



ARISTA :

Lignes de commande

Table des matières

1 Le démarrage 3
2 Le mode console CLI 6
2.1 Les commandes générales 6
2.2 Mise à jour de l'IOS EOS 7
2.3 Les interfaces 8
2.4 Les VLANs 8
2.5 Création d'un trunk-group 9
2.6 L'autostate sur les VLANS 10
2.7 Affectation d'une adresse IP à un VLAN pour administration à distance : 11
2.8 Affectation d'un port avec une adresse MAC : 11
2.9 L'agrégation de lien ou le port channel 12
2.10 Le protocole VRRP 14
2.11 Le protocole spanning tree 16
3 Présentation du MLAG 19
3.1 MLAG Applications 19
4 Le protocole SNMP 28
5 Le routage 31
6 Restauration et sauvegarde 35
7 VXLAN signifie Virtual Extensible LAN (réseau local extensible virtuel). 37

1 Le démarrage

La configuration

Trois fichiers définissent les paramètres de configuration de démarrage et d'exécution.

boot-config : contient l'emplacement et le nom de l'image (IOS) à être chargé.
running-config : contient la configuration actuelle du commutateur.
startup-config : contient la configuration du commutateur qui est chargée lorsque le commutateur démarre.

La configuration en cours d'exécution et la configuration de démarrage sont différentes l'une de l'autre lorsque les modifications de configuration n'ont pas été enregistrées depuis le dernier démarrage.

e fichier **boot-config** est un fichier ASCII qu'Aboot utilise pour configurer la console paramètres de communication, localisez l'image du flash EOS et spécifiez paramètres de configuration réseau initiaux.

show boot-config

le running-config est un fichier virtuel qui contient les informations d'exploitation du système configuration, formatée sous la forme d'une séquence de commandes. Les commandes saisies à partir de l'interface de ligne de commande modifient running-config et copient un fichier à running-config met à jour le fichier configuration de l'exploitation en exécutant les commandes dans le fichier copié.

Les commandes permettant d'afficher et de copier running-config sont les suivantes :

show running-config affiche le contenu de running-config.
copy running-config startup-config copie le contenu de running-config dans startup-config.
Write copie le contenu de running-config dans startup-config.

Le fichier startup-config est stocké dans la mémoire flash et contient la configuration que le commutateur charge lors du démarrage. Lors d'un démarrage du commutateur, running-config est remplacé par startup-config. Les modifications apportées à running-config qui ne sont pas copiées dans startup-config sont perdues lorsque le système Redémarre.

Les commandes affectant startup-config sont les suivantes :

show startup-config affiche le contenu de startup-config.
copy file_name startup-config copie le contenu du fichier spécifié à startup-config.
delete startup-config

Le bash

```
Arista-1#bash
Arista Networks EOS shell
[GAD@Arista-1 ~]$ ls
[GAD@Arista-1 ~]$ cd /
[GAD@Arista-1 /]$ cd /usr/
[GAD@Arista-1 usr]$ ls
```

Pour sortir du mode bash

```
[GAD@Arista-1 ~]$ Cli
```

La phase de restauration :

Si le nom d'utilisateur/mot de passe du commutateur est perdu, il existe deux méthodes pour réinitialiser le mot de passe :

- Modifiez la configuration de démarrage :
  - depuis l'invite aboot, allez dans /mnt/flash (en utilisant ***cd***) et éditez la configuration de démarrage (en utilisant VI)
  - Supprimer la ligne de nom d'utilisateur de la configuration
  - enregistrez le fichier et quittez Aboot
  - Connectez-vous avec le nom d'utilisateur par défaut (admin), entrez en mode Activer et définissez un nouveau nom d'utilisateur/mot de passe
- Déplacez/supprimez la configuration de démarrage actuelle :
  - depuis Aboot, allez dans /mnt/flash, puis renommez le fichier startup-config :

- **mv running-config startup-config2**

Il existe deux méthodes permettant de restaurer le commutateur aux paramètres d'usine par défaut à l'aide d'Aboot.

- **fullrecover** - le commutateur peut être restauré à son état d'usine par défaut d'origine en tapant **fullrecover** à partir de l'invite Aboot :

Aboot# **fullrecover**

Toutes les données sur /mnt/flash seront effacées ; tapez « oui » et appuyez sur Entrée pour continuer, ou appuyez simplement sur Entrée pour annuler:

1. Insérez le lecteur dans un ordinateur et formatez-le avec le système de fichiers MS-DOS ou FAT (la plupart des lecteurs USB sont généralement pré-formatés avec un système de fichiers compatible)
2. Créez un fichier texte nommé « fullrecover » (sans extension) sur la clé USB - le fichier peut être vide
3. Créez un fichier texte nommé « boot-config » (sans extension) sur le lecteur USB - le dernier horodatage modifié du fichier boot-config sur le flash USB **doit** différer du fichier boot-config sur le commutateur. Le fichier doit contenir une seule ligne : SWI=flash:EOS.swi.
4. Obtenez une image EOS et copiez-la sur la clé USB, en la renommant EOS.swi

ZTP ou zerotouch

En termes simples, ZTP est utilisé pour configurer un commutateur sans intervention de l'utilisateur. Dans des conditions normales, Arista EOS est responsable du chargement du fichier « startup-config » et du remplissage de son contenu dans la base de données système. Lorsqu'une « configuration de démarrage » n'est pas présente, le commutateur démarre le processus ZTP pour configurer automatiquement le commutateur. ZTP est conçu pour fournir l'intelligence nécessaire pour permettre au commutateur de démarrer avec une perturbation minimale du réseau. L'appareil est en mode Zero Touch Provisioning et tente de télécharger la configuration de démarrage à partir d'un système distant.

Pour désactiver cette fonction taper au démarrage

zerotouch cancel

le commutateur redémarre puis lancer la commande

zerotouch disable

Si ZTP est désactivé et que vous souhaitez le réactiver à nouveau ?

- Une fois Disable, un fichier "zerotouch-config" est créé.

localhost>
localhost> en
localhost# bash
[admin@localhost ~]$ ls /mnt/flash

```
localhost#bash

Arista Networks EOS shell

[admin@localhost ~]$ cd /mnt/flash
[admin@localhost flash]$ ls
AsuFastPktTransmit.log  boot-config       persist
Fossil                  debug             schedule
SsuRestore.log          fastpkttx.backup  vEOS-lab.swi
SsuRestoreLegacy.log    lost+found        zerotouch-config
[admin@localhost flash]$ vi zerotouch-config
DISABLE=True
```

Pour sortir du mode bash Cli

admin@localhost: exit
localhost: wr erase
localhost: reload

2 Le mode console CLI

- **Affectation d'une adresse IP administration à distance via SSH :**

```
localhost#conf t
localhost(config)#int management 1
localhost(config-if-Ma1)#ip add 192.168.0.1 255.255.255.0
localhost(config-if-Ma1)#ip route 0.0.0.0 0.0.0.0 192.168.0.8
localhost(config)#hostname arissw1
arissw1(config)#username admin secret 0 tpreseau11
arissw1(config)#end
arissw1#copy running-config startup-config
arissw1#reload
```

- Après Password
  - SwitchX> **en** ou **enable**
  - SwitchX#

2.1 Les commandes générales

Switch ou router# **wr erase** (pour effacer la configuration puis reload répondre non quand on vous pose la question la question la configuration du system a été modifié)
Switch ou router# **delete startup-config** (pour effacer la configuration)
Switch ou router#**copy running-config startup-config (pour sauvegarder la config)**
Switch ou router# **copy running-config flash:management.txt (pour sauvegarder la config dans un fichier)**
Switch ou router#**write (pour sauvegarder la config)**
Switch ou router# **show license all**
Switch ou router#**show switch**
Switch ou router#**show ver** (pour obtenir la version)
Switch ou router#**show clock**
Switch ou router#**copy running-config usb1:sw30config.txt** (save la config vers clef usb fichier sw30config.txt)
Switch ou router#**copy usb1:sw30config.txt startup-config** (restaurer la config de clef usb fichier sw30config.txt)
Switch ou router# **show boot-config** (pour obtenir des informations sur le boot)
Switch ou router# **reload** (pour redémarrer le commutateur)
Switch ou router# **username** admin **role network-admin priv** 15 **secret** arista

Pour obtenir le shell Arista Networks EOS

Pour rentrer dans le bash

```
arissw1#bash
[admin@arissw1 ~]$ cd /mnt/flash
[admin@arissw1 flash]$ ls
[admin@arissw1 flash]$ cp startup-config startup-config1
[admin@arissw1 flash]$ vi startup-config
[admin@arissw1 flash]$ logout
```

Switch Booting

switch(config)#boot console speed 4800 (pour modifier la vitesse du port console)
switch(config)#boot secret xr19v (pour modifier la password de Aboot)

switch(config)#boot system usb1:EOS1.swi (boot sur le fichier EOS1.swi sur l'interface usb)
switch(config)#boot system flash:EOS.swi boot sur le fichier EOS1.swi sur la flash)
switch(config)#show boot-config (obtenir des infos sur le boot config)

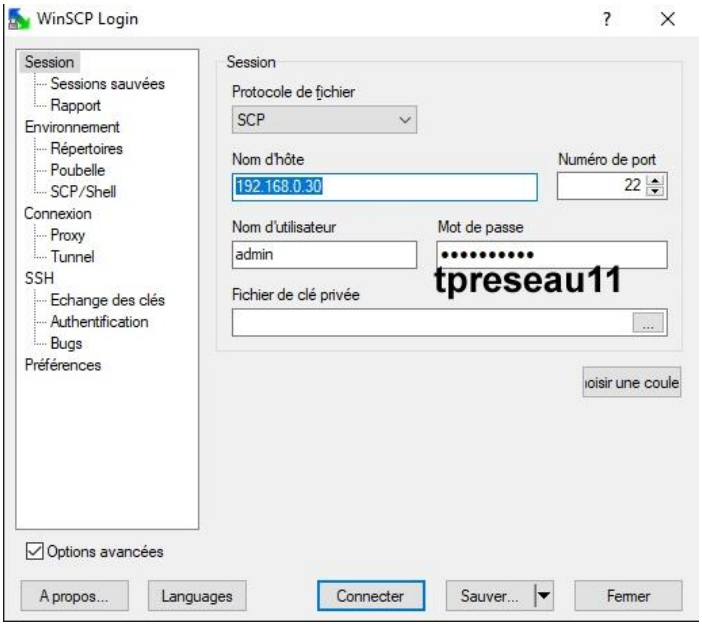
2.2 Mise à jour de l'IOS EOS

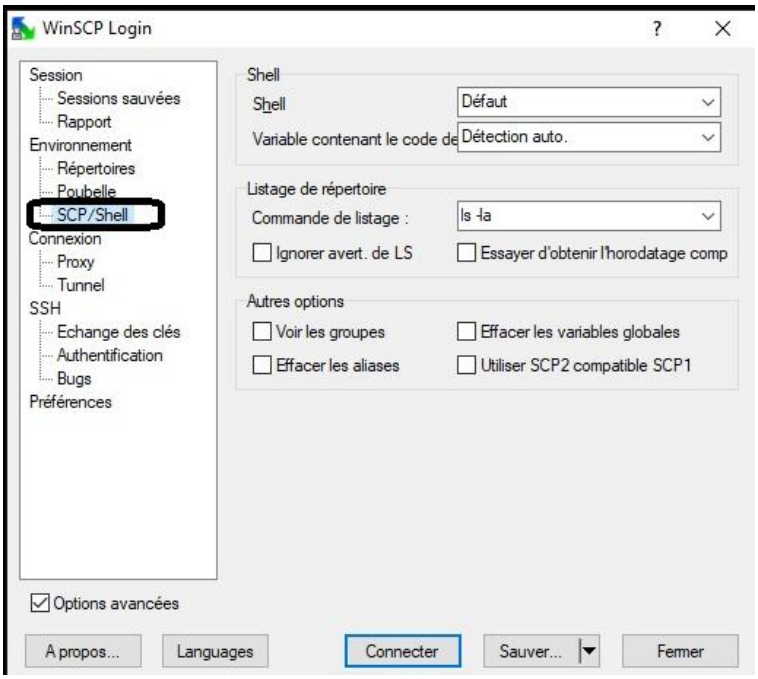
A partir d'un server (mise à jour de IOS):

scp /Users/Downloads/vEOS64-lab-4.24.2F.swi admin@192.168.86.125:/mnt/flash
Switch(config)#**conf t**
Switch(config)#**boot system flash:/vEOS64-lab-4.24.2F.swi**
Switch(config)#**copy running-config startup-config**

A partir de Winscp

Switch(config)#**conf t**
Switch(config)# **username admin shell /bin/bash**





2.3 Les interfaces

- SwitchX#**conf t**
- SwitchX#**show interfaces status** (voir toutes les interfaces)
- SwitchX#**show interfaces ethernet 15**(up down + statistique)
- SwitchX#**show mac address-table**
- SwitchX#**show interfaces ethernet** 15 **status**
- SwitchX(config)#**interface** ethernet *« numéro de l'interface»*
- SwitchX(config-if)#**no shut**
- SwitchX(config-if)#**shut**
- SwitchX(config-if) # **show interfaces ethernet** 4 **transceiver**(info sur le transceiver)
- SwitchX(config-if) # **show interfaces ethernet** 25/1 - 25/4 **status**
- SwitchX(config-if) # **show transceiver status interface ethernet** 15
- SwitchX(config-if) # **show interfaces ethernet 15 transceiver properties** (info Ethernet)

2.4 Les VLANs

- Création de VLAN (Virtual Local Area Network) :
  - SwitchX#**conf t**
  - SwitchX(VLAN)#**vlan** *«numéro du vlan»*
  - SwitchX(VLAN)#**name VLAN1**
  - SwitchX(VLAN)#**state suspend** (pour suspendre)
  - SwitchX(VLAN)#**state active** (pour rendre actif)
  - SwitchX#**sh vlan**
- Suppression un VLAN :
  - SwitchX#**conf t**
  - SWitehX(VLAN)#**no vlan** *«numéro du vlan »*

- Affectation des interfaces aux vlan :
  - SwitchX#**conf t**
  - SwitchX(config)#**interface** ethernet *« numéro de l'interface»*
  - SwitchX(config-if)#**switchport access vlan** *« numéro du vlan >>*
  - SwitchX(config-if)#***switchport mode trunk (pour un Trunk sur port)***
  - SwitchX(config-if)#***switchport trunk allowed vlan 15,20-22,40,75***
  - SwitchX(config)#**show interfaces ethernet 1-5 phy**

Par défaut, tous les VLAN sont autorisés sur un port configuré avec le « trunk en mode switchport ». Pour limiter le port à une liste de VLAN, utilisez la commande switchport trunk allow vlan.

SwitchX(config)#**show interfaces ethernet 1-5 status**

Pour supprimer

- SwitchX#**conf t**
- SwitchX(config)#**interface** ethernet *« numéro de l'interface»*
- SwitchX(config-if)# **no switchport access vlan**
- SwitchX(config-if)# **no switchport mode**
- SwitchX(config-if)# **no switchport trunk allowed vlan**

Création d'un vlan de niveau 3

- SwitchX#**conf t**
- SwitchX(config)#**interface** vlan *« numéro du vlan»*
- SwitchX (config-if-Vl10)#**ip address 192.9.203.2/24**
- SwitchX (config-if-Vl10)#**ip routing**

2.5 Création d'un trunk-group

Le trunking étend plusieurs VLAN au-delà du commutateur via une interface ethernet commune ou un canal de port . **Un trunk group est l'ensemble des interfaces physiques qui comprennent le trunk et la collection de VLAN dont le trafic s'effectue sur le trunk**. Le trafic d'un VLAN qui appartient à un ou plusieurs trunk group est acheminé uniquement sur les ports membres du trunk group auxquels appartient le VLAN, c'est-à-dire les VLAN configurés dans un groupe de lignes sont élagués de tous les ports qui ne sont pas associées aux trunk group.

La commande trunk group attribue le VLAN en mode de configuration à un trunk group spécifié.

switch(config)# **vlan 10**
switch(config-vlan-10)# **trunk group** trunk30
switch(config-vlan-)# no trunk group [name] pour supprimer un vlan d'un trunk group

Le Vlan 10 n'est plus sur les interfaces programmés précédemment c'est-à-dire qu'il a été "élagué" en raison de son appartenance au trunk group dans la configuration du vlan.

• Pour autoriser vlan 10 sur Et1 par la suite, vous devez associer l'interface au trunk group aussi comme suit :

switch(config)# **interface ethernet** 1
switch(config-if-Et1)#**switchport mode trunk**

switch(config-if-Et1)#**switchport trunk allowed vlan** 10 // peut être pas nécessaire
switch(config-if-Et1)#**switchport trunk group** trunk30

pour visualiser le trunk group

switch(config-if-Et1)# **show vlan trunk group**

switch(config-if-Et1)#**switchport trunk group** [***group_name***]
switch(config-if-Et1)# **no switchport trunk group** [***group_name***]

La commande switchport trunk group affecte l'interface du mode de configuration au Trunk group réseau. Les ports de trunk group gèrent le trafic des VLAN attribués au groupe.

Pour associer un trunk group à un canal de port

Création d'un canal de port

```
SW7(config-if-et1-2)# interface port-channel 101
SW7(config-if-po101)# switchport mode trunk
```

Association d'un trunk group à un canal de port

```
SW7(config-if-po101)# switchport trunk group peertrunk
SW7(config-if-po101)# exit
```

2.6 L'autostate sur les VLANS

Lorsque l'autostate est activé, l'interface VLAN sera opérationnelle lorsque :

- le VLAN correspondant existe et est dans l'état actif.
- un ou plusieurs ports de couche 2 dans le VLAN sont actifs et en état de transfert spanning-tree.
- l'interface VLAN existe et n'est pas dans un état d'arrêt.

L'autostate est activé par défaut. Lorsque l'autostate est désactivé, l'interface VLAN est forcée d'être active.

- Pour désactiver l'autostate sur le ***vlan 100***.

switch(config)# **interface vlan 100**
switch(config-if-Vl100)# **no autostate**
switch(config-if-Vl100)#

- Pour activer l'autostate sur le ***vlan 100***.

switch(config)# **interface vlan 100**
switch(config-if-Vl100)# **autostate**
switch(config-if-Vl100)#

2.7 Affectation d'une adresse IP à un VLAN pour administration à distance :

Pour l'administration à distance d'un switch, il faut l'emploi de telnet ou SSH.

