des « catégorie 6 (gigabit)».

6.1. Configuration Duplex et vitesse d'une interface

Sur les commutateurs, 4 vitesses sont possibles en fonction des ports :

- 10 Mbs
- 100 Mbs
- 1 Gbs
- 10 Gbs

Il y a 2 modes de fonctionnement :

- Half Duplex : Les émissions et les réceptions sur un port arrivent alternativement. C'est le cas lors d'une connexion à un Hub.
- Full Duplex : Les émissions et réceptions sur un port se font en même temps. C'est le mode le plus optimisé et le plus couramment utilisé sur les commutateurs.

Principe de l'auto-négociation **FLP** (Fast Link Pulse qui teste l'intégrité du lien) : Teste le mode de fonctionnement le plus élevé vers le plus bas. Exemple pour une interface 100 Mbs :

```
100 Full Duplex → 100 Half Duplex → 10 Full Duplex → 10 Half Duplex
```

Dans la majorité des cas l'auto-négociation fonctionne et configure le port de manière optimale.

Par défaut, les **auto-négociations** de la vitesse et du duplex sont activées sur les interfaces **Gigabit Ethernet** des commutateurs Juniper.

La vitesse par défaut des interfaces **10-Gigabit Ethernet** est 10 G et le mode par défaut est Full Duplex. Il n'y a pas d'auto-négociation possible.

Sur les commutateurs Juniper la configuration des paramètres de l'interface Ethernet se fait dans le contexte **ether-option** de chaque interface :

```
{master:0}[edit]
admin@form-o3-cg1# edit interfaces ge-fpc/pic/port ether-options
{master:0}[edit interfaces ge-fpc/pic/portether-options]
admin@form-o3-cg1# set auto-negotiation
```

Les paramètres du contexte **ether-options** vous permettent de changer les configurations suivantes :

- **802.3ad** : indique une interface agrégée
- **auto-negotiation** : active ou désactive l'auto-négociation
- **link-mode** : configure le duplex (**automatic**, **full-duplex**, **half-duplex**)
- **speed** : configure la vitesse (**10m**, **100m**, **1g**, **auto-negociation**)

La majorité des problèmes se situe au niveau du brochage des câbles ou de leur qualité, d'où le conseil d'utiliser toujours des câbles Ethernet de qualité. Il y a 2 types de câbles Ethernet :

- Câble droit : à utiliser pour raccorder un commutateur à un routeur ou à un poste client.
- Câble croisé : à utiliser pour raccorder 2 commutateurs, 2 PC ou 2 routeurs. Bref, du matériel de même nature.

Dans certains cas, on peut rencontrer des problèmes, souvent entre des commutateurs de marques différentes ou avec une carte réseau d'un poste client configurée avec des options pas toujours standards.

En cas de problèmes avec l'auto-négociation, il est conseillé de forcer la vitesse du port.

Attention! Si la vitesse et le duplex sont forcés d'un côté, il faut faire de même de l'autre côté du lien.

Commandes à passer (par défaut, même si ce n'est pas affiché, un port est en auto-négociation) :

```
{master:0}[edit]
admin@form-o3-cg1# edit interfaces ge-fpc/pic/port ether-options
{master:0}[edit interfaces ge-fpc/pic/port ether-options]
admin@form-o3-cg1# set speed 10m
{master:0}[edit interfaces ge-fpc/pic/port ether-options]
admin@form-o3-cg1# set speed 100m

{master:0}[edit interfaces ge-fpc/pic/port ether-options]
admin@form-o3-cg1# set speed 1g
{master:0}[edit interfaces ge-fpc/pic/port ether-options]
admin@form-o3-cg1# set speed auto-negotiation

{master:0}[edit interfaces ge-fpc/pic/port ether-options]
admin@form-o3-cg1# set link-mode half-duplex
{master:0}[edit interfaces ge-fpc/pic/port ether-options]
admin@form-o3-cg1# set link-mode full-duplex
{master:0}[edit interfaces ge-fpc/pic/port ether-options]
admin@form-o3-cg1# set link-mode automatic
```

Pour des raisons de sécurité, il est important de désactiver un port non utilisé avec l'option «disable» et de rajouter ces quelques configurations par défaut dans les interfaces.

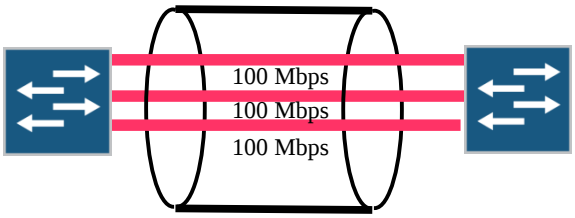
```
master:0}[edit]
admin@form-o3-cg1# set interfaces ge-fpc/pic/port disable
```

Pour réactiver une interface il faut enlever l'option «disable».

```
master:0}[edit]
admin@form-o3-cg1# edit interfaces ge-fpc/pic/port
master:0}[edit interfaces ge-fpc/pic/port]
admin@form-o3-cg1# delete disable
```

6.2. Agrégation de liens 802.3ad

L'agrégation de liens, appelée Etherchannel, permet à plusieurs liens physiques d'être vus comme un seul. Ceci est utile en cas de saturation ou pour assurer une redondance en cas de coupure de lien.



Lien virtuel à **300** Mbps

Nous utilisons pour agréger les liens le protocole LACP (Link Aggregate Control Protocol) normalisé (IEEE 802.3ad).

Paramétrage du nombre d'agrégats **N** sur le commutateur :

```
{master:0}[edit]
admin@form-o3-cg1# edit chassis aggregated-devices
{master:0}[edit chassis aggregated-devices]
admin@form-o3-cg1# set ethernet device-count N
```

Attention, N définit le nombre maximum d'agrégats et également le numéro d'interface de l'agrégat le plus élevé. N est limité à **64**. Par exemple, avec N=5, la plus grande interface d'agrégat sera **ae4**.

Création d'une interface virtuelle **ae0** :

```
{master:0}[edit]
admin@form-o3-cg1# edit interfaces ae0
{master:0}[edit interfaces ae0]
admin@form-o3-cg1# set aggregated-ether-options link-speed 1g
{master:0}[edit interfaces ae0]
admin@form-o3-cg1# set aggregated-ether-options lacp active
{master:0}[edit interfaces ae0]
admin@form-o3-cg1# set unit 0 family ethernet-switching
```

Agrégation d'interfaces sur la pseudo-interface **ae0** :

```
{master:0}[edit]
admin@form-o3-cg1# edit interfaces ge-fpc/pic/port
{master:0}[edit interfaces ge-fpc/pic/port]
admin@form-o3-cg1# set ether-options 802.3ad ae0
```

Enfin, on applique les configurations propres à une interface dans l'agrégat. Celles-ci sont automatiquement répliquées dans la configuration individuelle de chaque interface physique.

```
{master:0}[edit]
admin@form-o3-cg1# edit interfaces ae0
{master:0}[edit interfaces ae0]
admin@form-o3-cg1# set unit 0 family ethernet-switching port-mode trunk
{master:0}[edit interfaces ae0]
admin@form-o3-cg1# set unit 0 family ethernet-switching vlan members "listes des vlans
taggés sur cette interface"
```