- SwitchX#**conf t**
- SwitchX(config)#**int management 1**
- SwitchX(config-if)#**ip add** 192.168.0.1 *255.255.255.0*
- SwitchX(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.0.8
- Hostname ARISW1
- Username admin secret 0 tpreseau11
- End
- Copy running-config startup-config
- SwitchX(config-if)#**no shut**

Pour avoir accès au switch, il faut faire la commande suivante sous DOS :

telnet « *adresse IP du vlan1>>*

2.8 Affectation d'un port avec une adresse MAC :

On peut spécifier une @Mac par port pour le bloquer si une autre adresse Mac est connectée

- SwitchX#**conf t**
- SwitchX(config)#**int ethernet** « *numéro port >>*
- SwitchX(config)#***switchport port-security***
- SwitchX(config-if)# **switchport port-security mac-address maximum <<*nombre>>***
- SwitchX(config)# **#mac address-table static 0034.24c2.8f11 vlan <<numero du vlan>> interface ethernet <<numero interface >>**

mac address-table static 0034.24c2.8f11 vlan 1 interface ethernet 3

SwitchX(config-if)# clear mac address-table dynamic interface ethernet <<numero port>>

SwitchX(config-if)# show port-security

SwitchX(config-if)# show port-security mac-address

Pour désactiver les sécurités :

SwitchX#**conf t**
SwitchX(config)#**int ethernet** « *numéro port >>*
SwitchX(config-if)#**No switchport port-security**

SwitchX(config-if)#**No switchport port-security mac-address** maximum

Port Mirroring

Switch# **conf t**

switch(config)# **monitor session** redirect_1 **source ethernet** 7

switch(config)# **monitor session** redirect_1 **destination ethernet** 8

switch(config)# **show monitor session**

Pour désactiver le port miroring

switch(config)# **no monitor session** *session_name* **source INT_NAME DIRECTION**

redirect_1: nom associé à la redirection ou au port mirroring

2.9 L'agrégation de lien ou le port channel

Table 63: LACP Mode Combinations

Switch 1	Switch 2	Comments
active	active	Links aggregate when LACP negotiation is successful.
active	passive	Links aggregate when LACP negotiation is successful.
passive	passive	Links do not aggregate because LACP negotiation is not initiated.
on (static)	on (static)	Links aggregate without LACP.
on (static)	active or passive	Links aggregate on the static switch without LACP; links do not aggregate on the other switch, and no port-channel connection is established with the partner.

Créer un port channel avec la commande channel-group

La commande channel-group affecte les interfaces Ethernet en mode configuration à un groupe de canaux , crée le groupe de canaux s'il n'existe pas déjà et spécifie les attributs LACP pour le canal. Les groupes de canaux sont associés à une interface de canal de port (port channel) dès leur création. La commande qui crée un nouveau groupe de canaux crée également un canal de port avec un ID correspondant. Le port canal est configuré en mode de configuration port-canal. Modifications de la configuration d'un canal de port
l'interface se propagent à toutes les interfaces Ethernet dans le groupe de canaux correspondant. LACP est activé sur les interfaces membres en définissant le mode de groupe de canaux sur actif ou passif.

Exemple : On assigne aux ports 8 et 9 le canal de port 10 et on valide le LACP en mode négociation

switch(config)**#interface ethernet 8-9**
switch(config-if-Et8-9)**#channel-group 10 mode active**
switch(config-if-Et8-9)**#show active**

switch(config)# **show port-channel**.

L'interface de canal de port 10 est ainsi créé

canal de port avec un ID=10

On peut par la suite créer une interface à un canal de port sans dans un premier temps associé un ou des ports ethernet dessus voir commande ci-dessous **interface port-channel**

Création d'une interface de canal de port sans associer une interface ethernet

Le commutateur propose deux méthodes pour créer des interfaces de canal de port :

• la création d'un groupe de canaux crée simultanément un canal de port associé (**channel-group voir commande précédente) à une interface Ethernet**.
• la commande interface port-channel crée un canal de port sans affecter d'interface Ethernet
canaux vers la nouvelle interface.

switch(config)# **interface port-channel 8**
switch(config-if-Po8)#

switch(config)# **show port-channel**.

Lors de la configuration d'un canal de port, vous n'avez pas besoin d'émettre la commande **interface port-channel** avant d'affecter un port au canal de port (voir la commande channel-group). Le port le numéro de canal est créé implicitement lorsqu'un port est ajouté au canal de port spécifié avec le commande **channel-group number**.

La commande suivante permet de détruire un canal port en spécifiant son numéro. On détruit aussi les ports ethernet associés à ce channel port

switch(config)# **no interface port-channel <<numero>>**

La commande suivante permet de supprimer l'association du port ethernet 8 à son canal de port . On ne détruit pas l'interface associée à ce channel port
arissw1(config)#**interface ethernet 8**
arissw1(config-if-Et8)#**no channel-group**

2.10 Le protocole VRRP

On peut associer sur un VLAN de niveau 3 une passerelle par défaut identique à tous grâce au protocole VRRP. Un routeur virtuel associé sera alors mise en place avec une priorité.

Un numéro de VRRP est ainsi créé.

switch (config)**#vrrp** <<numero de vrrp >> **ip** <<adresse ip passerelle commune >>

switch (config)**#vrrp** <<numero de vrrp >> **priority** <<Valeur de la priorité >>

switch (config)**#vrrp** <<numero de vrrp >> **advertisement interval** <<temps en seconde>>

Le numero de vrrp correspond au numéro de routeur virtuel

Le code suivant configure le premier commutateur (commutateur A) en tant que routeur maître et le deuxième commutateur (commutateur B) comme routeur de secours pour le routeur virtuel 10 sur le VLAN 50. Le commutateur A devient le routeur virtuel maître en définissant sa priorité à 200 ; Le commutateur B conserve la priorité par défaut de 100. L'intervalle d'annonce est de trois secondes sur les deux commutateurs. La préemption de priorité est activée par défaut.

switch-A(config)**#interface vlan 50**
switch-A(config-if-vl50)**#ip address 10.10.4.1/24**
switch-A(config-if-vl50)**#no vrrp 10**
switch-A(config-if-vl50)**#vrrp 10 priority 200**
switch-A(config-if-vl50)**#vrrp 10 advertisement interval 3**
switch-A(config-if-vl50)**#vrrp 10 ip 10.10.4.10**
switch-A(config-if-vl50)**#exit**
switch-A **(config)# ip routing**

switch-B(config)**#interface vlan 50**
switch-B(config-if-vl50)**#ip address 10.10.4.2/24**
switch-B(config-if-vl50)**#no vrrp 10**
switch-B(config-if-vl50)**#vrrp 10 advertisement interval 3**
switch-B(config-if-vl50)**#vrrp 10 ip 10.10.4.10**
switch-B(config-if-vl50)**#exit**
switch-B **(config)# ip routing**

Le code suivant configure deux commutateurs en tant que maître et routeur de secours pour deux routeurs virtuels sur le VLAN 50.

- Le routeur A est le maître du routeur virtuel 10 et la sauvegarde du routeur virtuel 20.
- Le routeur B est le maître du routeur virtuel 20 et la sauvegarde du routeur virtuel 10.
- L'intervalle d'annonce VRRP est de 3 secondes sur le routeur virtuel 10 et de 5 secondes sur le routeur virtuel 20.
- La préemption de priorité est activée par défaut pour les deux routeurs virtuels.

switch-A(config)**#interface vlan 50**
switch-A(config-if-vl50)**#ip address 10.10.4.1/24**
switch-A(config-if-vl50)**#no vrrp 10**
switch-A(config-if-vl50)**#vrrp 10 priority 200**
switch-A(config-if-vl50)**#vrrp 10 advertisement interval 3**
switch-A(config-if-vl50)**#vrrp 10 ip 10.10.4.10**
switch-A(config-if-vl50)**#no vrrp 20**

switch-A(config-if-vl50)**#vrrp 20 advertisement interval 5**
switch-A(config-if-vl50)**#vrrp 20 ip 10.10.4.20**
switch-A(config-if-vl50)**#exit**
switch-A **(config)# ip routing**

switch-B(config)**#interface vlan 50**
switch-B(config-if-vl50)**#ip address 10.10.4.2/24**
switch-B(config-if-vl50)**#no vrrp 10**
switch-B(config-if-vl50)**#vrrp 10 advertisement interval 3**
switch-B(config-if-vl50)**#vrrp 10 ip 10.10.4.10**
switch-B(config-if-vl50)**#no vrrp 20**
switch-B(config-if-vl50)**#vrrp 20 priority 200**
switch-B(config-if-vl50)**#vrrp 20 advertisement interval 5**
switch-B(config-if-vl50)**#vrrp 20 ip 10.10.4.20**
switch-B(config-if-vl50)**#exit**
switch-B **(config)# ip routing**

Pour visualiser les éléments associés au protocole VRRP

Switch **(config)#**show vrrp brief

Pour supprimer le protocole VVRP

Switch **(config)#**no vrrp <<numero de vrrp >>

2.11 Le protocole spanning tree

Plusieurs variants du STP original améliore la performance et la capacité. Arista switche supporte ces versions du STP:

- Rapid Spanning Tree (RSTP)
- Multiple Spanning Tree (MSTP)
- Rapid Per-VLAN Spanning Tree (Rapid-PVST)

switch(config)#**spanning-tree mode mstp**

switch(config)#**spanning-tree mode rstp**

switch(config)#**spanning-tree mode rapid-pvst**

Par défaut en rapid-pvst tous les vlans sont associés au spanning tree

show spanning-tree detail

show spanning-tree interface ethernet 15 detail

show spanning-tree instance

Désactivation :

switch(config)#spanning-tree mode none

Configuration de l'instance Spanning Tree

Un réseau effectue ces étapes pour configurer une instance STP :

1. Le pont avec l'ID le plus bas est élu pont racine.
2. Les ports racine (RP) sont sélectionnés sur tous les autres ponts.
3. Des ponts désignés sont sélectionnés pour chaque segment de réseau.
4. Les ports désignés (DP) sont sélectionnés sur chaque pont désigné.
5. Les réseaux commencent à transmettre des données via les RP et les DP. Tous les autres ports sont bloqués.

Ces commandes s'appliquent à l'instance RST.

switch(config)#**spanning-tree priority** 4096

Ces commandes établissent l'interface Ethernet 7 comme port de secours pour l'interface Ethernet 1.

switch(config)#**interface ethernet 1**

switch(config-if-Et1)#**switchport backup-link ethernet** 7

Cette commande entre en mode de configuration de protection de boucle.

switch(config)#monitor loop-protection

switch(config-monitor-loop-protect)#

Ces commandes activent la protection contre les boucles sur les VLAN 1025-2000.

switch(config)#**monitor loop-protection**

switch(config-monitor-loop-protect)#**no shutdown**

switch(config-monitor-loop-protect)#**protect vlan 1025-2000**

Ces commandes configurent la protection en boucle avec un intervalle de transmission de 10 secondes, un temps de désactivation de deux jours, et un taux maximum de 500 images de détection de boucle par seconde.

switch(config-monitor-loop-protect)#**transmit-interval** 10

switch(config-monitor-loop-protect)#**disabled-time** 172800

switch(config-monitor-loop-protect)#**rate-limit** 500

switch(config-monitor-loop-protect)#

Cette commande affiche un tableau d'informations sur le pont racine.

switch>**show spanning-tree root**

Ces commandes configurent les priorités du pont d'instance MST avec la commande root :

switch(config)#**spanning-tree mst 0 root primary**

switch(config)#**spanning-tree mst 1 root secondary**

Ces commandes prioritaires configurent les priorités du pont Rapid-PVST VLAN :

switch(config**)#spanning-tree vlan-id 1 priority 8192**

switch(config)#**spanning-tree vlan-id 2 priority 16384**

switch(config)#**spanning-tree vlan-id 3 priority 8192**

switch(config)#**no spanning-tree vlan-id 4 priority**

switch(config)#show spanning-tree root

Cette commande définit la priorité du port d'accès de 144 pour l'interface Ethernet 5.

switch(config)#**interface ethernet 5**

switch(config-if-Et5)#**spanning-tree port-priority 144**

Cette commande active inconditionnellement Portfast sur l'interface Ethernet 5.

switch(config)#**interface ethernet 5**

switch(config-if-Et5)#**spanning-tree portfast**

Cette commande active la détection automatique des bords sur l'interface Ethernet 5.

switch(config)#**interface ethernet 5**

switch(config-if-Et5)#**spanning-tree portfast auto**

Cette commande configure l'interface Ethernet 5 en tant que port partagé.

switch(config)#interface ethernet 5

switch(config-if-Et5)#**spanning-tree link-type shared**

Cette commande active la protection racine sur l'interface Ethernet 5.

switch(config)#**interface ethernet 5**

switch(config-if-Et5)#**spanning-tree guard root**

Cette commande active la protection contre les boucles par défaut sur tous les ports du commutateur.

switch(config)#**spanning-tree guard loop default**

switch(config)#

• Cette commande active la protection contre les boucles sur l'interface Ethernet 6.

switch(config)#**interface ethernet 6**

switch(config-if-Et6)#**spanning-tree guard loop**

Ces commandes activent l'assurance du pont sur le commutateur, puis activent l'assurance du pont sur le port Ethernet 5 en en le désignant comme un port réseau.

switch(config)#**spanning-tree transmit active**

switch(config)#**interface ethernet 5**

switch(config-if-Et5)#**spanning-tree portfast network**

Cette commande configure un temps de salutation de 1 seconde (1000 ms).

switch(config)#**spanning-tree hello-time 1000**

Cette commande configure un nombre de mises en attente de transmission de 8 BPDU.

switch(config)#**spanning-tree bpdu tx hold-count 8**

spanning-tree bpduguard active la protection BPDU sur l'interface du mode de configuration.

Spanning-Tree bpduguard Disable désactive la protection BPDU sur l'interface du mode de configuration.

aucun bpduguard spanning-tree ne rétablit l'interface du mode de configuration au paramètre de garde BPDU par défaut.

• Ces commandes activent la protection BPDU par défaut sur tous les ports portfast, puis désactivent la protection BPDU sur Ethernet 5.

switch(config)#**spanning-tree edge-port bpduguard default**

switch(config)#**interface ethernet 5**

switch(config-if-Et5)#**spanning-tree bpduguard disable**

Ces commandes activent le filtrage BPDU sur Ethernet 5.

switch(config)#interface ethernet 5

switch(config-if-Et5)#**spanning-tree bpdufilter enable**

Cette commande configure la limite globale de 5 000 BPDU sur un intervalle de quatre secondes.

switch(config)#**spanning-tree bpduguard rate-limit count 5000 interval 4**

Cette commande active la limitation du débit sur les ports qui ne sont pas couverts par les commandes de limite de débit d'interface.

switch(config)#**spanning-tree bpduguard rate-limit default**

switch(config)#

• Ces commandes permettent une limitation de débit sur l'interface Ethernet 15.

switch(config)#**interface ethernet 15**

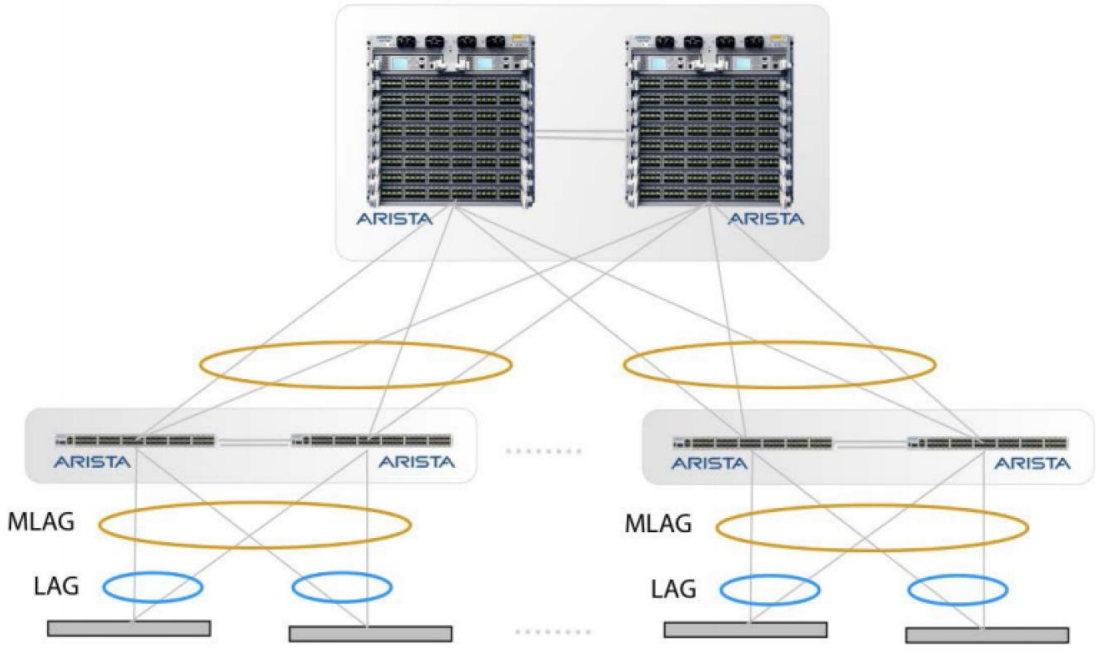
switch(config-if-Et15)#**spanning-tree bpduguard rate-limit enable**

3 Présentation du MLAG

Les topologies de centre de données à haute disponibilité offrent généralement une protection de redondance au détriment de la sursouscription en connectant des commutateurs et des serveurs top-of-rack (TOR) à des commutateurs à double agrégation. Dans ces topologies, le protocole Spanning Tree évite les boucles réseau en bloquant la moitié des liens vers les commutateurs d'agrégation. Cela réduit la bande passante disponible de 50 % Le déploiement du MLAG supprime la sursouscription en configurant un lien MLAG entre deux commutateurs agrégateurs pour créer une seule instance de commutation logique qui utilise toutes les connexions aux commutateurs. Les interfaces des deux appareils participent à un canal de port distribué, permettant à tous les chemins actifs de transporter trafic de données tout en maintenant l'intégrité de la topologie Spanning Tree.