6.3. Configuration OAM Link Fault Management

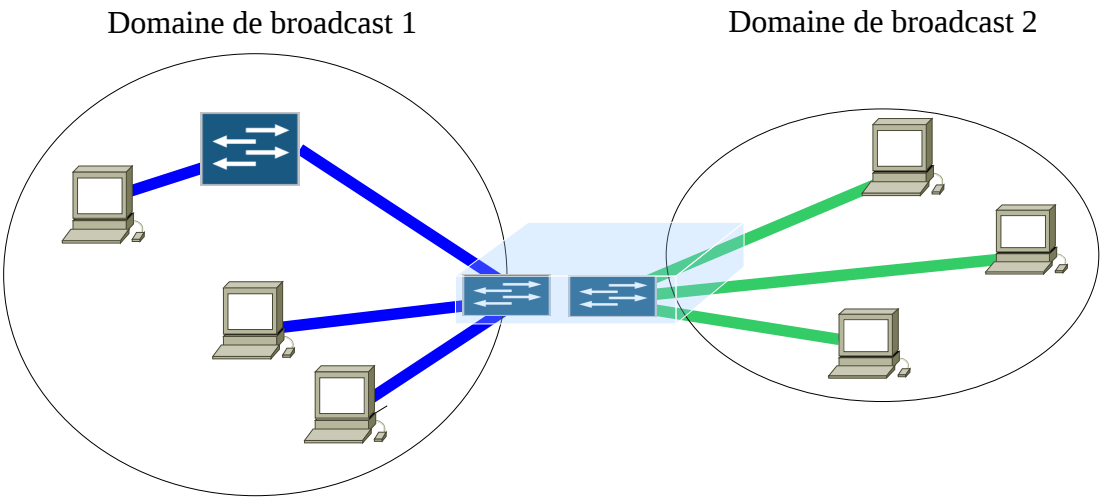
L'activation du paramétrage OAM Link Fault Management 802.3ah permet, sur les équipements Juniper EX3200 et EX4200, de détecter les liens unidirectionnel de niveau 2 et de désactiver les ports ou d'envoyer une alarme quand une telle condition est détectée. L'OAM LFM est l'équivalent de l'option UDLD (UniDirectional Link Detection) sur les équipements Cisco. Cette option aide à détecter et prévenir les problèmes de câblage fibre et les problèmes matériels de l'équipement.

Pour activer l'OAM LFM sur une interface :

```
{master:0}[edit]
admin@form-o3-cg1# edit protocols oam ethernet link-fault-management
{master:0}[edit protocols oam ethernet link-fault-management]
admin@form-o3-cg1# set interface ge-1/1/0 pdu-interval 1000
{master:0}[edit protocols oam ethernet link-fault-management]
admin@form-o3-cg1# set interface ge-1/1/0 pdu-threshold 5
```

7. Création de VLAN et de liens trunk

Un **VLAN** est un **réseau commuté logique** de niveau 2 rassemblant un nombre de machines indépendamment de l'architecture physique. Un commutateur peut gérer plusieurs VLAN totalement indépendants les uns par rapport aux autres. Par exemple : Un commutateur sur lequel sont configurés 3 VLAN peut être vu comme 3 commutateurs indépendants. Pour que les informations transitent d'un VLAN à l'autre, il faut faire du routage (niveau 3) à l'aide d'un routeur ou d'un firewall.



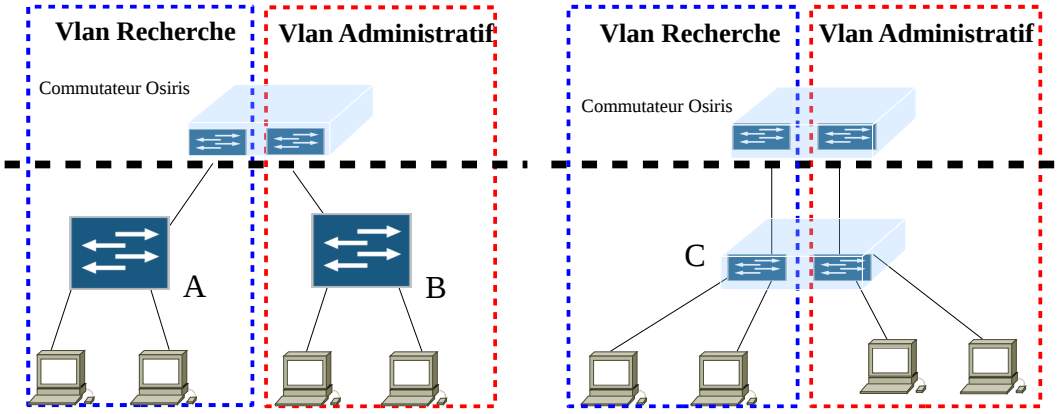
Quand faut-il utiliser des VLAN ?

- Quand on veut utiliser un seul commutateur pour plusieurs réseaux totalement indépendants et qui ne doivent pas se mélanger (administratif, recherche, enseignement, réseaux IP ...),
- Quand on veut apporter plus de sécurité au niveau IP. Les machines d'un même réseau IP ne sont connectées que sur le VLAN qui leur est attribué. Cela permet aux utilisateurs de ne pas introduire leurs machines dans un réseau qui ne leur est pas destiné.
- Si on veut limiter le trafic de broadcast, de cette façon ce trafic ne se limite qu'aux machines du VLAN (DHCP, requêtes ARP...). Pratique en cas d'infection d'un réseau par un virus.

Recommandation : Si plusieurs réseaux IP sont connectés sur un commutateur, il est important d'affecter chaque réseau à un VLAN.

Sur la majorité des sites Osiris, 2 types de réseaux sont présents : le réseau de enseignement/recherche et le réseau administratif. À la sortie du commutateur Osiris d'entrée de bâtiment, la Direction Informatique fournit **2 connexions** sur 2 interfaces, une pour chaque réseau.

Il y a donc en fonction des moyens 2 configurations possibles :

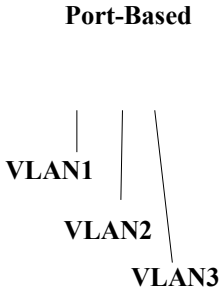


Sur le schéma de gauche, le réseau de recherche (commutateur A) est physiquement séparé du réseau administratif (commutateur B). La création de VLAN sur les commutateurs n'est pas nécessaire.

Sur le schéma de droite, le réseau de recherche est connecté sur le même commutateur (C) que le réseau administratif (c'est souvent le cas). Il faut impérativement les séparer en créant deux VLAN. Le premier pour les machines de la recherche. L'autre pour les machines administratives.

7.1. Configuration de VLAN par port

Chaque port d'un commutateur est affecté à un VLAN. C'est la configuration la plus utilisée.