MLAG offre ces avantages :

• Regroupe plusieurs ports Ethernet sur deux commutateurs agrégateurs.
• Fournit des liaisons à bande passante plus élevée à mesure que le trafic réseau augmente.
• Utilise la bande passante plus efficacement avec moins de liens bloqués par STP.
• Se connecte à d'autres commutateurs et serveurs par LAG statique ou LACP sans autres protocoles propriétaires.
• Prend en charge le fonctionnement STP normal pour éviter les boucles.
• Prend en charge la redondance couche 2 active-active.
Processus de fonctionnement du MLAG

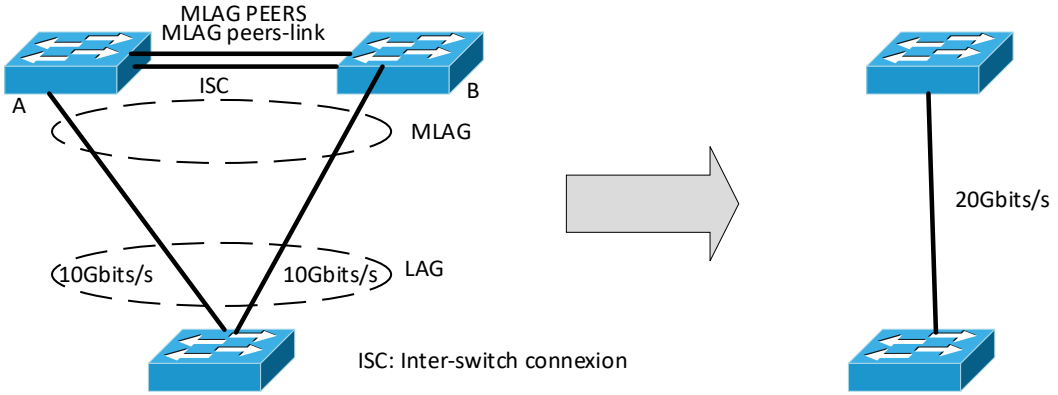


3.1 MLAG Applications

MLAG peut être utilisé à différents endroits du réseau pour éliminer les goulots d'étranglement et assurer la résilience.
Couche de feuilles (LEAF)
À la fin du réseau, les serveurs dotés de plusieurs interfaces se connectent aux commutateurs à l'aide de la liaison NIC ou de l'agrégation de liens standard. Avec deux de vos commutateurs leaf dans une paire MLAG, vous pouvez désormais avoir des connexions redondantes actives/actives entre le serveur et les commutateurs. Les groupes LAG peuvent être formés à l'aide de méthodes d'agrégation de liens statiques ou de négociation basées sur la LACP.
Couche de colonne vertébrale (SPINE)
Au niveau de la couche SPINE, deux commutateurs de la famille Arista 7000 peuvent former une paire MLAG et agréger toutes les liaisons montantes des racks du centre de données. Cela élimine les ports bloqués de Spanning Tree et vous permet d'utiliser la bande passante d'interconnexion sur tous les ports. MLAG au niveau de la couche vertébrale contribue grandement à améliorer l'évolutivité de la couche 2 de votre réseau, sans augmenter votre coût.

Un groupe d'agrégation de liens multi-châssis (MLAG) est une paire de liens qui se terminent sur deux commutateurs distinctes et apparaissent comme un groupe d'agrégation de liens (LAG) ordinaire. Les commutateurs coopérants sont Les commutateurs **voisins (peer)** MLAG et communiquent via une interface appelée lien homologue (**peers link**). Alors que le lien de pair est le but principal est d'échanger des informations de contrôle MLAG entre les commutateurs voisins, il transporte également des données de trafic provenant d'appareils connectés à un seul homologue MLAG et n'ayant pas d'autre chemin. Un MLAG Le domaine se compose des commutateurs voisins et des liaisons de contrôle qui connectent les commutateurs.

Dans la figure ci-dessous, le commutateur A et le commutateur B sont des commutateurs pairs dans le domaine MLAG et se connectent l'un à l'autre. l'autre via le lien de pairs. Chaque commutateur voisin utilise l'adresse homologue pour former et maintenir la liaison homologue. **L'ID de domaine** MLAG est une chaîne de texte configurée dans chaque commutateur voisin. Les commutateurs MLAG utilisent cette chaîne pour identifier ses pairs. **L'ID système MLAG (MSI)** est l'adresse MAC du domaine MLAG. Le MSI est automatiquement dérivé lorsque le MLAG se forme et ne correspond pas à l'adresse MAC de pont de l'un ou l'autre pair. Chaque pair utilise le MSI dans les PDU STP et LACP. La topologie illustrée ci-dessous contient quatre MLAG : un MLAG connecte chaque appareil au MLAG domaine. Chaque commutateur homologue se connecte aux quatre serveurs via des interfaces de liaison MLAG.



Dans une topologie conventionnelle, avec des dispositifs à double connexion à plusieurs commutateurs pour la redondance, Le protocole Spanning Tree (STP) bloque la moitié des liaisons commutateur-appareil. Dans la topologie MLAG, STP fait ne bloque aucune partie car il considère **le domaine MLAG comme un commutateur unique et chaque MLAG comme un port unique (voir schéma précédent)**. Le protocole MLAG facilite l'équilibrage du trafic des périphériques entre les commutateurs homologues.

Configuration des pairs MLAG

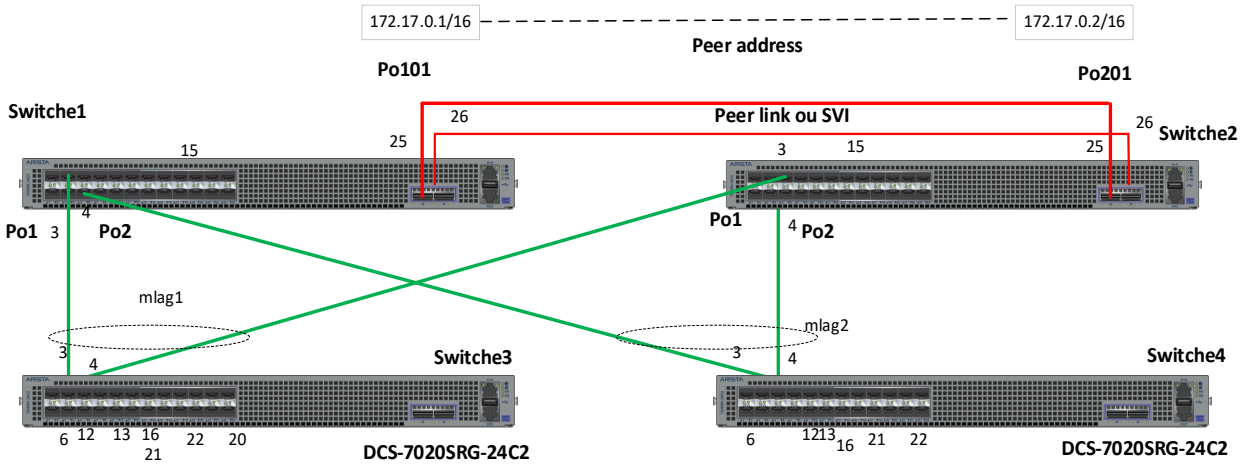
Par exemple, deux ports Ethernet 10 gigabits, un de chacun des deux commutateurs configurés MLAG, peut se connecter à deux ports 10 gigabits sur un hôte, un commutateur ou un périphérique réseau pour créer un lien qui apparaît comme un seul port 20 gigabits.
Les ports configurés MLAG fournissent un multipathing de couche 2, une bande passante accrue , une plus grande disponibilité et d'autres améliorations sur les systèmes traditionnels actifs-passifs ou régis par Spanning Tree infrastructures.

MLAG est une donc amélioration de LAG où les ports de différents châssis de commutateur sont regroupés pour agir comme un lien logique unique. Cela fournit également des liaisons montantes actives/actives sans boucles de couche 2.
Le commutateur MLAG est très similaire à la fonctionnalité VPC de Cisco Nexus, mais MLAG n'est pas propriétaire.

Terminologies MLAG :

- **Domaine MLAG** – Une paire de commutateurs physiques
- **Homologue MLAG (MLAG PEERS)** – Un seul commutateur au sein d'un domaine MLAG
- **MLAG peer-link** – Liaison physique Ethernet entre les homologues MLAG requise pour synchroniser l'état entre les homologues MLAG et transporter les données utilisateur
- **Port membre MLAG** – Un ou plusieurs ports physiques orientés utilisateur qui forment un MLAG
- **Canal de port MLAG** – Il s'agit d'un canal de port combiné orienté utilisateur entre les homologues MLAG composé de ports membres MLAG sur les deux homologues MLAG
- **MLAG VLAN** – Un VLAN utilisé exclusivement sur la liaison homologue MLAG, afin de faciliter la communication du plan de contrôle entre les pairs MLAG.

• Ces commandes créent une interface de canal de port LACP en mode actif à partir de deux interfaces Ethernet et configurez celle-ci dans le cadre d'un trunk group sur chaque commutateur. **La commande switchport mode trunk** autorise tous les VLAN sur l'interface par défaut, donc tous Les VLAN sont autorisés sur le canal de port 101 dans l'exemple suivant. La configuration d'un trunk group pour un VLAN limite uniquement ce VLAN spécifique aux ports associés : le VLAN 4094 est uniquement autorisé sur le canal de port 101 et non sur les autres ports du commutateur. Il est important de se rappeler que tous les VLAN doivent être autorisés entre les homologues sur la liaison homologue pour un fonctionnement correct.
Soit la configuration suivante :



Switch 1
switch1#**config**
switch1(config)#**vlan 4094**
switch1(config-vlan-4094)#**trunk group m1peer**
switch1#**config**
switch1(config)#**interface ethernet 25-26**
switch1(config-if-et25-26)#**channel-group 101 mode activ**e
switch1(config-if- et25-26)#**interface port-channel 1**01
switch1(config-if-po101)#**switchport mode trunk**
switch1(config-if-po101)#**switchport trunk group m1peer**
switch1(config-if-po101)#**exit**
switch1(config)#

Switch 2

switch2#**config**
switch2(config)#**vlan 4094**
switch2(config-vlan-4094)#**trunk group m1peer**
switch2(config-vlan-4094)#**exit**
switch2(config)#**interface ethernet 25-26**
switch2(config-if-et1-2)#**channel-group 201 mode active**
switch2(config)#**interface port-channel 201**
switch2(config-if-po101)#**switchport mode trunk**
switch2(config-if-po101)#**switchport trunk group m1peer**
switch2(config-if-po101)#**exit**
switch2(config)#

Autres possibilités créer en amont un port channel sans affectation d'interface ethernet (swicth1 et switch2)

switch1(config)# interface port-channel 101
switch1(config-if-po101)# switchport mode trunk
switch1(config-if-po101)#switchport trunk group **m1peer**
switch1(config-if-po101)#exit
switch1#**config**
switch1(config)#**vlan 4094**
switch1(config-vlan-4094)#**trunk group m1peer**
switch1#**config**
switch1(config)#**interface ethernet 25-26**
switch1(config-if-et25-26)#**channel-group 101 mode activ**e
switch1(config-if-po10)#**exit**
switch1(config)#

switch2(config)# interface port-channel 201
switch2(config-if-po201)# switchport mode trunk
switch2(config-if-po201)#switchport trunk group **m1peer**
switch2(config-if-po201)#exit
switch2#**config**
switch2(config)#**vlan 4094**
switch2(config-vlan-4094)#**trunk group m1peer**
switch2#**config**
switch2(config)#**interface ethernet 25-26**
switch2(config-if-et25-26)#**channel-group 201 mode activ**e
switch2(config-if-po201)#**exit**
switch2(config)#

Ces commandes précédentes créent un SVI (switch virtual interface) pour l'interface locale et l'associent au trunk group affecté au canal du port de liaison homologue. Le SVI crée un point de terminaison de couche 3 dans le commutateur et permet aux processus MLAG de communiquer par TCP. L'adresse IP peut être n'importe quelle adresse de monodiffusion qui n'entre pas en conflit avec d'autres SVI.

STP est désactivé pour la liaison homologue VLAN 4094 afin d'éviter toute perturbation STP potentielle de l'inter pair communications. Rappelez-vous que le VLAN a été limité au canal de port 101 dans la configuration de groupe empêchant ainsi les conditions potentielles de boucle de couche 2 dans le VLAN 4094.

Switch 1

switch1#**config**
switch1(config)#**interface vlan 4094**

switch1(config-if-vl4094)**#ip address 172.0.0.1/30**
switch1(config-if-vl4094)**#no autostate**
switch1(config-if-vl4094)**#exit**
switch1(config)**#no spanning-tree vlan-id 4094**
switch1(config)#
Switch 2
switch2**#config**
switch2(config)**#interface vlan 4094**
switch2(config-if-vl4094)**#ip address 172.0.0.2/30**
switch2(config-if-vl4094)**#no autostate**
switch2(config-if-vl4094)**#exit**
switch2(config)**#no spanning-tree vlan-id 4094**
switch2(config)#

Les paramètres de connexion homologue configurent la connexion entre les commutateurs homologues MLAG. Cette section décrit les paramètres de configuration d'homologue suivants.

• Mode de configuration MLAG
• Interface VLAN locale
• Adresse homologue
• Lien entre pairs
• ID de domaine
• Intervalle de pulsation et délai d'expiration
• Délai de rechargement
• shutdown

Se positionner en mode de configuration mlag

```
switch(config)# mlag configuration
```

Spécifier une interface de VLAN locale

Interface VLAN locale

L'interface locale spécifie le SVI sur lequel le commutateur **envoie le trafic de contrôle MLAG**. L'IP locale L'adresse est spécifiée dans la définition du VLAN associé à l'interface locale. Le pair L'adresse configure la destination du trafic de contrôle sur le commutateur homologue. La commande local-interface spécifie une interface VLAN en tant que SVI de liaison homologue.

```
switch(config-mlag)#local-interface vlan 4094
switch(config-mlag)#
```

L’adresse du voisin

L'adresse homologue ou voisin est l'adresse de destination sur le commutateur homologue pour le trafic de contrôle MLAG. Si l'adresse IP du pair l'adresse est inaccessible, l'appairage MLAG échoue et les deux commutateurs homologues reviennent à leur état indépendant.

```
switch(config-mlag)# peer-address 172.0.0.1
```

L’interface de port channel pour le contrôle MLAG

Un MLAG est formé en connectant deux commutateurs via une interface appelée lien homologue. Le pair lien transporte des messages MLAG, des messages keepalive et le trafic de données entre les commutateurs. Ces informations permettent aux deux commutateurs de fonctionner ensemble comme un seul. Tandis que les interfaces comprenant les liens homologues sur chaque commutateur doivent être compatibles, ils n'ont pas besoin d'utiliser le même numéro d'interface. Ethernet et canal de port les interfaces peuvent être configurées en tant que liens homologues.
La commande peer-link spécifie l'interface que le commutateur utilise pour communiquer le contrôle MLAG circulation.

```
switch(config-mlag)# peer-link port-channel 101
```

Le domaine ID

L'ID de domaine MLAG est un identifiant unique pour un domaine MLAG. L'ID de domaine MLAG doit être identique sur chaque switch pour faciliter la communication MLAG.
La commande domain-id configure l'ID de domaine MLAG.

switch(config-mlag)# **domain-id mlagDomain**

Configuration du message de heartbeat

L'intervalle de pulsation spécifie la période entre la transmission de messages keepalive successifs messages. Chaque commutateur MLAG transmet des messages keepalive et surveille la réception des messages de son pair. Le délai de pulsation est réinitialisé lorsque le commutateur reçoit un message keepalive. Si le battement de cœur expire, le commutateur désactive MLAG en partant du principe que le commutateur homologue ne fonctionne pas.
This command configures the heartbeat interval as ***2500*** milliseconds (2.5 seconds).

```
switch(config-mlag)# heartbeat-interval 2500
```

La période de rechargement

La période de délai de rechargement spécifie l'intervalle pendant lequel les liens non homologues sont désactivés après qu'un homologue MLAG redémarre. Cet intervalle permet aux liaisons non homologues d'apprendre les états de multidiffusion et OSPF et de synchroniser l'ARP caches avant que les ports ne commencent à gérer le trafic. Chaque commutateur Arista utilise par défaut le délai de rechargement recommandé valeur, qui varie selon la plate-forme du commutateur.
Cette commande configures l'intervalle de période de rechargement à ***2.5*** minutes (***150*** seconds).

switch(config-mlag)# **reload-delay 150**

La commande shutdown (MLAG) désactive les opérations MLAG sans perturber le MLAG configuration. La commande de configuration no mlag (mode de configuration globale) désactive MLAG et supprime la configuration MLAG. La commande no shutdown reprend l'activité MLAG.

La commande shutdown

La commande shutdown (MLAG) désactive les opérations MLAG sans perturber le MLAG configuration. La commande de configuration no mlag (mode de configuration globale) désactive MLAG et supprime la configuration MLAG. La commande no shutdown reprend l'activité MLAG.
Exemples
• Cette commande désactive l'activité MLAG sur le commutateur.
switch(config-mlag)# shutdown
• Cette commande reprend l'activité MLAG sur le commutateur.
switch(config-mlag)# no shutdown

Les commandes suivantes créent un lien entre voisin switch1

```
switch1(config)# mlag configuration
switch1(config-mlag)# local-interface vlan 4094
switch1(config-mlag)# peer-address 172.17.0.1
switch1(config-mlag)# peer-link port-channel 101
switch1(config-mlag)# domain-id mlag_01
switch1(config-mlag)# heartbeat-interval 2500
switch1(config-mlag)# reload-delay 150
switch1(config-mlag)# exit
```

```
Les commandes suivantes créent un lien entre voisin  switch2
switch2(config)# mlag configuration
switch2(config-mlag)# local-interface vlan 4094
switch2(config-mlag)# peer-address 172.17.0.2
switch2(config-mlag)# peer-link port-channel 201
switch2(config-mlag)# domain-id mlag_01
switch2(config-mlag)# heartbeat-interval 2500
switch2(config-mlag)# reload-delay 150
switch2(config-mlag)# exit
switch2(config)#
```

Configuration de la passerelle homologue MLAG

Dans une configuration MLAG, le routage sur un commutateur homologue MLAG est possible en utilisant son propre système de pont MAC, VARP MAC ou VRRP MAC. Sur un pair recevant un paquet IP avec l'adresse MAC de destination définie sur l'un de ces MAC, un paquet est acheminé si son matériel dispose de suffisamment d'informations pour acheminer le paquet. Configuration l'envoi de trafic vers un MAC mis en cache implique le routage de la table de session et du trafic homologue MLAG si les paquets sont reçu avec le pair MAC.