Créer un VLAN :

Toutes les interfaces physiques sont affectées dans le vlan par défaut « **default** ». Contrairement à Cisco, le VLAN par défaut chez Juniper **n'a pas de vlan-id associé**. Pour éviter toute erreur, il est conseillé de numéroter les VLANs à partir de 2.

```
{master:0}[edit]
admin@form-o3-cg1# set vlans rch
{master:0}[edit]
admin@form-o3-cg1# edit vlans rch
{master:0}[edit vlans rch]
admin@form-o3-cg1# set description « reseau recherche »
{master:0}[edit vlans rch]
admin@form-o3-cg1# set vlan-id 2
```

Affecter une adresse IP à un VLAN :

```
{master:0}[edit vlans rch]
admin@form-o3-cg1# set l3-interface vlan.2
{master:0}[edit vlans rch]
admin@form-o3-cg1# top
{master:0}[edit]
admin@form-o3-cg1# set interface vlan unit 2 family inet address 10.1.2.3/24
```

Visualiser la configuration des VLANs :

```
{master:0}[edit]
admin@form-o3-cg1# show vlans
```

Visualiser les VLANs avec leur ports associés (en mode opérationnel) :

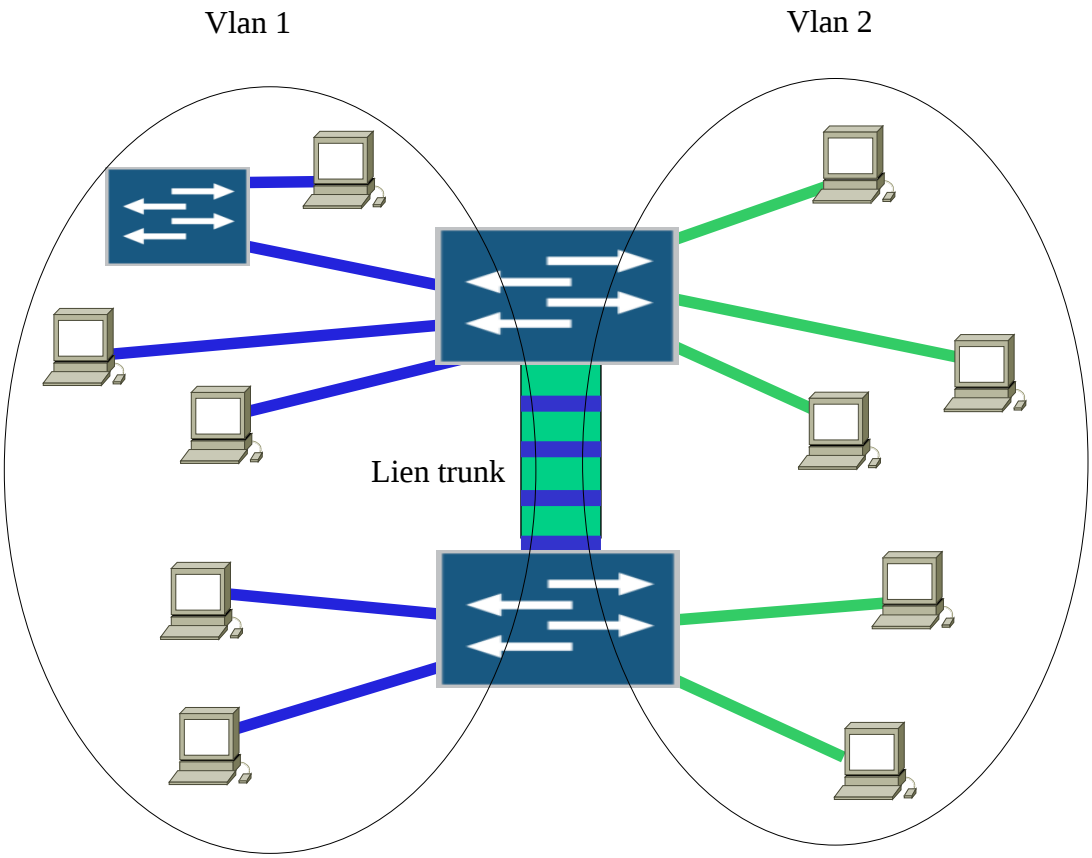
```
{master:0}
admin@form-o3-cg1> show vlans
```

Mettre un port en mode access et lui associer un VLAN :

```
{master:0}[edit]
admin@form-o3-cg1# set interface <interface name> unit <unit number> family ethernet-
switching port-mode access
{master:0}[edit]
admin@form-o3-cg1# set interface <interface name> unit <unit number> family ethernet-
switching vlan members <nom du vlan ou vlan-id>
```

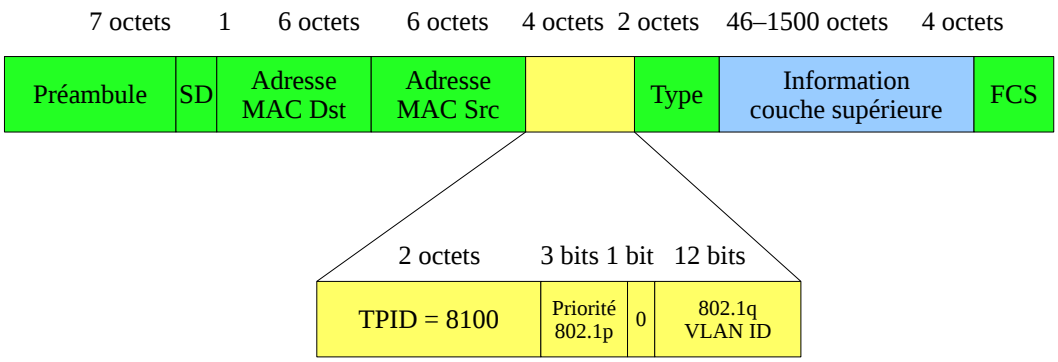
7.2. Configuration d'un lien trunk 802.1q

Souvent un même VLAN doit se trouver géographiquement à plusieurs endroits, donc sur plusieurs commutateurs. Au lieu de raccorder les commutateurs avec autant de liens physiques qu'il y a de VLAN, on peut les raccorder à l'aide d'un lien « trunk » qui va transporter tous les VLAN configurés sur les différents commutateurs.



Un lien « trunk » doit faire passer les trames de tous les VLAN sur le même support physique sans pour autant provoquer une perte d'étanchéité de ces derniers. Pour cela, chaque trame Ethernet est « taguée » avec le numéro de VLAN à qui elle appartient.

Voici la représentation d'une trame taguée :



4 octets sont insérés entre le champ « Adresse MAC source » et « Type ». En voici la description :

- TPID : Tag Protocol Indentifier. La valeur est de 8100, indiquant que la trame est taguée et que sa taille maximale passe de 1518 à 1522 octets.
- Priorité 802.1p : Il s'agit d'un champ de priorité, 000 pour la priorité la plus faible, 111 pour la priorité la plus haute.
- 802.1q VLAN ID : Indique le numéro du VLAN à qui appartient la trame Ethernet.

Configurer un port en mode trunk et lui ajouter un ou plusieurs VLANs :

```
{master:0}[edit]
admin@form-o3-cg1# set interface <interface name> unit <unit number> family
ethernet-switching vlan members <nom des vlan> (ou all pour tous les affecter)

{master:0}[edit]
admin@form-o3-cg1# set interface <interface name> unit <unit number> family
ethernet-switching port-mode trunk
```

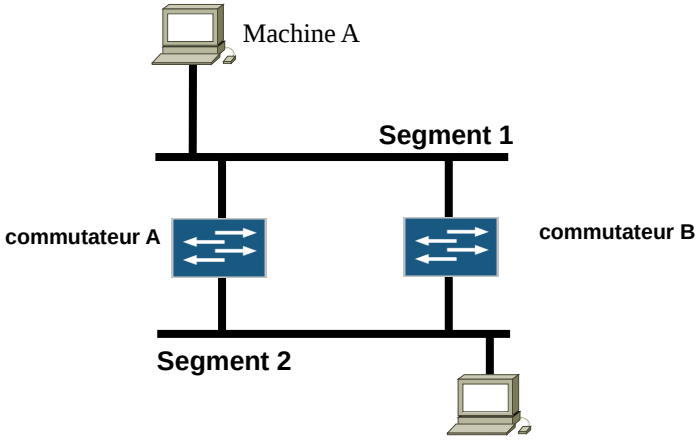
8. Gestion des Liaisons redondantes niveau 2 : Spanning Tree Protocol