Exemples

• Cette commande active la passerelle homologue MLAG.

switch(config)# **ip virtual-router mac-address mlg-peer**
switch1(config)#
• Cette commande désactive la passerelle homologue MLAG.
switch(config)# **no ip virtual-router mac-address mlg-peer**

Configuration des services MLAG

Un MLAG est une paire de liens qui proviennent d'un périphérique connecté au réseau et se terminent sur les deux MLAG commutateurs homologues. Les commutateurs MLAG coordonnent le trafic vers l'appareil via un mlag commun (portchannel configuration de l'interface) sur les interfaces qui se connectent au périphérique.
L'ID MLAG diffère de l'ID de domaine MLAG. L'ID de domaine MLAG est attribué globalement par commutateur en mode de configuration MLAG, et le même ID de domaine MLAG doit se trouver sur les deux commutateurs. Il n'est pas recommandé d'utiliser des MLAG avec des LAG statiques. Configurez le commutateur en aval ou routeur connecté aux pairs MLAG pour négocier un LAG avec LACP. Pour les commutateurs Arista Networks, cela concerne une configuration telle que le mode numéro de groupe de groupes de canaux activé.
Configuration des interfaces
Les canaux de port configurés en tant que MLAG doivent avoir des numéros de canal de port identiques. Bien que le MLAG L'ID est un paramètre distinct du numéro de canal de port, les meilleures pratiques recommandent d'attribuer le ID MLAG correspondant au numéro de canal du port.
Un MLAG est une paire de liens qui proviennent d'un périphérique connecté au réseau et se terminent sur les deux MLAG commutateurs homologues. Les commutateurs MLAG coordonnent le trafic vers l'appareil via un mlag commun (portchannel configuration de l'interface) sur les interfaces qui se connectent au périphérique. L'ID MLAG diffère de l'ID de domaine MLAG. L'ID de domaine MLAG est attribué globalement par commutateur en mode de configuration MLAG, et le même ID de domaine MLAG doit se trouver sur les deux commutateurs. Il n'est pas recommandé d'utiliser des MLAG avec des LAG statiques. Configurez le commutateur en aval ou routeur connecté aux pairs MLAG pour négocier un LAG avec LACP. Pour les commutateurs Arista Networks, cela concerne une configuration telle que le mode numéro de groupe de groupes de canaux activé. 1178

Configuration des interfaces

Les canaux de port configurés en tant que MLAG doivent avoir des numéros de canal de port identiques. Bien que le MLAG L'ID est un paramètre distinct du numéro de canal de port, les meilleures pratiques recommandent d'attribuer le ID MLAG correspondant au numéro de canal du port.

.

```
switch1(config)#interface ethernet 3
switch1(config-if-et3)#channel-group 1 mode active
switch1(config-if-et3)#interface port-channel 1
switch1(config-if-et3)#switchport mode trunk
switch1(config-if-po1)#mlag 1
switch1(config-if-po1)#exit
switch1(config)#

switch1(config)#interface ethernet 4
switch1(config-if-et4)#channel-group 2 mode active
switch1(config-if-et4)#interface port-channel 2
switch1(config-if-po2)#mlag 2
switch1(config-if-po2)#exit
switch1(config)#


switch2(config)#interface ethernet 3
switch2(config-if-et3)#channel-group 2 mode active
switch2(config-if-et3)#interface port-channel 2
switch2(config-if-et3)#switchport mode trunk
switch2(config-if-po1)#mlag 1
switch2(config-if-po1)#exit
switch2(config)#

switch2(config)#interface ethernet 4
switch2(config-if-et4)#channel-group 1 mode active
switch2(config-if-et4)#interface port-channel 1
switch2(config-if-po2)#mlag 2
switch2(config-if-po2)#exit
switch2(config)#
```

LAG statiques

En mode statique (avec le mode groupe de canaux configuré comme activé sur les interfaces membres), le commutateur regroupe les liaisons sans connaissance des LAG sur le commutateur partenaire et sans négociation LACP. Les ports membres n'envoient pas de paquets LACP et ne traitent pas les paquets LACP entrants sur des LAG statiques. Les paquets peuvent chuter lorsque les configurations LAG statiques diffèrent entre les commutateurs.

LAG dynamiques

Les LAG dynamiques connaissent l'état du canal de port de leurs partenaires. Interfaces configurées comme dynamiques Les LAG sont désignés comme actifs ou passifs.

• Les interfaces actives envoient des unités de données de protocole LACP (PDU LACP) à raison d'une par seconde lorsqu'elles forment un canal avec une interface sur le commutateur homologue. Un agrégat se forme si le pair exécute LACP dans mode actif ou passif.

• Les interfaces passives envoient uniquement des PDU LACP en réponse aux PDU reçues du partenaire. Le commutateur partenaire doit être en mode actif et initie la négociation en envoyant un paquet LACP. le commutateur de mode passif reçoit et répond au paquet pour former un LAG.

Une interface active peut former des canaux de port avec des interfaces partenaires passives ou actives, mais les canaux de port ne sont pas formés lorsque l'interface de chaque commutateur est passive.

Enabling IPv4 Routing

Lorsque le routage IPv4 est activé, le commutateur tente de livrer les paquets entrants à la destination IPv4 adresses en les transmettant aux interfaces ou aux adresses de saut suivant spécifiées par la table de routage. La commande ip routing active le routage IPv4.

Example
This command enables IP routing:
switch(config)#**ip routing**
switch(config)#

Dans une configuration MLAG, le routage sur un commutateur homologue MLAG est possible en utilisant son propre système de pont MAC, VARP MAC ou VRRP MAC. Sur un pair recevant un paquet IP avec l'adresse MAC de destination définie sur l'un de ces MAC, un paquet est acheminé si son matériel dispose de suffisamment d'informations pour acheminer le paquet. Configuration l'envoi de trafic vers un MAC mis en cache implique le routage de la table de session et du trafic homologue MLAG si les paquets sont reçu avec le pair MAC.

switch(config)#**ip virtual-router mac-address mlag-peer**

La commande ip virtual-router address attribue une adresse IP virtuelle à l'interface VLAN en cours de configuration. Contrairement à VRRP, l'adresse IP virtuelle n'a pas besoin d'être dans le même sous-réseau que le interface physique. Une adresse IPv4 virtuelle peut éventuellement être configurée avec un sous-réseau, mais cela modifiera le comportement des requêtes ARP envoyées par le routeur. Lorsque le routeur envoie une requête ARP pour un IPv4 dans un sous-réseau virtuel, la requête ARP utilisera l'adresse IPv4 virtuelle comme adresse IP source

switch(config)#**interface vlan 10**
switch(config-if-Vl10)#**ip address** 10.0.0.2/24
switch(config-if-Vl10)#**ip virtual-router address** 10.0.0.6

La commande ip virtual-router mac-address attribue une adresse MAC virtuelle au commutateur.
Le commutateur mappe toutes les adresses IP du routeur virtuel à cette adresse MAC. L'adresse est en réception uniquement Le commutateur n'envoie jamais de paquets avec cette adresse comme source. Lorsque le MAC de destination d'un paquet destiné à un réseau distant correspond à l'adresse MAC virtuelle l'homologue MLAG transfère le trafic vers la destination du saut suivant. Chaque pair MLAG doit avoir la même route disponible, soit via une configuration statique, soit via un protocole de routage dynamique.

This command configures a virtual MAC address.
switch(config)#**ip virtual-router mac-address 001c.7300.0099**
switch(config)#

4 Le protocole SNMP

La commande show snmp engineID affiche les informations du moteur SNMP local configurées sur le

switch.

switch(config)#**show snmp engineID**

La commande locale snmp-server engineID configure le nom du Moteur de protocole de gestion (SNMP). L'engineID SNMP par défaut est généré par le commutateur et est utilisé lorsqu'un engineID n'est pas configuré avec cette commande.

switch(config)#**snmp-server engineID local** DC945798CAB4

la commande snmp-server local-interface spécifie l'interface d'où provient les informations SNMP et les TRAPS
Les commandes interface locale no snmp-server et l'interface locale du serveur snmp par défaut suppriment l'affectation de la source inform ou trap en supprimant l'interface locale snmp-server commande du fichier running-config.

cette command configures ***interface ethernet 1*** comme la source des traps SNMP et des informations.

switch(config)#**snmp-server local-interface ethernet 1**

switch(config)#**snmp-server local-interface Management1**

La commande snmp-server view définit une vue.

Une vue SNMP définit un sous-ensemble d'objets d'une MIB. Chaque groupe d'accès SNMP spécifie des vues, chacun associé à des droits d'accès en lecture ou en écriture, pour autoriser ou limiter l'accès du groupe aux objets MIB. La commande no snmp-server view supprime une entrée de vue en supprimant la commande snmpserver view dans le fichier running-config.

snmp-server view *view_name family_name* **INCLUSION**

Paramètres :

• nom_vue Libellé de l'enregistrement de vue que la commande met à jour. D'autres commandes font référence à voir avec cette étiquette.
• nom_famille nom de l'objet ou de la famille MIB.

Les objets MIB et les sous-arborescences MIB peuvent être identifiés par leur nom ou par les numéros représentant la position de l'objet ou de la sous-arborescence dans la hiérarchie MIB.

INCLUSION Niveau d'inclusion de la famille spécifiée dans la vue. Les options incluent :

- include la vue inclut la sous-arborescence spécifiée.
- exclude la vue exclut la sous-arborescence spécifiée.

switch(config)#**snmp-server view sys-view system include**
switch(config)#**snmp-server view sys-view system.2 exclude**

switch(config)#**snmp-server view all-items iso included**

La vue s'appelle all-items la famille iso et on inclut tout

La commande snmp-server group configure un nouveau protocole de gestion de réseau simple (SNMP) ou modifie un groupe existant. Un groupe SNMP est une structure de données que les déclarations d'utilisateur référence pour mapper les utilisateurs SNMP aux contextes et vues SNMP, fournissant une politique d'accès commune au utilisateurs spécifiés

snmp-server group *group_name* **VERSION** [**CNTX**][**READ**][**WRITE**][**NOTIFY**]

Cette commande configure **group_name** comme groupe SNMP version 3 (authentification et cryptage) qui donne accès à la vue de lecture et écriture de la famille all-items.

Exemples :

switch(config)#**snmp-server group** <group_name> **v3 priv read write all-items**

v3 priv SNMPv3. HMAC-MD5 or HMAC-SHA authentication. AES or DES encryption.

all-items: nom de la famille

La commande snmp-server user ajoute un utilisateur à un protocole SNMP (Simple Network Management Protocol) groupe ou modifie les paramètres d'un utilisateur existant.

snmp-server user *user_name group_name* [**AGENT**] **VERSION** [**ENGINE**][**SECURITY**]

SÉCURITY Spécifie les niveaux d'authentification et de cryptage. Disponible uniquement si SNMP est v3.

Le chiffrement est disponible uniquement lorsque l'authentification est configurée.

- pas de paramètre pas d'authentification ni de cryptage.
- paramètres d'authentification auth a_meth a_pass [priv e_meth e_pass].
- Méthode d'authentification a_meth : les options sont **md5** (HMAC-MD5-96) et **sha** (HMAC-SHA-96).
- chaîne d'authentification a-pass pour les utilisateurs recevant des paquets.
- Méthode de cryptage e-meth : les options sont **aes** (AES-128) et **des** (CBC-DES).
- Chaîne de cryptage e-pass pour les utilisateurs envoyant des paquets.

switch(config)#**snmp-server user** <user_name> <group_name> **v3 auth sha** <auth_password> **priv aes** <priv_password>

switch(config)#**snmp-server user** <user_name> <group_name> **v3 auth md5** <auth_password> **priv des** <priv_password>

La commande snmp-server host configure un hôte SNMP (auquel seront envoyés les traps SNMP) et définit la chaîne de communauté si elle n'a pas été configurée précédemment. L'hôte est désigné par l'emplacement de l'hôte et la chaîne communautaire. La commande spécifie également le type de notifications SNMP qui sont envoyées

switch(config)#**snmp-server host <IP_address> version 3 auth <user_name>**

Connexion SSH

Sur l'ordinateur
mkdir mgmt
cd mgmt
ssh-keygen
cat ssh_key.pub
Arista-720XP-CS1(config)#username kevin privilege 15 role network-admin secret secret_pass
Arista-720XP-CS1(config)#username kevin ssh-key ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABkeypublic
sur ordi
ssh kevin@192.168.30.30 -i ssh_key

Restauration et sauvegarde

switch#copy flash:/EOS-4.8.3.swi ftp:/FTP_Username@FTP_IP/EOS-4.8.3.swi

5 Le routage

Création d'une route statique

Niveau 3 : le routage statique

Conf t
Interface ethernet1
Ip address 192.9.201.0/24 Vlan10
ip route 192.9.201.0/24 Vlan10
ip route 0.0.0.0/0 192.14.0.4 route par défaut
show ip route

Pour améliorer les routage statique avec ce swicth
Ip routing
Ip route network netmask gateway

Niveau 3 : le routage dynamique

RIP:
SW-1(config)#**router rip**
SW-1(config-router-rip)#**no shutdown**
Ces commandes attribuent une distance administrative de 75 aux routes RIP. La commande de distance attribue un distance administrative par rapport aux routes que le commutateur apprend via RIP.
switch(config)#**router rip**
switch(config-router-rip)#**distance 75**
Les commandes suivantes démontrent qu'une liste d'accès ou une liste de préfixes peut être utilisée dans une feuille de route pour une utilisation dans une liste de distribution.
switch(config)#**ip prefix-list 8to24 seq 5 permit 0.0.0.0/0 ge 8 le 24**
switch(config)#**route-map myRouteMap permit 10**
switch(config-route-map-myRouteMap)#**match ip address prefix-list 8to24**
switch(config-route-map-myRouteMap)#**exit**
switch(config)#
switch(config)#**router rip**
switch(config-router-rip)#**distribute-list in route-map myRouteMap**
switch(config-router-rip)#
• Ces commandes suppriment les routes annoncées sur une interface particulière.
switch(config)#**ip prefix-list 2 seq 10 deny 30.1.1.0/24**
switch(config)#**route-map myRmOut permit 10**
switch(config-route-map-myRmOut)#**match ip address prefix-list 2**
switch(config-route-map-myRouteMap)#**exit**
switch(config)#**router rip**
switch(config-router-rip)# **distribute-list out route-map myRmOut**
Cette commande définit la valeur de métrique par défaut sur cinq.switch(config)#**router rip**
switch(config-router-rip)#**metric default 5**
Cette commande active RIP sur 10.168.1.1/24

switch(config)#**router rip**
switch(config-router-rip)#**network 10.168.1.1/24**
Cette commande définit l'intervalle de mise à jour sur 60 secondes, le délai d'expiration sur 90 secondes et le délai de suppression sur 150 secondes.
switch(config-router-rip)#**timers 60 90 150**
switch>**show ip rip database**
switch>**show ip rip neighbors**

OSPF:
SW-1# **conf t**
SW-1(config)#**int eth5**
SW-1(config-if-Et5)#**ip ospf authentication-key abcdefgh**
SW-1(config-if-Et5)#**ip ospf cost 10**
SW-1(config-if-Et5)#**ip ospf priority 6**
SW-1(config-if-Et5)#**router ospf 1**
SW-1(config-router-ospf)#**router-id 1.1.1.1**
SW-1(config-router-ospf)#**network 2.2.2.0/24 area 0**
SW-1(config-router-ospf)#**no shut**
SW-1#**show ip ospf neighbor**
Interface d'adresse de temps mort d'état Pri VRF d'identification de voisin
1.1.1.2 default 4 FULL/BDR 00:00:36 2.2.2.2 Ethernet5
SW-2#**show ip ospf interface**
Ethernet5 is up
Interface Address 2.2.2.2/24, VRF default, Area 0.0.0.0
Network Type Broadcast, Cost: 20
Transmit Delay is 1 sec, State Backup DR, Priority 4
Designated Router is 1.1.1.1
Backup Designated Router is 1.1.1.2
Timer intervals configured, Hello 10, Dead 40, Retransmit 5

BGP:
Ce code configure l'instance BGP de l'exemple 1 sur les deux commutateurs.
Step 1 Configurez les adresses des voisins.
a. Specify the neighbor to Switch A.
switchA(config)#**router bgp 100**
switchA(config-router-bgp)#**neighbor 10.100.100.2 remote-as 100**
b. Spécifiez le voisin du commutateur B.
switchB(config)#**router bgp 100**
switchB(config-router-bgp)#**neighbor 10.100.100.1 remote-as 100**
Step 2 Configurez les itinéraires à annoncer.
a. Annoncez les itinéraires du commutateur A.
switchA(config-router-bgp)#**network 10.10.1.0/24**
switchA(config-router-bgp)#**network 10.10.2.0/24**
b. Annoncez les itinéraires du commutateur B.
switchB(config-router-bgp)#**network 10.10.3.0/24**
switchB(config-router-bgp)#**network 10.10.4.0/24**

Step 3 Configure the LOCAL_PREF.
switchA(config-router-bgp)#**neighbor 10.100.100.2 export-localpref 150**
switchB(config-router-bgp)#**neighbor 10.100.100.1 export-localpref 75**
Step 4 Modify the hold time and keepalive interval.
switchA(config-router-bgp)#**timer bgp 30 90**
switchB(config-router-bgp)#**timer bgp 30 90**
SW-1#**show ip bgp summary**
BGP summary information for VRF default
Router identifier 1.1.1.1, local AS number 100
Neighbor Status Codes: m - Under maintenance
Neighbor V AS MsgRcvd MsgSent InQ OutQ Up/Down State PfxRcd PfxAcc
2.2.2.2 4 **100** 5 5 0 0 00:00:40 Estab 1 1

SW-2#**show ip bgp summary**
BGP summary information for VRF default
Router identifier 1.1.1.2, local AS number 100
Neighbor Status Codes: m - Under maintenance
Neighbor V AS MsgRcvd MsgSent InQ OutQ Up/Down State PfxRcd PfxAcc
2.2.2.1 4 **100** 5 5 0 0 00:00:22 Estab 1 1
SW-1#**show ip bgp summary**
Router identifier 1.1.1.1, local AS number 100
Neighbor Status Codes: m - Under maintenance
Neighbor V AS MsgRcvd MsgSent InQ OutQ Up/Down State PfxRcd PfxAcc
2.2.2.2 4 **200** 5 5 0 0 00:00:41 Estab 1 1

IS-IS:
Ces commandes définissent l'adresse actuelle de la zone IS-IS et l'ID système de l'appareil.
switch(config)#**router isis Osiris**
switch(config-router-isis)# **net 49.0001.1010.1040.1030.00**
Ces commandes activent et entrent dans le mode famille d'adresses pour la monodiffusion IPv4.switch(config)#**router isis Osiris**
switch(config-router-isis)#**address-family ipv4 unicast**
switch(config-router-isis)#**interface ethernet 5**
switch(config-if-Eth4)#**isis enable Osiris**

MPLS
This command enables MPLS routing.
switch(config)#**mpls ip**
switch(config)#**show running-config**
Example
mpls ip
These commands create an MPLS rule that matches packets with a top label value of 3400 and causes the removal of the top label from the header stack. The nexthop destination of the IPv4 payload is IP address 10.14.4.4 through Ethernet interface 3/3/3. This rule has a metric value of 100.
switch(config)#**mpls static top-label 3400 ethernet 3/3/3 10.14.4.4 pop payload-type ipv4**
These commands create a backup rule that forwards the packet through Ethernet interface 4/3. This rule's metric value of 150 assigns it backup status prior to the first rule.

switch(config)#**mpls static top-label 3400 ethernet 4/3 10.14.4.4 pop payload-type ipv4 metric 150**
These commands create an MPLS rule that forwards the packet to the nexthop address through any interface.
switch(config)#**mpls static top-label 4400 10.15.46.45 pop payload-type ipv4**
This command configures a static tunnel for the tunnel endpoint 64.0.0.1 and pushes a label 11111 to it.
switch(config)#**mpls static STATIC 64.0.0.1/32 54.0.0.1 Port-Channel7 label-stack 11111**
switch>**show mpls config route**
switch>**show mpls route summary**
SW-1#**show mpls config route**
Codes: S - Static MPLS Route, IA - IS-IS SR Adjacency Segment,
IP - IS-IS SR Prefix Segment, L - LDP,
IL - IS-IS SR Segment to LDP, LI - LDP to IS-IS SR Segment, R - RSVP
In-Label Out-Label Metric Payload NextHop Egress-Acl
-------- --------- ------ ------- ----------- ----------
3400 pop 100 ipv4 2.2.2.2,Et5 Apply
3400 pop 100 ipv4 2.2.2.2,Et4 Apply
4400 pop 100 ipv4 2.2.2.2 Apply

6 Restauration et sauvegarde

AristaSwitch# **username william secret william privilege 15**

utilisateur Ensuite, nous aurons besoin de ce compte d'utilisateur pour se connecter directement au mode Activer (l'invite #), et non au mode Utilisateur (l'invite >).
Pour configurer le commutateur pour qu'il devienne un serveur SCP et que nous supposerons que le serveur RADIUS ou TACACS n'est pas utilisé par le commutateur Arista

Pour ce faire, utilisez les commandes d'autorisation aaa.