8.1. Généralités

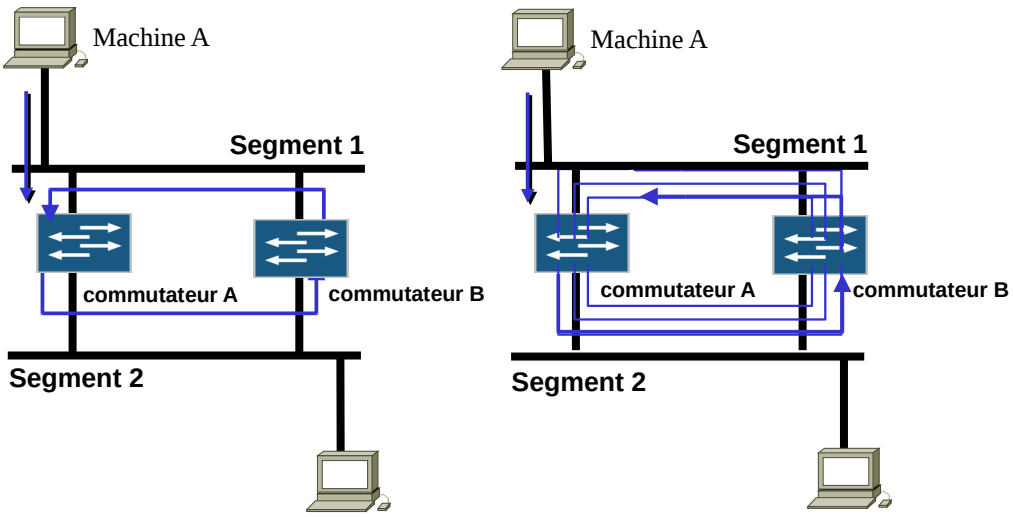
Comme nous avons pu le constater dans le chapitre 1, un commutateur diffuse sur tous ses ports les trames ayant pour destination une adresse de broadcast ou une adresse inconnue.

En cas de formation de boucle physique volontairement (pour assurer une redondance) ou involontairement (erreur de câblage), le trafic peut exploser dès la première trame de broadcast ou à destination inconnue.

Exemple : Voici une architecture où une boucle physique est créée.



Une trame de broadcast est envoyée par la machine A. La trame arrive sur le commutateur A, puis est retransmise vers le commutateur B sur le segment 2. Comme il s'agit d'un broadcast, le commutateur B retransmet la trame sur le port du segment 1 et ainsi de suite. Une boucle infinie est formée. On appelle cela une **tempête de broadcasts.** Des attaques de ce type existent. Un utilisateur mal intentionné peut envoyer des broadcasts en rafale.



8.2. La solution : Spanning Tree Protocol – 802.1d

Le Spanning Tree Protocol sert à éviter la formation de boucles et à assurer la redondance dans un réseau de niveau 2.

Ce protocole est **activé par défaut sur tous les commutateurs Juniper**. Lors du démarrage d'un commutateur neuf avec sa configuration d'usine, les configurations du spanning tree sont déjà actives. Le protocole de spanning tree utilisé par défaut sur les Juniper est **RSTP (Rapid STP).**

STP est un protocole de gestion de couche 2 qui détermine les chemins redondants (boucles logiques) d'un réseau et les supprime. Il a pour but de créer un arbre de diffusion.

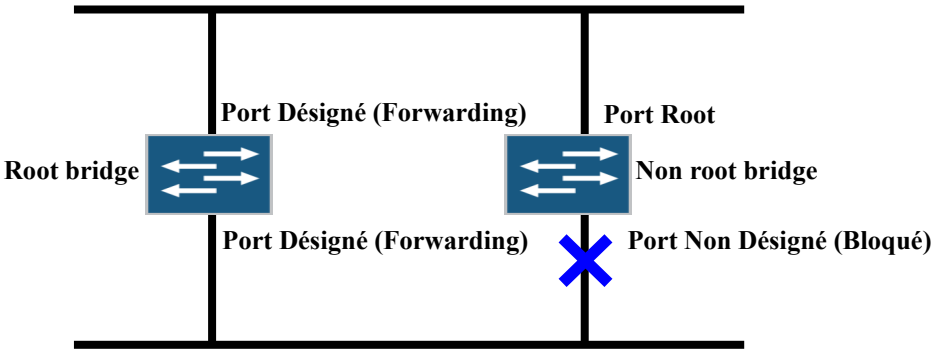
Pour rappel, le protocole de spanning tree par défaut sur les commutateurs Cisco est PVST (Per VLAN STP).

Le protocole par défaut RSTP sur Juniper ne dispose que d'une seule instance pour tous les VLANs contrairement au protocole PVST des commutateurs Cisco qui disposent d'une instance par VLAN.

Pour garantir l'interopérabilité entre les commutateurs Juniper et Cisco, l'utilisation du protocole **VSTP** sur les équipements Juniper et **PVST** sur les équipements Cisco est **obligatoire**.

Les commandes pour désactiver RSTP puis activer VSTP sur Juniper sont les suivantes :

```
{master:0}[edit]
admin@form-o3-cg1# delete protocols rstp
{master:0}[edit]
admin@form-o3-cg1# set protocols vstp vlan all
```



Le protocole STP utilise un algorithme distribué qui sélectionne un commutateur (**root bridge**), comme étant la racine d'un arbre associé à la topologie courante. Le spanning tree du réseau Osiris est configuré de manière à ce que le Root Bridge se trouve toujours sur un commutateur de coeur (jamais dans les réseaux des composants). Le spanning Tree assigne des rôles aux ports selon la fonction de chacun dans la topologie courante.

Chaque **port** peut prendre **2 états finaux** : **Forwarding** (les trames transitent par ce port) - **Blocking** (les trames ne transitent pas par ce port).

Il y a aussi **2 types de ports** : **Port désigné** et **Port Root**. Un port désigné est un port qui ne mène pas vers le Root Bridge. Un port Root est un port qui mène vers le Root Bridge.

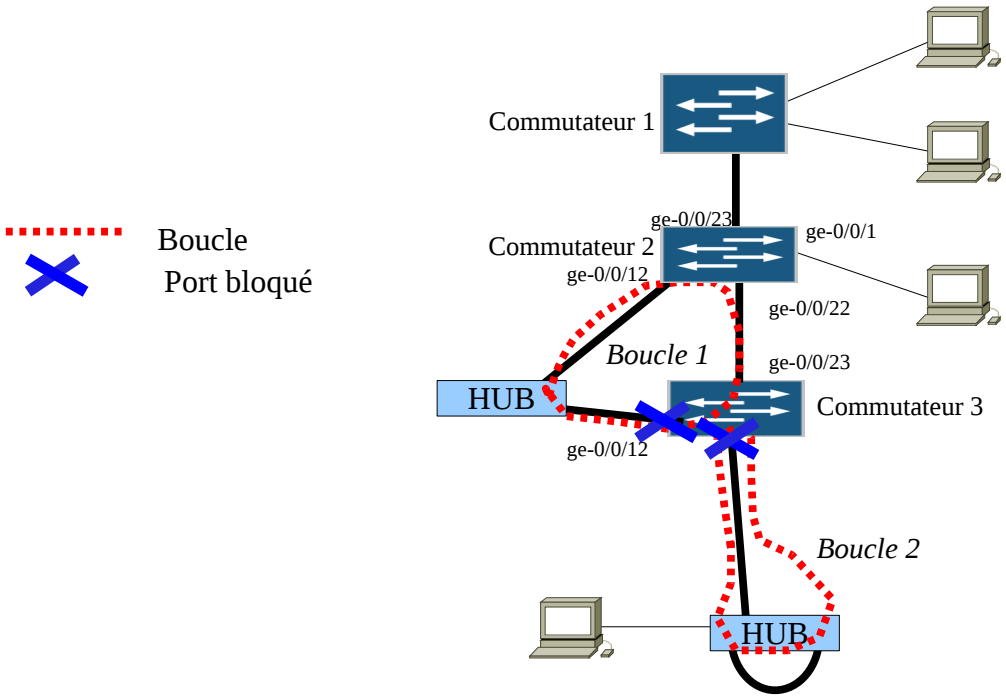
Root Bridge = Commutateur avec le plus petit Bridge ID