AristaSwitch#**aaa authorization exec default local**

Copier le fichier d'un hôte distant vers un hôte local

scp username@from_host:file.txt /local/directory/

déplacer un fichier du commutateur vers un répertoire local sur mon ordinateur :

*arista-switch#***scp eos-admin@192.168.30.30 :/mnt/flash/ARP_Output.txt**

Copier un fichier d'un hôte local vers un hôte distant

scp file.txt username@to_host:/remote/directory/

Voici comment transférer une image logicielle EOS d'un commutateur vers un hote distant

cd /mnt/flash/

*arista-switch#***scp EOS-4.25.5.1M.swi eos-admin@192.168.30.70 :/mnt/flash/**

Copier un IOS de la clef usb vers la flash

copy usb1:/EOS-4.14.4.swi flash:/EOS-4.14.4.swi

Copier un IOS d'un serveur ssh vers la flash

copy scp://user@10.1.1.8/user/EOS-4.13.2.swi flash:/EOS-4.13.2.swi

scp /Users/mohammadtahir/Downloads/vEOS64-lab-4.24.2F.swi admin@192.168.86.125:/mnt/flash

switch#**configure terminal**
switch(config)#**boot system flash:/EOS-4.14.4.swi**
switch(config)#**show boot-config**
switch#**write**

Ces commandes configurent le 10.15.17.9 comme adresse IP source que le commutateur utilise lorsque communiquer avec les serveurs TFTP.

switch(config)#**interface vlan 10**
switch(config-if-Vl10)#**ip address 10.15.17.9/24**
switch(config-if-Vl10)#**ip tftp client source-interface vlan 10**
switch(config)#

Activation du SSH

cat ssh_key.pub

Il est maintenant temps de créer le compte sur le commutateur Arista. Vous pouvez configurer le compte pour qu'il utilise une clé ssh uniquement :

*arista-switch***(config)#username kevin privilege 15 role network-admin nopassword**

Vous pouvez également configurer le compte pour qu'il accepte également un mot de passe en cas de perte de la clé SSH :

*arista-switch#***(config)#username kevin privilege 15 role network-admin secret secret_pass**

Vous devez maintenant ajouter la clé publique du nom d'utilisateur que vous avez configuré :

*arista-switch#***(config)#username kevin ssh-key ssh-rsa AAAAB3NzaC1yc2EAAAA……**

Temps de test :

Mon ordi$ ssh kevin@192.168.30.30 -i ssh_key

scp /mnt/flash/startup-config <USER>@<SERVER>:/<path> >> /etc/cron.daily/configpush
chmod 755 /etc/cron.daily/configpush

SSH

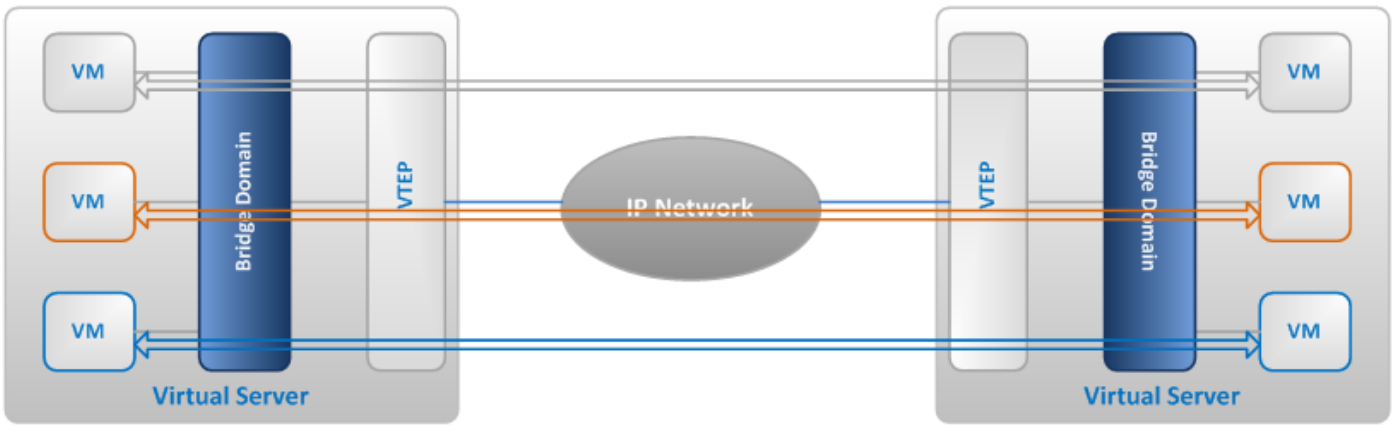
SSH est activé par défaut et une clé est générée par défaut, mais vous devez avoir un nom d'utilisateur/mot de passe pour pouvoir vous connecter

Vous pouvez configurer un nom d'utilisateur avec :

username admin role network-admin priv 15 secret arista

7 VXLAN signifie Virtual Extensible LAN (réseau local extensible virtuel).

Il s'agit d'une technologie de virtualisation de réseau utilisée pour étendre les segments de réseau de la couche 2 (couche de liaison de données) sur un réseau IP. Elle a été introduite pour répondre aux limites des VLAN traditionnels dans les centres de données à grande échelle.

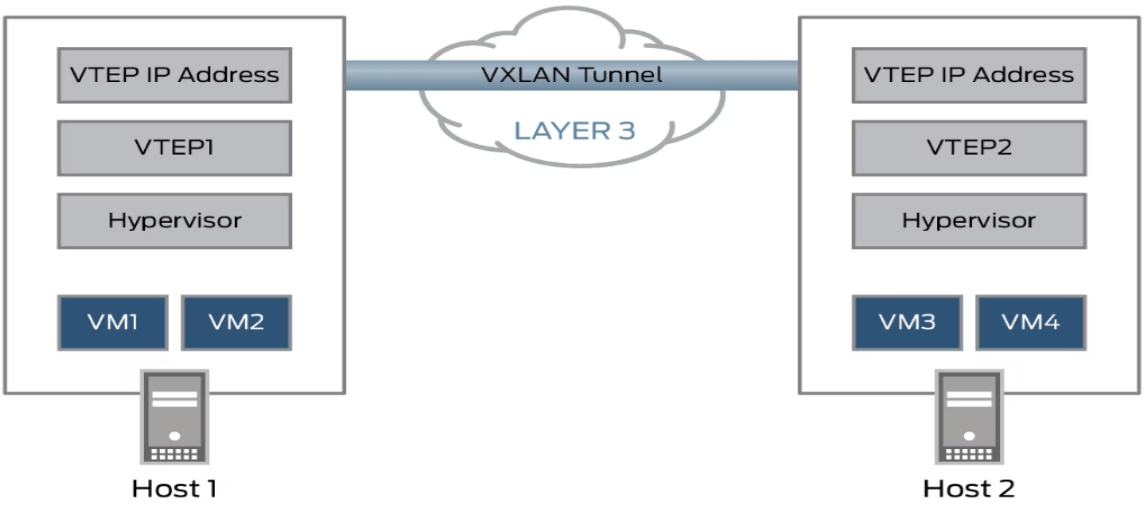


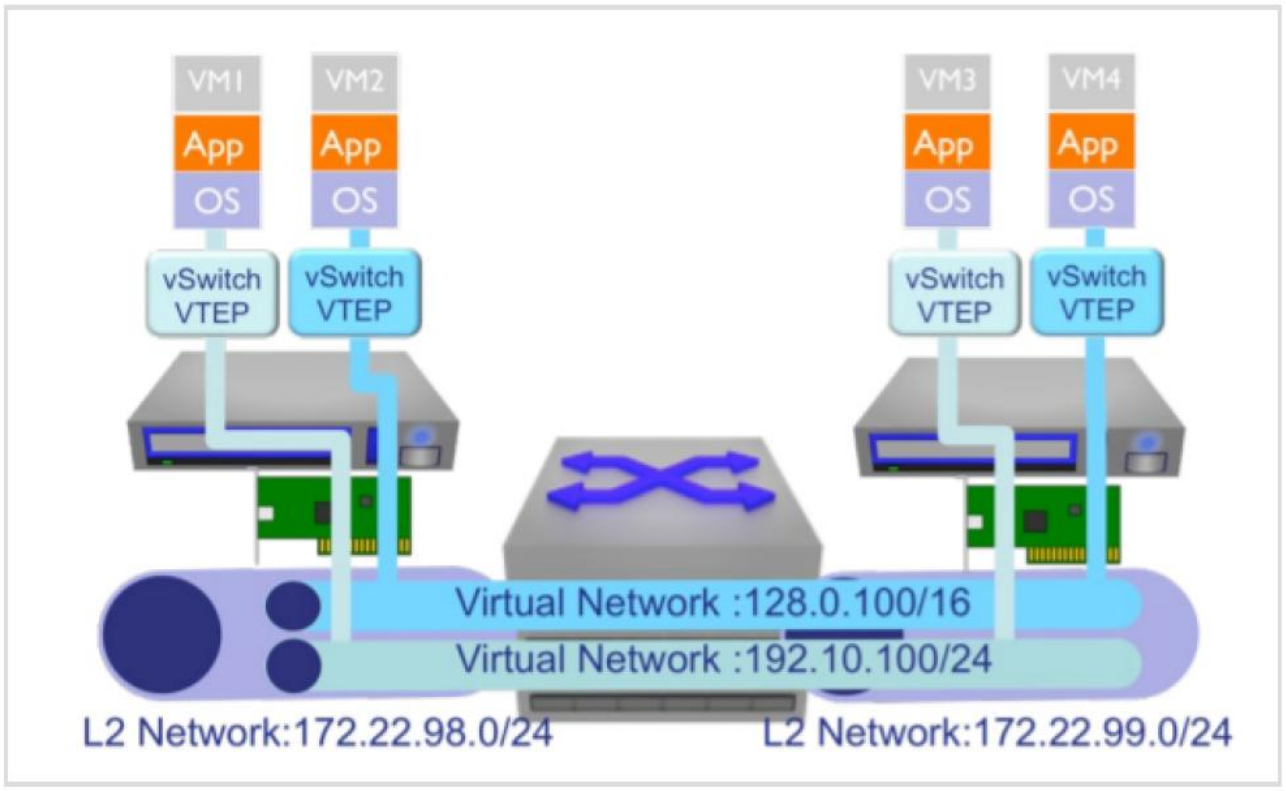
Il est couramment utilisé dans les centres de données et les environnements en nuage pour créer des superpositions de réseaux logiques qui peuvent couvrir plusieurs segments de réseaux physiques.
VXLAN encapsule les trames Ethernet de couche 2 dans des paquets UDP de couche 3, ce qui leur permet d'être transmises sur un réseau IP de couche 3.



Encapsulation VXLAN

Comment fonctionne VXLAN ?
Imaginez que vous ayez un grand centre de données avec plusieurs serveurs physiques et des machines virtuelles (VM)fonctionnant sur ces serveurs.
Dans un réseau traditionnel basé sur un VLAN, chaque machine virtuelle est affectée à un VLAN spécifique. La communication entre les machines virtuelles de différents VLAN nécessiterait un routage au niveau de la couche 3. Cette approche peut devenir complexe et présenter des problèmes d'évolutivité en raison du nombre limité d'ID de VLAN disponibles.





chaque VM sur une machine physique est identifiée par un identifiant réseau VxLAN sur 24 bits, nommé VNI.
L'hyperviseur de chaque serveur gère l'encapsulation et la décapsulation des trames contenues dans les VxLANs (VTEP: VxLAN Tunnel EndPoint).
Supposons qu'une machine virtuelle située sur un réseau virtuel (VxLAN) dans un serveur physique souhaite transmettre des données vers une machine virtuelle située dans un autre serveur physique (VxLAN). La machine virtuelle source construit sa trame Ethernet avec les champs suivants :

L'hyperviseur de la machine virtuelle encapsule la trame Ethernet dans la couche UDP

Examinons un scénario pour comprendre le fonctionnement de ce VXLAN.

Il y a deux hôtes physiques. Dans l'hôte 1, il y a VM1 et VM2, et dans l'hôte 2, il y a VM3 et VM4.
Supposons que les hôtes 1 et 2 font partie d'un réseau VXLAN et que VM1 souhaite communiquer avec VM3.

Configuration VXLAN

L'hôte 1 et l'hôte 2 sont configurés en tant que points d'extrémité de tunnel VXLAN (VTEP). Cela signifie qu'ils disposent des composants logiciels ou matériels nécessaires pour gérer l'encapsulation et la décapsulation VXLAN.

Identifiant de réseau VXLAN (VNI)

Un VNI unique est attribué au réseau virtuel. Disons que le VNI de ce réseau est 1001.

Encapsulation

VM1, qui réside sur l'hôte 1, souhaite communiquer avec VM3, qui se trouve sur l'hôte 2.

Lorsque VM1 envoie un paquet à VM3, il est encapsulé avec un en-tête VXLAN.

L'en-tête VXLAN comprend les adresses VTEP source et destination (adresses IP de l'hôte 1 et de l'hôte 2) et le VNI (1001).

Réseau IP sous-jacent

Le paquet encapsulé est transmis sur le réseau IP sous-jacent – il peut s'agir d'IPv4 ou d'IPv6. Le réseau IP sert d'infrastructure de transport pour les paquets VXLAN.

Décapsulation

À la réception du paquet, le VTEP de l'hôte 2 décapsule l'en-tête VXLAN, ce qui révèle la trame Ethernet de couche 2 d'origine.

Livraison à VM3

Après la décapsulation, le VTEP transmet la trame Ethernet de couche 2 au VM3 de l'hôte 2.

VM1 sur l'hôte 1 peut communiquer avec VM3 sur l'hôte 2 comme s'ils étaient connectés au même réseau Ethernet de couche 2, même s'ils sont situés sur des hôtes physiques différents.

VXLAN permet cette communication en encapsulant et en tunnelant le trafic de la couche 2 sur les réseaux de la couche 3, ce qui permet d'étendre la connectivité de la couche 2 au-delà des limites du réseau.

Évolutivité

VXLAN répond aux limites des VLAN traditionnels en permettant de créer jusqu'à 16 millions de réseaux virtuels, alors que les VLAN sont limités à 4 096. Cette évolutivité est obtenue grâce à l'identificateur de réseau VXLAN (VNI) de 24 bits.

Segmentation du réseau

VXLAN permet une segmentation efficace du réseau en encapsulant les trames Ethernet de couche 2 dans des paquets UDP. Cela permet de créer des réseaux virtuels isolés qui peuvent s'étendre au-delà des frontières physiques, comme les centres de données ou les environnements en nuage.

Multi-tenance

Il prend en charge le modèle multi-tenant, qui permet à différentes organisations de partager la même infrastructure physique tout en conservant leurs propres réseaux virtuels isolés.

Extension de la couche 2 sur les réseaux de la couche 3

Ceci est important pour la construction de centres de données géographiquement distribués et permet la mobilité des machines virtuelles sur différents sites sans avoir recours à des technologies complexes d'extension de la couche 2 telles que Virtual Private LAN Service (VPLS).
La mise en œuvre correcte de VXLAN nécessite des dispositifs compatibles VXLAN qui prennent en charge les protocoles et les techniques d'encapsulation nécessaires.
Les réseaux VXLAN peuvent être créés et gérés à l'aide de ces dispositifs.
D'autre part, les VLAN sont plus largement utilisés et plus simples à mettre en œuvre dans les infrastructures de réseau actuelles, car la majorité des équipements de réseau les prennent en charge sans nécessiter de matériel supplémentaire ou de support spécialisé.

Interconnexion de centres de données

VXLAN est utilisé pour interconnecter plusieurs centres de données sur un réseau étendu. Il étend la connectivité de couche 2 entre les centres de données, ce qui permet de migrer les machines virtuelles et les charges de travail entre les sites tout en conservant leur configuration réseau.

Infrastructure en nuage
Elle est couramment utilisée dans les environnements en nuage afin de fournir une virtualisation du réseau pour les services et les applications en nuage. Il permet une distribution efficace de la charge de travail dans l'infrastructure en nuage.