Bridge ID = Bridge priority + adresse MAC

Bridge priority par défaut = 32768

8.3. Utilité du Spanning Tree

Dans bon nombre d'installations réseaux, les commutateurs sont fréquemment connectés en cascade. Il est très facile de créer des boucles sur le réseau souvent de manière accidentelle par l'ajout de HUB de manière non contrôlée ou par un mauvais câblage (rebouclage).



Dans ces cas là, le Spanning Tree va entrer en action et **bloquer des ports** sur l'un des commutateurs touché par une boucle. Une partie du réseau ne sera plus opérationnelle afin de protéger tout le reste.

Attention, le Spanning Tree se base sur les priorités appliquées aux commutateurs soit par leur configuration ou automatiquement avec les adresses MAC. Le port bloqué dans la boucle 1 (ge-0/0/12 sur commutateur 3) peut aussi se trouver sur le lien entre le commutateur 2 et le commutateur 3. Ici, ce n'est pas le cas car un Hub à une priorité moindre qu'un commutateur et ne fait que du half duplex.

En cas de problème, voici donc une commande très utile pour visualiser la configuration du Spanning Tree, « **run show spanning-tree interface** ».

Cette commande affiche un listing des interfaces avec leur rôle, leur statut et le coût du lien (4). On constate que l'interface ge-0/0/22 sur le commutateur 3 est celle qui mène vers la racine (colonne *Role*) et que l'interface ge-0/0/12 est connectée au Hub car son coût (2000000) est beaucoup plus élevé. Enfin, le commutateur 2 est racine car tous ses ports ont un rôle DESG.

Cet commande montre également l'état du Spanning Tree sur les commutateurs 2 et 3 lorsque l'on crée une boucle avec un HUB (boucle 1). Les numéros de ports sont inscrits sur le schéma.

Le Spanning Tree s'applique au VLAN 2 (1) qui peut être assimilé à un VLAN d'une entité d'enseignement et recherche.

On peut voir l'identifiant du Root Bridge (2) et (5). Il est bien sûr le même sur les 2 commutateurs. À chaque identifiant de Root Bridge est associé un port, qui permet d'attendre le Root Bridge.

Sur le commutateur 2 (Racine) :

```
{master:0}
admin@commutateur2> show spanning-tree interface

Spanning tree interface parameters for VLAN 2 (1)
                                              (5)
Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID         bridge ID          Cost
ge-0/0/12.0    128:525      128:525  32770.b0c69a6652c0   2000000  FWD   DESG
ge-0/0/23.0    128:536      128:536  32770.b0c69a6652c0     20000  FWD   DESG

Spanning tree interface parameters for VLAN 3

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID         bridge ID          Cost
ge-0/0/23.0    128:536      128:536  32771.b0c69a6652c0     20000  FWD   DESG
```

Sur le commutateur 3 :

```
{master:0}
admin@commutateur3> show spanning-tree interface

Spanning tree interface parameters for VLAN 2 (1)
                                             (2)
Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID         bridge ID          Cost
ge-0/0/12.0    128:525      128:525  32770.b0c69a6652c0   2000000  BLK    ALT  (4)
ge-0/0/22.0    128:535      128:536  32770.b0c69a6652c0     20000  FWD    ROOT

Spanning tree interface parameters for VLAN 3

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID         bridge ID          Cost
ge-0/0/22.0    128:535      128:536  32771.b0c69a6652c0     20000  FWD    ROOT
```

On trouve l'identifiant du commutateur sur lequel la commande est lancée en (3) en tapant la commande suivante :

```
{master:0}
admin@commutateur3> show spanning-tree bridge vlan-id 2

STP bridge parameters
Context ID                          : 1
Enabled protocol                    : RSTP

STP bridge parameters for VLAN 2
  Root ID                           : 32770.b0:c6:9a:66:52:c0
  Root cost                         : 20000
  Root port                         : ge-0/0/22.0
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Message age                       : 1
  Number of topology changes        : 6
  Time since last topology change   : 1467 seconds
  Topology change initiator         : ge-0/0/22.0
  Topology change last recvd. from  : b0:c6:9a:66:52:d7
  Local parameters
    Bridge ID                       : 32770.b0:c6:9a:67:88:00 (3)
    Extended system ID              : 1
    Internal instance ID            : 0
```

Les commandes optionnelles suivantes à rajouter dans les configurations des interfaces du commutateur sont l'équivalent de l'option « spanning-tree portfast » sur Cisco. Elles permettent la montée plus rapide d'un port sur lequel on branche un PC.

```
{master:0}[edit]
admin@form-o3-cg1# edit protocols vstp vlan all

{master:0}[edit protocols vstp vlan all]
admin@form-o3-cg1# set interface ge-0/0/13 edge
```

Cette commande permet de spécifier au commutateur qu'il est relié directement à un équipement ne faisant pas de Spanning Tree et donc qu'il n'a pas à négocier. Le port monte immédiatement en état « up ». Cette commande peut éviter des problèmes avec certaines configurations DHCP qui n'attendent pas assez longtemps la montée du port.

9. Commandes de diagnostic

Nous allons faire dans cette partie un inventaire des commandes les plus couramment utilisées pour les diagnostics. Ces commandes doivent, pour la plupart, être passées en mode opérationnel.

9.1. Sessions utilisateur

Pour visualiser qui est connecté sur le commutateur, taper **show system users :**

```
{master:0}
admin@form-o3-cg1> show system users
 3:29PM  up 8 days, 23:47, 2 users, load averages: 0.02, 0.03, 0.00
USER     TTY      FROM                              LOGIN@  IDLE WHAT
admin    p0       crc.u-strasbg.fr                 Fri02PM    21 -cli (cli)
```

Pour fermer la session d'un utilisateur, taper **request system logout terminal <numero de ligne>** :

```
{master:0}
admin@form-o3-cg1> request system logout terminal p0
```

9.2. Visualiser les logs

Pour lister les différents fichiers de log disponibles, taper **show log ? :**

```
{master:0}
admin@form-o3-cg1> show log ?
Possible completions:
  <[Enter]>            Execute this command
  <filename>           Name of log file
  authd_sdb.log        Size: 0, Last changed: Mar 31 23:32:30
  chassisd             Size: 93224, Last changed: Jun 03 14:35:48
  cosd                 Size: 1122, Last changed: May 25 15:42:55
  dcd                  Size: 34939, Last changed: Jun 03 14:35:48
  default-log-messages  Size: 0, Last changed: Jun 03 14:35:41
  dfwc                 Size: 0, Last changed: Mar 31 23:32:25
  dfwd                 Size: 104, Last changed: May 25 15:41:13
  eccd                 Size: 0, Last changed: Mar 31 23:32:24
  ext/                 Last changed: Mar 31 23:31:10
  flowc/               Last changed: Mar 31 23:30:58
  ggsn/                Last changed: Mar 31 23:31:10
  gres-tp              Size: 3509, Last changed: May 25 15:42:55
  httpd.log            Size: 322431, Last changed: Jun 03 16:14:29
  httpd.log.old        Size: 28419, Last changed: May 25 15:41:13
  install              Size: 484, Last changed: May 25 16:13:14
  interactive-commands  Size: 129450, Last changed: Jun 03 16:33:31
```

Pour lister les les messages systèmes (fichier de log message), taper **show log message :**

```
{master:0}
admin@form-o3-cg1> show log messages
Jun  3 14:40:23  form-o3-cg1 mgd[10026]: UI_LOAD_EVENT: User 'admin' is performing a 'rollback'
Jun  3 14:40:25  form-o3-cg1 mgd[10026]: UI_COMMIT: User 'admin' requested 'commit' operation (comment: none)
Jun  3 15:13:26  form-o3-cg1 mgd[10026]: UI_DBASE_LOGOUT_EVENT: User 'admin' exiting configuration mode
Jun  3 15:35:32  form-o3-cg1 sshd: sendmsg to 130.79.202.1(130.79.202.1).1812 failed: Can't assign requested address
Jun  3 15:35:32  form-o3-cg1 sshd: rad_send_request: Tried all servers unsucessfully
Jun  3 15:35:32  form-o3-cg1 sshd[11580]: Accepted password for admin from 130.79.203.175 port 54399 ssh2
Jun  3 15:36:15  form-o3-cg1 mgd[11584]: UI_CHILD_EXITED: Child exited: PID 11588, status 1, command '/usr/libexec/ui/logout-
user'
```

Pour lister les dernières connexions des utilisateurs sur l'équipement, taper **show log user :**

```
{master:0}
admin@form-o3-cg1> show log user
admin    ttyp1    130.79.203.175                  Thu Jun  3 15:35   still logged in
admin    ttyp1    130.79.203.175                  Thu Jun  3 11:17 - 15:35  (04:17)
admin    ttyp1    130.79.203.175                  Thu Jun  3 10:09 - 10:35  (00:26)
admin    ttyp2    130.79.203.175                  Wed Jun  2 11:09 - 12:19  (01:09)
admin    ttyp1    130.79.203.175                  Wed Jun  2 09:21 - 12:22  (03:00)
```

9.3. Obtenir des renseignements sur le matériel et la version JUNOS

Pour obtenir la version de JUNOS installée, taper **show version :**

```
{master:0}
admin@form-o3-cg1> show version
fpc0:
--------------------------------------------------------------------------
Hostname: form-o3-cg1
Model: ex4200-24t
JUNOS Base OS boot [10.1S1.3]
JUNOS Base OS Software Suite [10.1S1.3]
JUNOS Kernel Software Suite [10.1S1.3]
JUNOS Crypto Software Suite [10.1S1.3]
JUNOS Online Documentation [10.1S1.3]
JUNOS Enterprise Software Suite [10.1S1.3]
JUNOS Packet Forwarding Engine Enterprise Software Suite [10.1S1.3]
JUNOS Routing Software Suite [10.1S1.3]
JUNOS Web Management [10.1S1.3]
```

Pour remonter les alarmes du châssis, taper **show chassis alarms :**

```
{master:0}
admin@form-o3-cg1> show chassis alarms
1 alarms currently active
Alarm time               Class  Description
2010-05-25 15:42:59 CEST Major  Management Ethernet Link Down
```

Pour montrer le matériel installé dans le châssis, taper **show chassis hardware :**

```
{master:0}
admin@form-o3-cg1> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                BM0209485828      EX4200-24T
Routing Engine 0 REV 18   750-021256   BM0209485828      EX4200-24T, 8 POE
FPC 0            REV 18   750-021256   BM0209485828      EX4200-24T, 8 POE
  CPU                     BUILTIN      BUILTIN           FPC CPU
  PIC 0                   BUILTIN      BUILTIN           24x 10/100/1000 Base-T
Power Supply 0   REV 04   740-020957   AT0509452859      PS 320W AC
Fan Tray                                                 Fan Tray
```

Pour obtenir des informations sur la santé du commutateur (température, ventilateurs), taper **show chassis environment** :

```
{master:0}
admin@form-o3-cg1> show chassis environment
Class Item                          Status     Measurement
Power FPC 0 Power Supply 0          OK
      FPC 0 Power Supply 1          Absent
Temp  FPC 0 CPU                     OK         40 degrees C / 104 degrees F
      FPC 0 EX-PFE1                 OK         46 degrees C / 114 degrees F
      FPC 0 EX-PFE2                 OK         48 degrees C / 118 degrees F
      FPC 0 GEPHY Front Left        OK         29 degrees C / 84 degrees F
      FPC 0 GEPHY Front Right       OK         31 degrees C / 87 degrees F
      FPC 0 Uplink Conn             OK         34 degrees C / 93 degrees F
Fans  FPC 0 Fan 1                   OK         Spinning at normal speed
      FPC 0 Fan 2                   OK         Spinning at normal speed
      FPC 0 Fan 3                   OK         Spinning at normal speed
```

9.4. Obtenir des informations sur les interfaces

Avec les commandes suivantes, on obtient une vision générale des interfaces du commutateur et de leur statut.

Pour lister rapidement des interfaces avec leur statut (activée/désactivée, connectée/déconnectée), taper **show interface terse :**

```
{master:0}
admin@form-o3-cg1> show interfaces terse
Interface               Admin Link Proto    Local                 Remote
ge-0/0/0                up    down
ge-0/0/0.0              up    down eth-switch
ge-0/0/1                up    down
ge-0/0/1.0              up    down eth-switch
ge-0/0/2                up    down
ge-0/0/2.0              up    down eth-switch
ge-0/0/3                up    down
ge-0/0/3.0              up    down eth-switch
ge-0/0/4                up    down
ge-0/0/4.0              up    down eth-switch
ge-0/0/5                up    down
ge-0/0/5.0              up    down eth-switch
```

Pour lister rapidement des interfaces avec leur description (nécessite que le l'attribut **description** soit renseigné pour chaque interface), taper **show interface descriptions :**

```
{master:0}
admin@form-o3-cg1> show interfaces descriptions
Interface       Admin Link Description
ge-0/0/1        up    up reseau labo recherche
ge-0/0/2        up    up reseau labo recherche
ge-0/0/3        up    up reseau labo recherche
ge-0/0/4        up    up reseau labo recherche
ge-0/0/5        up    up reseau enseignement
ge-0/0/6        up    up reseau enseignement
```