Réseaux superposés
VXLAN sert de base aux réseaux superposés qui permettent aux ingénieurs réseau d'allouer dynamiquement les ressources et de s'adapter à l'évolution de la charge de travail.

Reprise après sinistre
Utilisé dans les scénarios de reprise après sinistre pour fournir une connectivité réseau et un basculement (mode opérationnel de secours) entre les centres de données primaires et secondaires.

Voici un tableau comparatif entre VXLAN et VLAN.

Fonctionnalités	**VXLAN**	**VLAN**
Encapsulation	Utilise UDP pour l'encapsulation et le transport des paquets	Pas d'encapsulation – repose sur le marquage 802.1Q
Évolutivité	Prend en charge jusqu'à 16 millions de réseaux virtuels	Limité à 4 096 VLAN
Isolation des réseaux	Permet d'isoler les réseaux de la couche 2 à travers les frontières de la couche 3	Isolation au sein d'un réseau de couche 2
Gestion du trafic de diffusion	Utilise la réplication basée sur le multicast ou l'unicast pour optimiser le trafic de diffusion	Le trafic de diffusion est propagé à tous les ports du VLAN
Couverture de plusieurs sites	Permet d'étendre les réseaux de couche 2 à des sites géographiquement dispersés	Limité à un seul domaine de diffusion
Gestion	Nécessite une passerelle VXLAN pour interconnecter les réseaux virtuels et physiques	Peut être géré par des commutateurs compatibles avec les VLANs

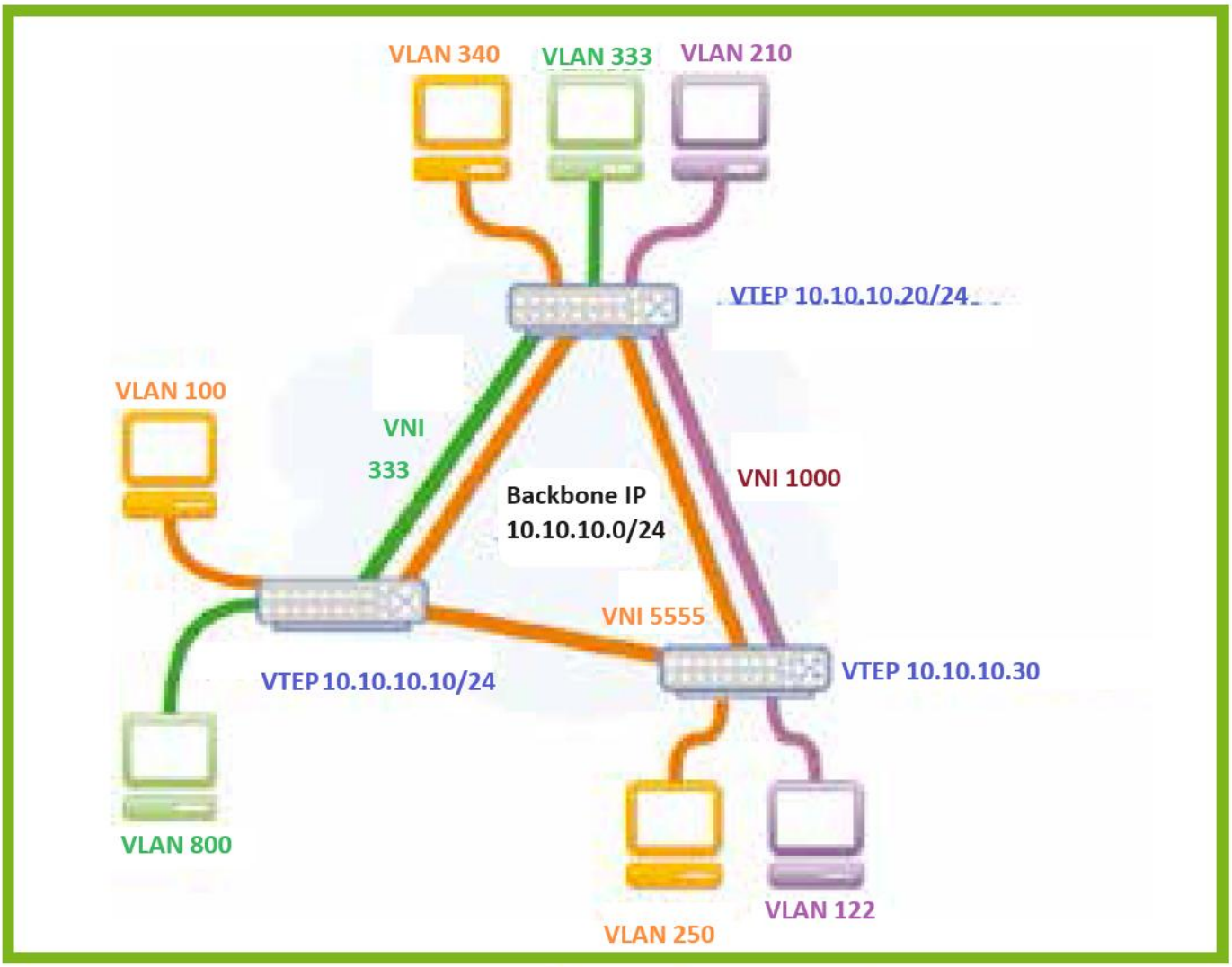


Figure 5 : Binding des VNI / VTEP.

Prenons un exemple simple avec 3 VTEP, 3 VNI et autant de VLAN que de machines. Au travers du VNI 5555, nous pourrons faire communiquer les VLAN locaux 100, 340 et 250. Au travers du VNI 1000, nous pourrons faire communiquer les VLAN 122 et 210, qui sont uniques et bien différents, car pas sur le même switch ni derrière la même VTEP. Idem pour le VNI 333.
VxLAN permettre d'étendre les domaines de broadcast par l'usage des réseaux IP. Cela pose un problème de taille : comment faire fonctionner des réseaux de niveau 2 travaillant uniquement sur le forwarding par adresse MAC de destination à travers des réseaux IP se basant sur des technologies de routage ?
Dans le cas où les adresses MAC sont connues, cela est simple, on forwarde le paquet encapsulé localement, ou à la VTEP identifiée
comme portant l'adresse MAC. Mais comment faire lorsque l'adresse MAC n'est pas connue ? Où envoyer le paquet ? C'est le problème bien connu du « Flood and Learn », car dans les cas des paquets BUM (Broadcast, Unknown Unicast, Multicast), Figure 4 : il va falloir répliquer le paquet sur l'ensemble des VTEP participant au réseau VxLAN pour garantir le fonctionnement normal du domaine de broadcast.
Ainsi, lorsque les adresses MAC sont connues, la VTEP et son switch disposeront, en plus d'une table d'association MAC <> Port pour le forwarding, d'une table d'association MAC <> IP, l'IP étant la VTEP sur laquelle il faudra router le paquet encapsulé.

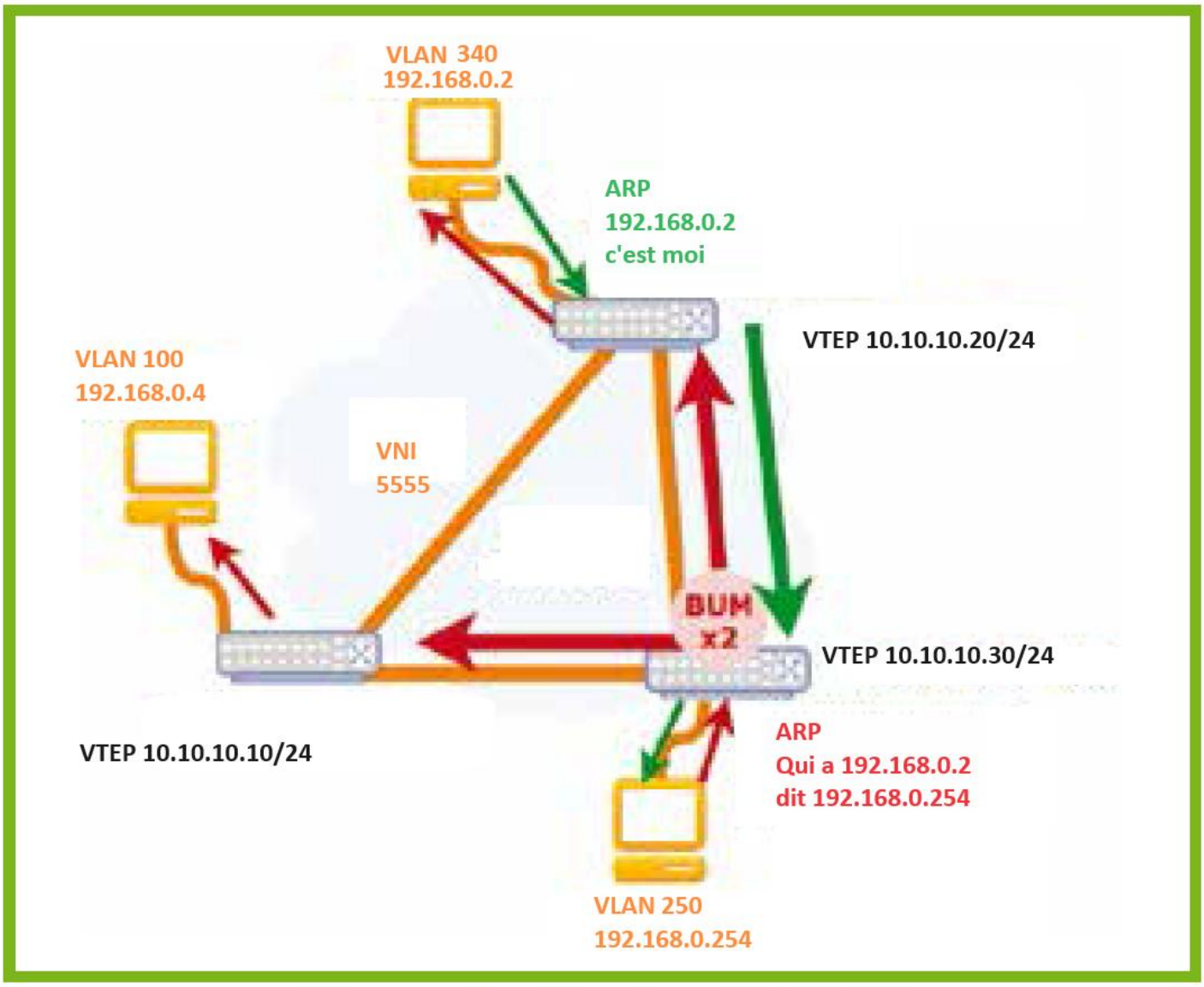


Figure 6 : Gestion du BUM.

Ces deux méthodes n'étant pas ultimes ou ayant leurs propres limitations, l'idée est venue de gérer les réseaux VxLAN avec des extensions déjà existantes dans le protocole BGP, MP-BGP (Multi Protocol BGP). Ceci permet de séparer le Control Plane (décision de routage/forwarding) et le Data Plane (actions de routage/ forwarding). Dans le cas de MP-BGP, on remplace le RendezVousPoint par un ou plusieurs Route Reflector qui occupera le rôle de Control Plane. Ce dernier va s'occuper pour la famille d'adresses E-VPN de maintenir la table de routage des MAC au travers du VxLAN et de la distribuer par le protocole BGP aux switchs clients portant chacun une VTEP, tout en conservant HER, mais en simplifiant la configuration. Ces switchs seront alors uniquement des membres du Data Plane.
Cette méthode [9] de déploiement est très intéressante, car au-delà d'utiliser des technologies existantes et éprouvées (BGP), celle-ci introduit des mécanismes de NLRI (Network Layer Reachability Information) permettant de limiter les floods de BUM, voire de programmer des routes vers certaines MAC en dur pour sécuriser l'infrastructure finale. Cette méthode permet également de sécuriser plus facilement les VTEP, par l'ajout de mécanismes d'authentification déjà existants dans BGP.

VXLAN

Ces commandes créent l'interface de tunnel VXLAN 1, placent le commutateur en mode de configuration d'interface VXLAN et afficher les paramètres du nouveau VTI.

switch(config)#interface vxlan 1
switch(config-if-Vx1)#show active

Ces commandes configurent VTI 1 pour utiliser l'adresse IP 10.25.25.3 (interface de bouclage 15) comme interface source dans le champs d'encapsulation des trames VXLAN sortantes.

switch(config)**#interface loopback 15**
switch(config-if-Lo15)**#ip address 10.25.25.3/24**
switch(config-if-Lo15)**#exit**
switch(config)**#interface vxlan 1**
switch(config-if-Vx1)**#vxlan source-interface loopback 15**
switch(config-if-Vx1)**#show active**

Cette commande associe le port UDP 5500 à l'interface VXLAN 1.

switch(config)**#interface vxlan 1**
switch(config-if-Vx1)**#vxlan udp-port 5500**
switch(config-if-Vx1)**#show active**

Ces commandes associent le VLAN 100 au VNI 100 et le VLAN 200 au VNI 10.10.200.

switch(config)**#interface vxlan 1**
switch(config-if-Vx1)**#vxlan vlan 100 vni 100**
switch(config-if-Vx1)**#vxlan vlan 200 vni 10.10.200**
switch(config-if-Vx1)**#show active**
switch(config-if-Vx1)**#vxlan vni notation dotted**
switch(config-if-Vx1)**#show active**

Cette commande associe l'adresse de multidiffusion 227.10.1.1 au VTI 1.

switch(config)**#interface vxlan 1**
switch(config-if-Vx1)**#vxlan multicast-group 227.10.1.1**
switch(config-if-Vx1)**#show active**

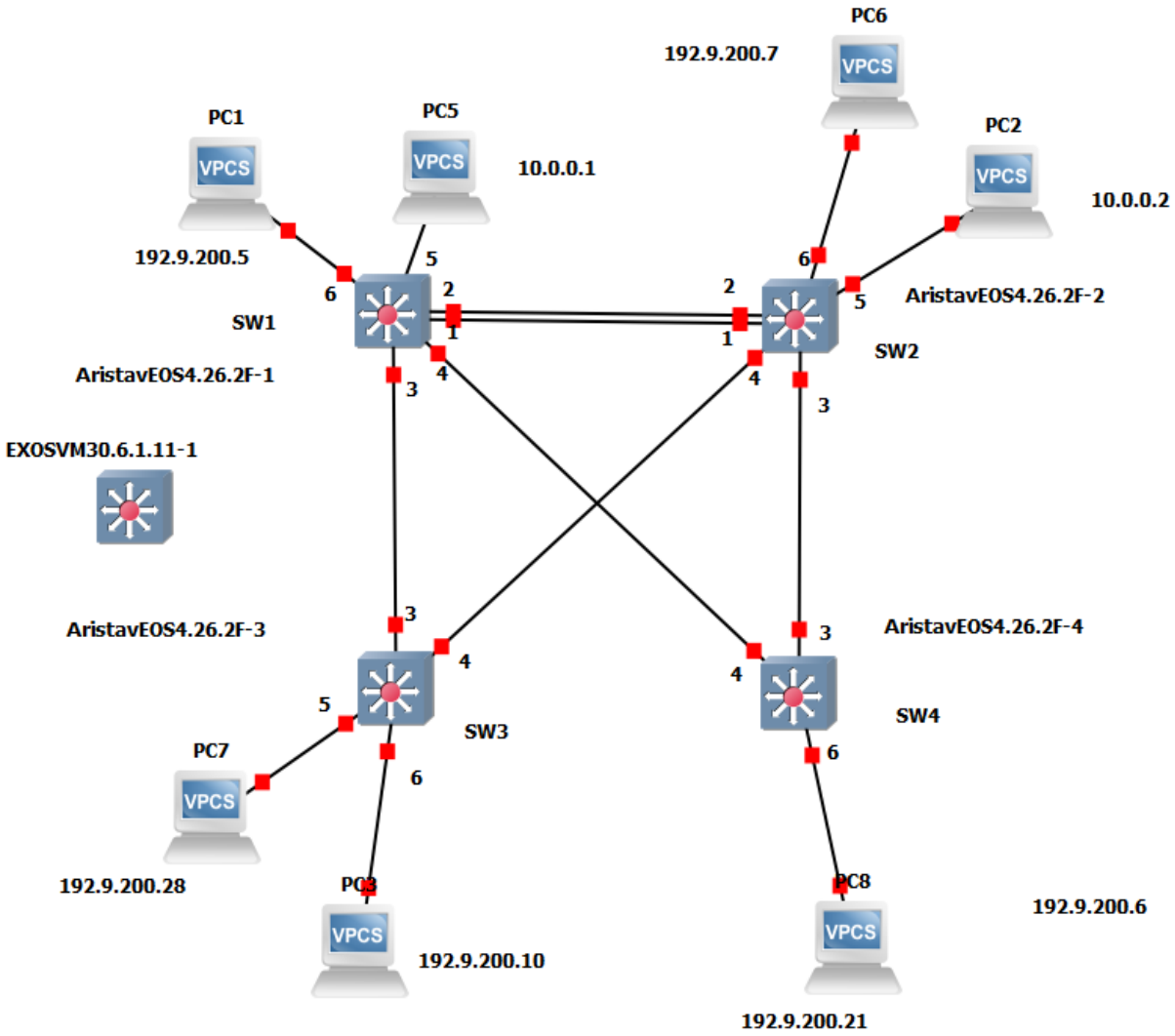
Ces commandes configurent le commutateur A pour effectuer le routage VXLAN. L'exemple inclut le routage OSPF utilisé pour routage de sous-couche.

switch-A(config)**#route-map vxlanvlan permit 10**
switch-A(config-route-map-vxlanvlan)**#match interface loopb5**
switch-A(config-route-map-vxlanvlan)**#exit**
switch-A(config)**#route-map vxlanvlan permit 20**
switch-A(config-route-map-vxlanvlan)**#match interface vlan 100**
switch-A(config-route-map-vxlanvlan)**#exit**
switch-A(config)**#router ospf 1**
switch-A(config-router-ospf)**#redistribute connected route-map vxlanvlan**
switch-A(config-router-ospf)**#exit**
switch-A(config)**#interface loopback 5**
switch-A(config-if-Lo5)**#ip address 10.25.25.3/24**
switch-A(config-if-Lo5)**#exit**
switch-A(config)**#interface vxlan 1**
switch-A(config-if-Vx1)**#vxlan source-interface loopback 5**
switch-A(config-if-Vx1)**#vxlan vlan 100 vni 10000**
switch-A(config)**#interface vlan 100**
switch-A(config-if-Vl100)**#ip address 10.10.10.1/28**

switch-A(config-if-Vl100)**#exit**

Ces commandes créent une liste de réplication de tête de réseau VXLAN par défaut.