Pour obtenir des informations complètes sur une interface, son statut, son adresse MAC, sa vitesse, le débit sur l'interface avec des compteurs d'erreurs, taper **show interface <nom_interface> :**

```
{master:0}
admin@form-o3-cg1> show interfaces ge-0/0/23
Physical interface: ge-0/0/23, Enabled, Physical link is Up
  Interface index: 152, SNMP ifIndex: 156
  Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto, BPDU Error: None,
MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled, Flow control:
Enabled, Auto-negotiation: Enabled, Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x0
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: b0:c6:9a:6e:19:97, Hardware address: b0:c6:9a:6e:19:97
  Last flapped   : 2010-05-25 15:43:10 CEST (1w2d 01:08 ago)
  Input rate     : 1376 bps (2 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None
  Active defects : None

  Logical interface ge-0/0/23.0 (Index 88) (SNMP ifIndex 600)
    Flags: SNMP-Traps 0x0 Encapsulation: ENET2
    Bandwidth: 0
    Input packets : 2186026
    Output packets: 190640
    Protocol eth-switch
      Flags: Trunk-Mode
```

Pour visualiser les erreurs détectées sur une interface, taper **show interfaces extensive <interface> :**

```
{master:0}
admin@form-o3-cg1> show interfaces extensive ge-0/0/12
Physical interface: ge-0/0/12, Enabled, Physical link is Up
  Interface index: 141, SNMP ifIndex: 117, Generation: 144
  Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto,
  BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x0
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: b0:c6:9a:67:88:0c, Hardware address: b0:c6:9a:67:88:0c
  Last flapped   : 2010-03-31 22:24:19 UTC (01:03:11 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :              165515                 512 bps
   Output bytes  :              206124                 512 bps
   Input  packets:                2203                   1 pps
   Output packets:                2478                   1 pps
   IPv6 transit statistics:
    Input  bytes  :                   0
    Output bytes  :                   0
    Input  packets:                   0
---(more)---
```

Pour obtenir la table de commutation du switch avec toutes les adresses MAC connues dans chaque VLAN, taper **show ethernet-switching table :**

```
admin@form-o3-cg1> show ethernet-switching table
Ethernet-switching table: 19 entries, 17 learned
  VLAN              MAC address       Type          Age Interfaces
  vlan_821          *                 Flood           - All-members
  vlan_821          00:00:5e:00:01:34 Learn           0 ge-0/0/23.0
  vlan_821          00:05:85:8a:1b:f1 Learn           0 ge-0/0/23.0
  vlan_821          00:0f:23:43:62:59 Learn           0 ge-0/0/23.0
  vlan_821          00:16:35:10:cf:80 Learn        2:13 ge-0/0/23.0
  vlan_821          00:16:35:11:27:80 Learn        3:47 ge-0/0/23.0
  vlan_821          00:18:fe:33:93:01 Learn           0 ge-0/0/23.0
  vlan_821          00:18:fe:d5:ce:e0 Learn        3:44 ge-0/0/23.0
  vlan_821          00:1b:3f:72:da:00 Learn        2:33 ge-0/0/23.0
  vlan_821          00:1b:3f:80:6b:00 Learn        2:16 ge-0/0/23.0
  vlan_821          00:1c:2e:21:21:00 Learn        2:14 ge-0/0/23.0
  vlan_821          00:1c:2e:28:69:80 Learn        2:04 ge-0/0/23.0
  vlan_821          00:1c:2e:38:1c:80 Learn        2:29 ge-0/0/23.0
  vlan_821          00:1c:2e:38:dc:80 Learn        2:13 ge-0/0/23.0
  vlan_821          00:1c:2e:39:34:80 Learn        2:10 ge-0/0/23.0
  vlan_821          00:1c:2e:39:b0:80 Learn        2:33 ge-0/0/23.0
  vlan_821          2c:6b:f5:3b:51:00 Learn        1:31 ge-0/0/23.0
  vlan_821          2c:6b:f5:96:e1:40 Learn        3:58 ge-0/0/23.0
  vlan_821          b0:c6:9a:6e:19:80 Static          - Router
```

Pour remettre à zéro la table des adresses MAC pour toutes les interface, taper **clear ethernet-switching table :**

```
{master:0}
admin@form-o3-cg1> clear ethernet-switching table
```

9.5. Obtenir des informations sur les VLANs

Pour obtenir des informations sur tous les VLANs avec la liste des interfaces sur lesquelles ils sont actifs, taper **show vlan :**

```
{master:0}
admin@form-o3-cg1> show vlans
Name            Tag     Interfaces
default
                        ge-0/0/0.0, ge-0/0/1.0, ge-0/0/2.0, ge-0/0/3.0, ge-0/0/4.0, ge-
0/0/5.0, ge-0/0/6.0, ge-0/0/7.0, ge-0/0/8.0, ge-0/0/9.0, ge-0/0/10.0, ge-0/0/11.0, ge-
0/0/12.0, ge-0/0/13.0, ge-0/0/14.0, ge-0/0/15.0, ge-0/0/16.0,
                        ge-0/0/17.0, ge-0/0/18.0, ge-0/0/19.0, ge-0/0/20.0, ge-0/0/21.0
vlan_821        821
                        ge-0/0/23.0*
vlan_test       15
                        None
```

9.6. Obtenir des informations sur les agrégations de liens

Pour obtenir des informations sur les ensembles de liens agrégés, taper **show lacp interfaces :**

```
{master:0}
admin@form-o3-cg1> show lacp interfaces
Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-1/0/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      xe-1/0/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-1/0/1                  Current   Fast periodic Collecting distributing

Aggregated interface: ae6
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-5/0/34      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-5/0/34    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-5/0/35      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-5/0/35    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-5/0/34                 Current   Fast periodic Collecting distributing
      ge-5/0/35                 Current   Fast periodic Collecting distributing

Aggregated interface: ae7
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-5/0/46      Actor    No    No   Yes  Yes  Yes   Yes     Slow    Active
      ge-5/0/46    Partner    No    No   Yes  Yes  Yes   Yes     Slow    Active
      ge-5/0/47      Actor    No    No   Yes  Yes  Yes   Yes     Slow    Active
      ge-5/0/47    Partner    No    No   Yes  Yes  Yes   Yes     Slow    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-5/0/46                 Current   Slow periodic Collecting distributing
      ge-5/0/47                 Current   Slow periodic Collecting distributing
```

Pour obtenir des informations sur l'interface virtuelle formée par l'agrégation de plusieurs liens comme les compteurs de débit, d'erreurs, taper **show lacp statistics interfaces** :

```
{master:0}
admin@form-o3-cg1> show lacp statistics interfaces
Aggregated interface: ae1
    LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
      xe-1/0/1             1401638     1400852            0            0

Aggregated interface: ae6
    LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
      ge-5/0/34            1817357     1819281            0            0
      ge-5/0/35            1817368     1819290            0            0

Aggregated interface: ae7
    LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
      ge-5/0/46             109202      101064            0            0
      ge-5/0/47             109239      101065            0            0
```

9.7. Obtenir des informations sur le Spanning Tree

Pour lister l'état des ports relatif au Spanning Tree, taper **show ethernet-switching interfaces :**

```
{master:0}
admin@form-o3-cg1> show ethernet-switching interfaces
Interface    State  VLAN members        Tag   Tagging  Blocking
ge-0/0/0.0   down   default                   untagged unblocked
ge-0/0/1.0   down   default                   untagged unblocked
ge-0/0/2.0   down   default                   untagged unblocked
ge-0/0/3.0   down   default                   untagged unblocked
ge-0/0/4.0   down   default                   untagged unblocked
ge-0/0/5.0   down   default                   untagged unblocked
ge-0/0/6.0   down   default                   untagged unblocked
ge-0/0/7.0   down   default                   untagged unblocked
ge-0/0/8.0   down   default                   untagged unblocked
ge-0/0/9.0   down   default                   untagged unblocked
ge-0/0/10.0  down   default                   untagged unblocked
ge-0/0/11.0  down   default                   untagged unblocked
ge-0/0/12.0  up     vlan_2              2     untagged blocked by STP
ge-0/0/13.0  down   default                   untagged unblocked
ge-0/0/14.0  down   default                   untagged unblocked
ge-0/0/15.0  down   default                   untagged unblocked
ge-0/0/16.0  down   default                   untagged unblocked
ge-0/0/17.0  down   default                   untagged unblocked
ge-0/0/18.0  down   default                   untagged unblocked
ge-0/0/19.0  down   default                   untagged unblocked
ge-0/0/20.0  down   default                   untagged unblocked
ge-0/0/21.0  down   default                   untagged unblocked
ge-0/0/22.0  up     vlan_2              2     tagged   unblocked
                    vlan_3              3     tagged   unblocked
ge-0/0/23.0  down   default                   untagged unblocked
me0.0        down   mgmt                      untagged unblocked
```

Pour afficher des informations détaillées sur l'état du Spanning Tree pour un VLAN particulier, taper **show spanning-tree bridge vlan-id <numero VLAN> :**

```
{master:0}
admin@form-o3-cg1> show spanning-tree bridge vlan-id 2

STP bridge parameters
Context ID                          : 1
Enabled protocol                    : RSTP

STP bridge parameters for VLAN 2
  Root ID                           : 32770.b0:c6:9a:66:52:c0
  Root cost                         : 20000
  Root port                         : ge-0/0/22.0
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Message age                       : 1
  Number of topology changes        : 6
  Time since last topology change   : 4008 seconds
  Topology change initiator         : ge-0/0/22.0
  Topology change last recvd. from  : b0:c6:9a:66:52:d7
  Local parameters
    Bridge ID                       : 32770.b0:c6:9a:67:88:00
    Extended system ID              : 1
    Internal instance ID            : 0
```

Pour obtenir une information rapide sur toutes les instances Spanning Tree d'un commutateur, taper **show spanning-tree bridge brief :**

```
{master:0}
admin@form-o3-cg1> show spanning-tree bridge brief

STP bridge parameters
Context ID                          : 1
Enabled protocol                    : RSTP

STP bridge parameters for VLAN 821
  Root ID                           : 33589.00:0d:28:3d:2d:00
  Root cost                         : 20008
  Root port                         : ge-0/0/23.0
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Message age                       : 3
  Number of topology changes        : 1
  Time since last topology change   : 782628 seconds
  Topology change initiator         : ge-0/0/23.0
  Topology change last recvd. from  : 00:0f:23:43:62:59
  Local parameters
    Bridge ID                       : 33589.b0:c6:9a:6e:19:80
    Extended system ID              : 1
    Internal instance ID            : 0
```

10. Annexes

10.1. Configuration standard recommandée par la DI

```
## Last changed: 2010-06-11 15:46:31 CEST
version 10.1S1.3;
system {
    host-name form-o3-cg1;
    domain-name u-strasbg.fr;
    time-zone Europe/Paris;
    use-imported-time-zones;
    arp {
        aging-timer 5;
    }
    root-authentication {
        encrypted-password "$1XXXXXXXXXXXXXXXXXXX";
    }
    name-server {
        130.79.200.200;
    }
    login {
        user admin {
            uid 2000;
            class superuser;
            authentication {
                encrypted-password "$1XXXXXXXXXXXXXXXXXX";
            }
        }
    }
    services {
        ssh {
            root-login deny;
            connection-limit 10;
            rate-limit 250;
        }
        web-management {
            https {
                local-certificate my-https-certif;
            }
        }
    }
    syslog {
        archive;
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    ntp {
        server 130.79.14.177;
    }
}
```

```
interfaces {
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching;
        }
    }
[...]
    vlan {
        unit 1 {
            family inet {
                address 130.79.X.Y/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 130.79.X.Z;
    }
}
protocols {
    igmp-snooping {
        vlan all;
    }
    vstp {
        vlan all;
    }
    lldp {
        disable;
    }
    lldp-med {
        disable;
    }
}
security {
    certificates {
        local {
            my-https-certif {
                                    "-----BEGIN                 RSA                 PRIVATE
KEY-----\nMIICXAIBAAKBgQCzcZk28P9iMx7AYtK9S5AIht7MRcEpXy58NQLQ5tDrXBCJboAc\nHKaMnPoT1m
+aw0e7m1FyiJjsUCQEualXxDmwltwqUzVe2GTJIW6N6lm0cnIXpUIoCwsSJE\nHYFp98g29VquGQSZu4mgxHH6
aT4XQt3/g9XmV2cBkFk=\n-----END         RSA         PRIVATE         KEY-----\n-----BEGIN
CERTIFICATE-----\nMIID4DCCA0mgAwIBAgIJAJgx0f+9ons7MA0GCSqGSIb3DQEBBQUAMIGnMQswCQYD\nVQ
QGEwJGUjEPMA0GA1UECBMGRnJhbmNlMRMwEQYDVQQHEwpTdHJhc2JvdXJnMSIw\nIAYDVQQKFBlVbml2ZXJzaX
TDqSBMb3VpcyBQYXN/yTS9uHOqjd8091Y4Ya0+jUGu8NcHs5QGy47I7goM6T9rAweq9ILHE\nNKwqDyVMCP1lw
pyS1Qe2NHFcmOkA09hbep7aSGj6P5OO8U8hIvqE13alMAgTGL4E\nB4hajd6sSmsqLlKDnvH85biKa4LqqVN0E
NFnG6NUZFidRmyt\n-----END CERTIFICATE-----\n ";
            }
        }
    }
}
ethernet-switching-options {
    storm-control {
        interface all;
    }
}
vlans {
    default {
        description "vlan natif";
        vlan-id 1;
        l3-interface vlan.1;
    }
}
```

10.2. Procédure de récupération de mot de passe

Voici la procédure de récupération de mot de passe du super utilisateur **root** :

1. Eteindre le commutateur
2. Connecter un PC sur le port console
3. Démarrer une émulation terminale sur le PC (hyperterminal ou minicom) avec les paramètres :
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
4. Redémarrer le commutateur
5. Quand le prompt suivant apparait, appuyer sur la barre d'espace pour accéder au prompt du chargeur d'amorçage :

```
Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel] in 1 second...
```

6. Au prompt suivant, entrer la commande « boot -s » pour démarrer le système en mode « single-user » :

```
loader> boot -s
```

7. Au prompt suivant, entrer la commande « recovery » pour démarrer la procédure de récupération :

```
Enter full path name of shell or 'recovery' for root password recovery or RETURN
for /bin/sh: recovery
```

8. Au prompt suivant, entrer la commande « cli »

```
user@switch> cli
```

9. Modifier le mot de passe root :

```
user@switch# set system root-authentication plain-text-password
```

10. Au prompt suivant, entrer le nouveau mot de passe :

```
New password: <mot de passe>
Retype new password :
```

11. Sauvegarder la configuration :

```
root@switch# commit
commit complete
```

12. Sortir du mode CLI.

```
root@switch# exit
```

13. Sortir du mode opérationnel :

```
root@switch> exit
```

14. Au prompt suivant, entrer « y » pour redémarrer le commutateur :

```
Reboot the system? [y/n] y
```