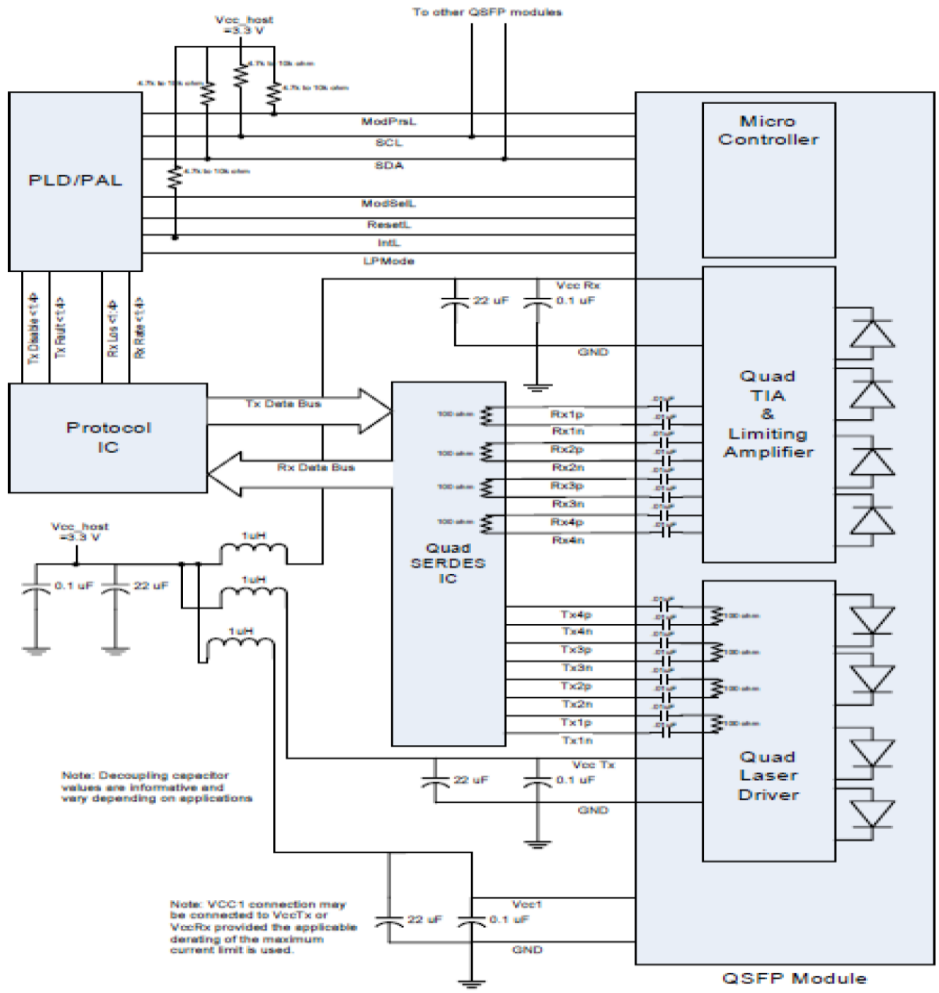
switch(config)**#interface vxlan 1**
switch(config-if-Vx1)**#vxlan flood vtep 10.1.1.1 10.1.1.2**

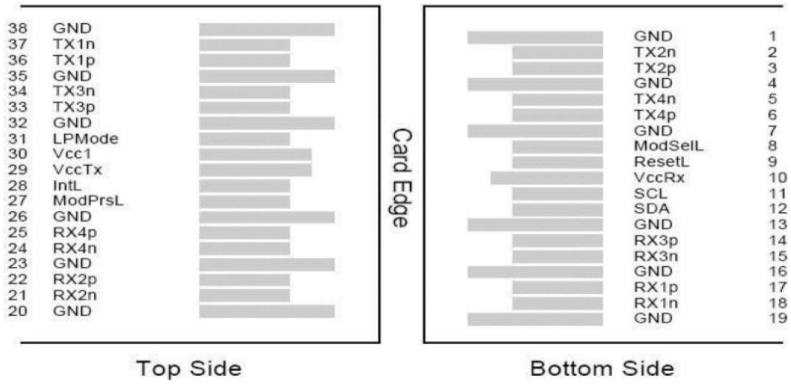


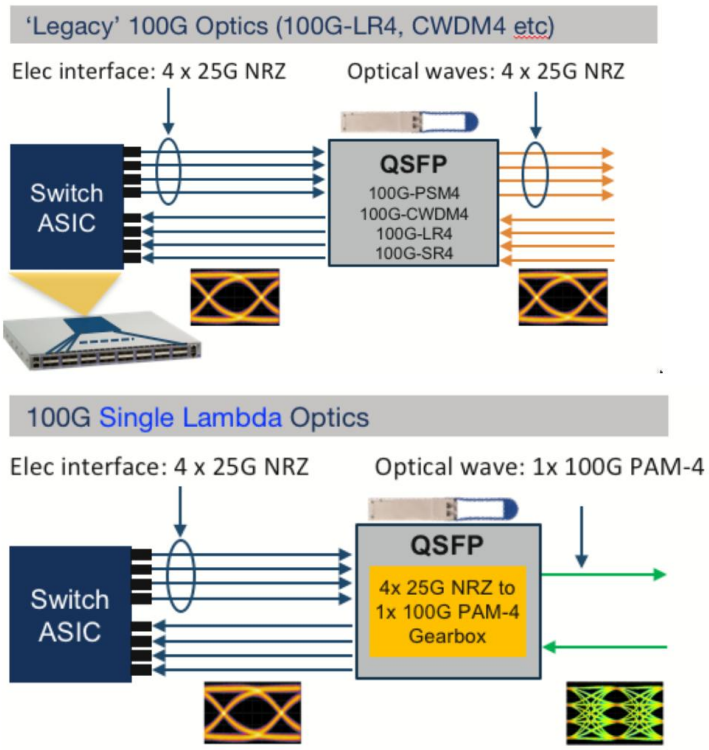
Configuration d'un module QSFP100 en tant qu'interface 100GbE unique

Par défaut, le module QSFP100 fonctionne comme une seule interface 100GbE ; en utilisant la vitesse par défaut ou aucune commande de vitesse sur la voie principale rétablit le comportement par défaut.

Pour configurer explicitement le port comme une seule interface 100GbE, combinez les quatre voies de données du module en en utilisant la commande de vitesse (vitesse forcée 100 gfull) sur la voie /1 du port (la voie principale).



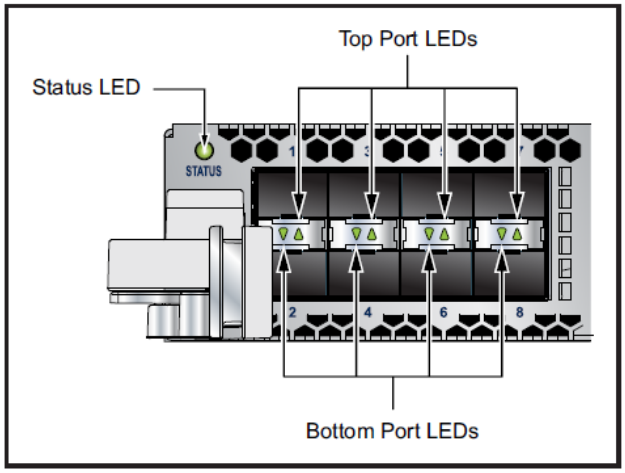


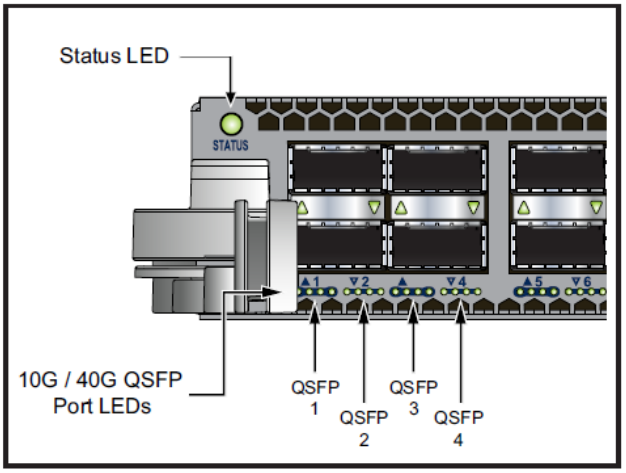


QSFP-100G-SR4

100GBASE-SR4 QSFP optical transceiver, up to 70m over parallel OM3 or 100m over OM4 multimode fiber

QSFP-100G-SR4 / XSR4 MPO-12 (or MTP-12) Parallel Multi-mode Fiber (MMF), OM3 or OM4





La figure à droite affiche les voyants du module QSFP. **Un jeu de quatre LED correspond à chaque module.**
Lorsque le module est programmé comme port 100G, **la première LED de l'ensemble indique l'état** les autres LED sont oranges.
Quand le module est programmé comme quatre ports 25G, chaque port est attribué à une LED dans l'ensemble.

LED State	Status
Off	Port link is down.
Green	Port link is up.
Yellow	Port is disabled in software.

Configuration MLAG

SW1

sw1#sh run

```
! Command: show running-config
! device: sw1 (vEOS-lab, EOS-4.26.5M)
!
! boot system flash:/vEOS-lab.swi
!
no aaa root
!
transceiver qsfp default-mode 4x10G
!
service routing protocols model ribd
!
hostname sw1
!
spanning-tree mode mstp
no spanning-tree vlan-id 4094
!
vlan 10
!
vlan 4094
   trunk group peertrunk
!
interface Port-Channel1
   switchport mode trunk
   mlag 1
!
interface Port-Channel2
   switchport mode trunk
   mlag 2
!
interface Port-Channel101
   switchport mode trunk
   switchport trunk group peertrunk
!
interface Ethernet1
   channel-group 101 mode active
!
interface Ethernet2
   channel-group 101 mode active
!
interface Ethernet3
   channel-group 1 mode active
!
interface Ethernet4
   channel-group 2 mode active
!
interface Ethernet5
!
interface Ethernet6
   switchport access vlan 10
!
interface Ethernet7
!
interface Ethernet8
!
```

```
interface Ethernet9
!
interface Ethernet10
!
interface Ethernet11
!
interface Ethernet12
!
interface Management1
!
interface Vlan10
  ip address 192.9.200.11/24
  vrrp 10 ipv4 192.9.200.8
!
interface Vlan4094
  no autostate
  ip address 172.17.0.1/16
!
no ip routing
!
mlag configuration
  domain-id mlag_01
  heartbeat-interval 2500
  local-interface Vlan4094
  peer-address 172.17.0.2
  peer-link Port-Channel101
  reload-delay 150
!
end
```

SW2

```
sw2#sh run
! Command: show running-config
! device: sw2 (vEOS-lab, EOS-4.26.5M)
!
! boot system flash:/vEOS-lab.swi
!
no aaa root
!
transceiver qsfp default-mode 4x10G
!
service routing protocols model ribd
!
hostname sw2
!
spanning-tree mode mstp
no spanning-tree vlan-id 4094
!
vlan 10
!
vlan 4094
  trunk group trunkpeer
!
interface Port-Channel1
  switchport mode trunk
  mlag 1
```

```
!
interface Port-Channel2
   switchport mode trunk
   mlag 2
!
interface Port-Channel201
   switchport mode trunk
   switchport trunk group trunkpeer
!
interface Ethernet1
   channel-group 201 mode active
!
interface Ethernet2
   channel-group 201 mode active
!
interface Ethernet3
   channel-group 2 mode active
!
interface Ethernet4
   channel-group 1 mode active
!
interface Ethernet5
!
interface Ethernet6
   switchport access vlan 10
!
interface Ethernet7
!
interface Ethernet8
!
interface Ethernet9
!
interface Ethernet10
!
interface Ethernet11
!
interface Ethernet12
!
interface Management1
!
interface Vlan10
   ip address 192.9.200.12/24
   vrrp 10 ipv4 192.9.200.8
!
interface Vlan4094
   no autostate
   ip address 172.17.0.2/16
!
no ip routing
!
mlag configuration
   domain-id mlag_01
   heartbeat-interval 2500
   local-interface Vlan4094
   peer-address 172.17.0.1
   peer-link Port-Channel201
   reload-delay 150
!
```

```
end
SW3

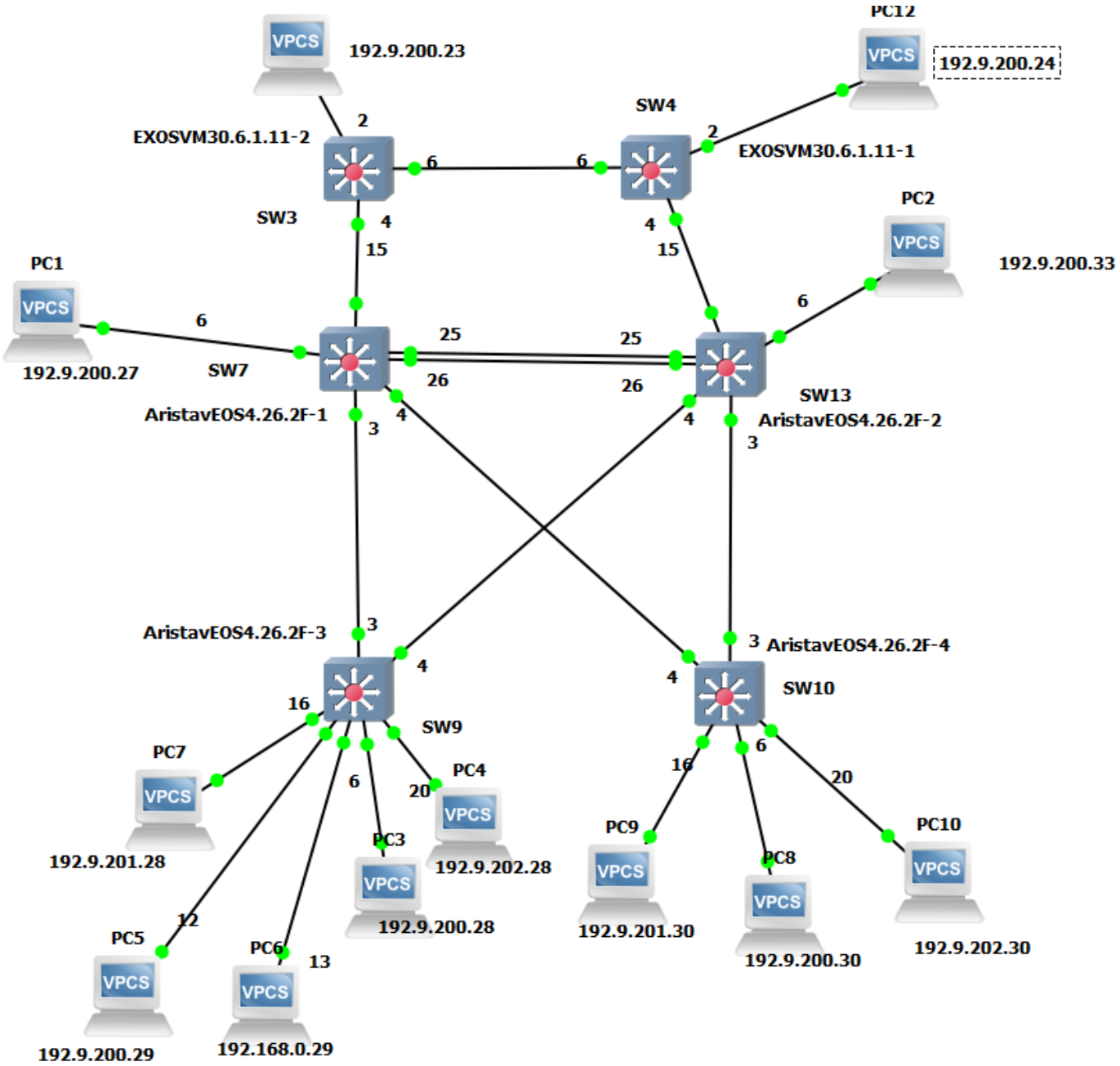

sw3#sh run
! Command: show running-config
! device: sw3 (vEOS-lab, EOS-4.26.5M)
!
! boot system flash:/vEOS-lab.swi
!
no aaa root
!
transceiver qsfp default-mode 4x10G
!
service routing protocols model ribd
!
hostname sw3
!
spanning-tree mode mstp
!
vlan 10
!
interface Port-Channel1
   switchport mode trunk
!
interface Ethernet1
!
interface Ethernet2
!
interface Ethernet3
   channel-group 1 mode active
!
interface Ethernet4
   channel-group 1 mode active
!
interface Ethernet5
   switchport access vlan 10
!
interface Ethernet6
   switchport access vlan 10
!
interface Ethernet7
!
interface Ethernet8
!
interface Ethernet9
!
interface Ethernet10
!
interface Ethernet11
!
interface Ethernet12
!
interface Management1
!
interface Vlan10
   ip address 192.9.200.13/24
   vrrp 10 ipv4 192.9.200.8
```

```
!
no ip routing
!
end
```

SW4

```
sw4#sh run
! Command: show running-config
! device: sw4 (vEOS-lab, EOS-4.26.5M)
!
! boot system flash:/vEOS-lab.swi
!
no aaa root
!
transceiver qsfp default-mode 4x10G
!
service routing protocols model ribd
!
hostname sw4
!
spanning-tree mode mstp
!
vlan 10
!
interface Port-Channel2
   switchport mode trunk
!
interface Ethernet1
!
interface Ethernet2
!
interface Ethernet3
   channel-group 2 mode active
!
interface Ethernet4
   channel-group 2 mode active
!
interface Ethernet5
!
interface Ethernet6
   switchport access vlan 10
!
interface Ethernet7
!
interface Ethernet8
!
interface Ethernet9
!
interface Ethernet10
!
interface Ethernet11
!
interface Ethernet12
!
interface Management1
!
```

```
interface Vlan10
   ip address 192.9.200.14/24
   vrrp 10 ipv4 192.9.200.8
!
ip routing
!
end
```



Pour SW7

localhost(config)#zerotouch cancel

localhost(config)#zerotouch disable

localhost(config)#conf t

localhost(config)#int management 1

localhost(config-if-Ma1)#

localhost(config-if-Ma1)#ip route 0.0.0.0 0.0.0.0 192.168.0.8

localhost(config)#hostname SW7

SW7(config)#username admin secret 0 tpreseau11

SW7(config)#end

SW7(config)#write

SW7(config)#reload

```
SW7(config-if-et1-2)# interface port-channel 101
SW7(config-if-po101)# switchport mode trunk
SW7(config-if-po101)# switchport trunk group peertrunk
SW7(config-if-po101)# exit
SW7(config)#
SW7(config)# vlan 4094
SW7(config-vlan-4094)# trunk group peertrunk
SW7(config-vlan-4094)# interface vlan 4094
SW7(config-if-vl4094)# ip address 172.17.0.1/16
SW7(config-if-vl4094)# no autostate
SW7(config-if-vl4094)# exit
SW7(config)# no spanning-tree vlan-id 4094
SW7(config)#
SW7(config)# mlag configuration
SW7(config-mlag)# local-interface vlan 4094
SW7(config-mlag)# peer-address 172.17.0.2
SW7(config-mlag)# peer-link port-channel 101
SW7(config-mlag)# domain-id mlag_01
SW7(config-mlag)# heartbeat-interval 2500
SW7(config-mlag)# reload-delay 150
SW7(config-mlag)# exit
SW7(config)#vlan 10
SW7(config)#vlan 11
SW7(config)#vlan 12
SW7(config)#vlan 1001
SW7(config)#exit
SW7(config-P01)#interface Port-Channel 1
SW7(config-P01)#switchport mode trunk
SW7(config-P01)#mlag 1
SW7(config-P01)#exit
SW7(config-P02)#interface Port-Channel 2
SW7(config-P02)#switchport mode trunk
SW7(config-P02)#mlag 2
SW7(config-P02)#exit
SW7(config-ET3)#interface Ethernet 3
SW7(config-ET3)#channel-group 1 mode active
SW7(config-ET4)#interface Ethernet 4
SW7(config-ET4)#channel-group 2 mode active
SW7(config-ET4)#exit
SW7(config-ET6)#interface Ethernet 6
SW7(config-ET6)#switchport access vlan 10
```

SW7(config-ET6)#exit
SW7(config-if-eth15)#interface Ethernet 15
SW7(config-if-eth15)#switchport mode trunk
SW7(config-if-eth15)#switchport trunk allowed vlan 10,11,12,1001
SW7(config)# interface ethernet 25-26
SW7(config-if-et25-26)# channel-group 101 mode active
SW7(config)#interface Vlan10
SW7(config-vl10)#ip address 192.9.200.7/24
SW7(config-vl10)#vrrp 10 ipv4 192.9.200.8
SW7(config)#exit
SW7(config)#interface Vlan11
SW7(config-vl10)#ip address 192.9.201.7/24
SW7(config-vl10)#vrrp 11 ipv4 192.9.201.8
SW7(config)#exit
SW7(config)#ip routing
SW7(config)#interface Vlan12
SW7(config-vl10)#ip address 192.9.202.7/24
SW7(config-vl10)#vrrp 12 ipv4 192.9.202.8
SW7(config)#exit
SW7(config)#interface Vlan1001
SW7(config-vl10)#ip address 192.168.0.7/24
SW7(config-vl10)#vrrp 100 ipv4 192.168.0.8
SW7(config)#exit
SW7(config)#ip routing
SW7(config)#snmp-server local-interface Management1
SW7(config)#snmp-server view all-items iso included
SW7(config)#snmp-server group v3group v3 priv read all-items
SW7(config)#snmp-server user v3admin v3group v3 auth md5 v3adminpriv priv des v3adminpriv
SW7(config)#spanning-tree mode rapid-pvst
SW7(config)#write

Switche SW13

localhost(config)#zerotouch cancel
localhost(config)#enable
localhost(config)#zerotouch disable
localhost(config)#conf t
localhost(config)#int management 1
localhost(config-if-Ma1)#
localhost(config-if-Ma1)#ip route 0.0.0.0 0.0.0.0 192.168.0.8
localhost(config)#hostname SW13
SW13(config)#username admin secret 0 tpreseau11

```
SW13(config)#end
SW13(config)#write
SW13(config)#reload
SW13(config-if-et1-2)# interface port-channel 201
SW13(config-if-po201)# switchport mode trunk
SW13(config-if-po201)# switchport trunk group trunkpeer
SW13(config-if-po201)# exit
SW13(config)#
SW13(config)# vlan 4094
SW13(config-vlan-4094)# trunk group trunkpeer
SW13(config-vlan-4094)# interface vlan 4094
SW13(config-if-vl4094)# ip address 172.17.0.2/16
SW13(config-if-vl4094)# no autostate
SW13(config-if-vl4094)# exit
SW13(config)# no spanning-tree vlan-id 4094
SW13(config)#
SW13(config)# mlag configuration
SW13(config-mlag)# local-interface vlan 4094
SW13(config-mlag)# peer-address 172.17.0.1
SW13(config-mlag)# peer-link port-channel 201
SW13(config-mlag)# domain-id mlag_01
SW13(config-mlag)# heartbeat-interval 2500
SW13(config-mlag)# reload-delay 150
SW13(config-mlag)# exit
SW13(config)#
SW13(config)#vlan 10
SW13(config)#vlan 11
SW13(config)#vlan 12
SW13(config)#vlan 1001
SW13(config)#exit
SW13(config-P01)#interface Port-Channel 1
SW13(config-P01)#switchport mode trunk
SW13(config-P01)#mlag 1
SW13(config-P01)#exit
SW13(config-P02)#interface Port-Channel 2
SW13(config-P02)#switchport mode trunk
SW13(config-P02)#mlag 2
SW13(config-P02)#exit
SW13(config-ET3)#interface Ethernet 3
SW13(config-ET3)#channel-group 2 mode active
SW13(config-ET4)#interface Ethernet 4
```

SW13(config-ET4)#channel-group 1 mode active
SW13(config-ET4)#exit
SW13(config-ET6)#interface Ethernet 6
SW13(config-ET6)#switchport access vlan 10
SW13(config-ET6)#exit
SW13(config-if-eth15)#interface Ethernet 15
SW13(config-if-eth15)#switchport mode trunk
SW13(config-if-eth15)#switchport trunk allowed vlan 10,11,12,1001
SW13(config)# interface ethernet 25-26
SW13(config-if-et25-26)# channel-group 201 mode active
SW13(config)#interface Vlan 10
SW13(config-vl10)#ip address 192.9.200.13/24
SW13(config-vl10)#vrrp 10 ipv4 192.9.200.8
SW13(config)#exit
SW13(config)#interface Vlan 11
SW13(config-vl10)#ip address 192.9.201.13/24
SW13(config-vl10)#vrrp 11 ipv4 192.9.201.8
SW13(config)#exit
SW13(config)#ip routing
SW13(config)#interface Vlan 12
SW13(config-vl10)#ip address 192.9.202.13/24
SW13(config-vl10)#vrrp 12 ipv4 192.9.202.8
SW13(config)#exit
SW13(config)#interface Vlan1001
SW13(config-vl10)#ip address 192.168.0.13/24
SW13(config-vl10)#vrrp 100 ipv4 192.168.0.8
SW13(config)#exit
SW13(config)#ip routing
SW13(config)#snmp-server local-interface Management1
SW13(config)#snmp-server view all-items iso included
SW13(config)#snmp-server group v3group v3 priv read all-items
SW13(config)#snmp-server user v3admin v3group v3 auth md5 v3adminpriv priv des v3adminpriv
SW13(config)#spanning-tree mode rapid-pvst
SW13(config)#write

Pour SW9

These commands configure the port channels on SW9
localhost(config)#zerotouch cancel
localhost(config)#zerotouch disable
localhost(config)#conf t

```
localhost(config)#int management 1
localhost(config-if-Ma1)#
localhost(config-if-Ma1)#ip route 0.0.0.0 0.0.0.0 192.168.0.8
localhost(config)#hostname SW9
SW9(config)#username admin secret 0 tpreseau11
SW9(config)#end
SW9(config)#write
SW9(config)#reload
SW9(config)# vlan 10
SW9(config)# vlan 11
SW9(config)# vlan 12
SW9(config)# vlan 1001
SW9(config)#interface Port-Channel 1
SW9(config-if-P01)#switchport mode trunk
SW9(config-if-P01)#switchport
SW9(config-if-P01)#exit
SW9(config-if-eth3)#interface Ethernet 3
SW9(config-if-eth3)#switchport
SW9(config-if-eth3)#channel-group 1 mode active
SW9(config-if-eth3)#exit
SW9(config-if-eth4)#interface Ethernet 4
SW9(config-if-eth4)#switchport
SW9(config-if-eth4)#channel-group 1 mode active
SW9(config-if-eth4)#exit
SW9(config-if-eth6)#interface Ethernet 6
SW9(config-if-eth6)#switchport
SW9(config-if-eth6)#switchport access vlan 10
SW9(config-if-eth6)#exit
SW9(config-if-eth12)#interface Ethernet 12
SW9(config-if-eth12)#switchport mode trunk
SW9(config-if-eth12)#switchport trunk allowed vlan 10,11,12
SW9(config-if-eth13)#interface Ethernet 13
SW9(config-if-eth13)#switchport access vlan 1001
SW9(config-if-eth13)#switchport
SW9(config-ET13)#exit
SW9(config-if-eth16)#interface Ethernet 16
SW9(config-if-eth16)#switchport access vlan 11
SW9(config-if-eth16)#switchport
SW9(config-ET16)#exit
SW9(config-if-eth20)#interface Ethernet 20
SW9(config-if-eth20)#switchport access vlan 12
```

SW9(config-if-eth20)#switchport
SW9(config-ET20)#exit
SW9(config-if-eth21)#interface Ethernet 21
SW9(config-if-eth2&)#switchport mode trunk
SW9(config-if-eth21)#switchport trunk allowed vlan 10,11,12
SW9(config-if-eth22)#interface Ethernet 22
SW9(config-if-eth22)#switchport access vlan 1001
SW9(config-if-eth22)#switchport
SW9(config-ET22)#exit
SW9(config)#interface Vlan10
SW9(config-vl10)#ip address 192.9.200.9/24
SW9(config-vl10)#vrrp 10 ipv4 192.9.200.8
SW9(config)#interface Vlan11
SW9(config-vl10)#ip address 192.9.201.9/24
SW9(config-vl10)#vrrp 11 ipv4 192.9.201.8
SW9(config)#exit
SW9(config)#interface Vlan12
SW9(config-vl10)#ip address 192.9.202.9/24
SW9(config-vl10)#vrrp 12 ipv4 192.9.202.8
SW9(config)#exit
SW9(config)#interface Vlan1001
SW9(config-vl10)#ip address 192.168.0.9/24
SW9(config-vl10)#vrrp 100 ipv4 192.168.0.8
SW9(config)#exit
SW9(config)#ip routing
SW9(config)#snmp-server local-interface Management1
SW9(config)#snmp-server view all-items iso included
SW9(config)#snmp-server group v3group v3 priv read all-items
SW9(config)#snmp-server user v3admin v3group v3 auth md5 v3adminpriv priv des v3adminpriv
SW13(config)#write

Pour SW10

These commands configure the port channels on SW10
localhost(config)#zerotouch cancel
localhost(config)#zerotouch disable
localhost(config)#conf t
localhost(config)#int management 1
localhost(config-if-Ma1)#
localhost(config-if-Ma1)#ip route 0.0.0.0 0.0.0.0 192.168.0.8
localhost(config)#hostname SW10
SW10(config)#username admin secret 0 tpreseau11

```
SW10(config)#end
SW10(config)#write
SW10(config)#reload
SW10(config-if-P01000)#interface Port-Channel 2
SW10(config-if-P01000)#switchport mode trunk
SW10(config-if-P01000)#switchport
SW10(config-if-P01000)#exit
SW10(config)# vlan 10
SW10(config)# vlan 11
SW10(config)# vlan 12
SW10(config)# vlan 1000
SW10(config-if-eth3)#interface Ethernet 3
SW10(config-if-eth3)#switchport
SW10(config-if-eth3)#channel-group 2 mode active
SW10(config-if-eth3)#exit
SW10(config-if-eth4)#interface Ethernet 4
SW10(config-if-eth4)#switchport
SW10(config-if-eth4)#channel-group 2 mode active
SW10(config-if-eth4)#exit
SW10(config-if-eth6)#interface Ethernet 6
SW10(config-if-eth6)#switchport
SW10(config-if-eth6)#switchport access vlan 10
SW10(config-if-eth6)#exit
SW10(config-if-eth12)#interface Ethernet 12
SW10(config-if-eth12)#switchport mode trunk
SW10(config-if-eth12)#switchport trunk allowed vlan 10,11,12
SW10(config-ET12)#exit
SW10(config-if-eth13)#interface Ethernet 13
SW10(config-if-eth13)#switchport access vlan 1001
SW10(config-if-eth13)#switchport
SW10(config-ET6)#exit
SW10(config-if-eth16)#interface Ethernet 16
SW10(config-if-eth16)#switchport access vlan 11
SW10(config-if-eth16)#switchport
SW10(config-ET16)#exit
SW10(config-if-eth20)#interface Ethernet 20
SW10(config-if-eth20)#switchport access vlan 12
SW10(config-if-eth20)#switchport
SW10(config-ET20)#exit
SW10(config-if-eth21)#interface Ethernet 21
SW10(config-if-eth21)#switchport mode trunk
```

SW10(config-if-eth21)#switchport trunk allowed vlan 10,11,12
SW10(config-ET6)#exit
SW10(config-if-eth22)#interface Ethernet 22
SW10(config-if-eth22)#switchport access vlan 1001
SW10(config-if-eth22)#switchport
SW10(config-ET6)#exit
SW10(config)#interface Vlan10
SW10(config-vl10)#ip address 192.9.200.10/24
SW10(config-vl10)#vrrp 10 ipv4 192.9.200.8
SW10(config)#exit
SW10(config)#interface Vlan11
SW10(config-vl10)#ip address 192.9.201.10/24
SW10(config-vl10)#vrrp 11 ipv4 192.9.201.8
SW10(config)#exit
SW10(config)#interface Vlan12
SW10(config-vl10)#ip address 192.9.202.10/24
SW10(config-vl10)#vrrp 12 ipv4 192.9.202.8
SW10(config)#exit
SW10(config)#interface Vlan1001
SW10(config-vl10)#ip address 192.168.0.10/24
SW10(config-vl10)#vrrp 100 ipv4 192.168.0.8
SW10(config)#exit
SW10(config)#ip routing
SW10(config)#snmp-server local-interface Management1
SW10(config)#snmp-server view all-items iso included
SW10(config)#snmp-server group v3group v3 priv read all-items
SW10(config)#snmp-server user v3admin v3group v3 auth md5 v3adminpriv priv des v3adminpriv
SW10(config)#write

Pour SW3

configure snmp sysName SW3
configure vlan default delete port all
create vlan VLAN1
configure vlan VLAN1 tag 10
configure vlan VLAN1 add port 2 untagged
create vlan VLAN2
configure vlan VLAN2 tag 11
configure vlan VLAN2 add port 7 untagged
create vlan VLAN3
configure vlan VLAN3 tag 12
configure vlan VLAN3 add port 8 untagged
create vlan ADMIN

```
configure vlan  ADMIN tag 1001
configure vlan ADMIN add port 4,6 tagged
configure vlan VLAN2 add port 4,6 tagged
configure vlan VLAN1 add port 4,6 tagged
configure vlan VLAN3 add port 4,6 tagged
configure vlan VLAN1 ipaddress 192.9.200.3 255.255.255.0
enable ipforwarding vlan VLAN1
configure vlan VLAN2 ipaddress 192.9.201.3 255.255.255.0
enable ipforwarding vlan VLAN2
configure vlan VLAN3 ipaddress 192.9.202.3 255.255.255.0
enable ipforwarding vlan VLAN3
configure vlan ADMIN ipaddress 192.168.0.3 255.255.255.0
enable ipforwarding vlan ADMIN
configure stpd s0 delete vlan default ports all
create stpd s10
configure stpd s10 mode dot1w
configure stpd s10 default-encapsulation pvst-plus
configure stpd s10 add vlan VLAN1 ports 6 pvst-plus
configure stpd s10 add vlan VLAN1 ports 4 pvst-plus
configure stpd s10 ports mode pvst-plus 6
configure stpd s10 ports mode pvst-plus 4
configure stpd s10 tag 10
enable stpd s10
create stpd s11
configure stpd s11 mode dot1w
configure stpd s11 default-encapsulation pvst-plus
configure stpd s11 add vlan VLAN2 ports 6 pvst-plus
configure stpd s11 add vlan VLAN2 ports 4 pvst-plus
configure stpd s11 ports mode pvst-plus 6
configure stpd s11 ports mode pvst-plus 4
configure stpd s11 tag 11
enable stpd s11
create stpd s12
configure stpd s12 mode dot1w
configure stpd s12 default-encapsulation pvst-plus
configure stpd s12 add vlan VLAN3 ports 6 pvst-plus
configure stpd s12 add vlan VLAN3 ports 4 pvst-plus
configure stpd s12 ports mode pvst-plus 6
configure stpd s12 ports mode pvst-plus 4
configure stpd s12 tag 12
enable stpd s12
```

create stpd s1001
configure stpd s1001 mode dot1w
configure stpd s1001 default-encapsulation pvst-plus
configure stpd s1001 add vlan ADMIN ports 6 pvst-plus
configure stpd s1001 add vlan ADMIN ports 4 pvst-plus
configure stpd s1001 ports mode pvst-plus 6
configure stpd s1001 ports mode pvst-plus 4
configure stpd s1001 tag 1001
enable stpd s1001
create vrrp vlan VLAN1 vrid 10
create vrrp vlan VLAN2 vrid 11
create vrrp vlan VLAN3 vrid 12
create vrrp vlan ADMIN vrid 100
configure vrrp vlan VLAN1 vrid 10 add 192.9.200.8
configure vrrp vlan VLAN2 vrid 11 add 192.9.201.8
configure vrrp vlan VLAN3 vrid 12 add 192.9.202.8
configure vrrp vlan ADMIN vrid 100 add 192.168.0.8
enable vrrp vlan VLAN1 vrid 10
enable vrrp vlan VLAN2 vrid 11
enable vrrp vlan VLAN3 vrid 12
enable vrrp vlan ADMIN vrid 100
configure vrrp vlan vlan1 vrid 10 version v3-v2
configure vrrp vlan vlan2 vrid 11 version v3-v2
configure vrrp vlan vlan3 vrid 12 version v3-v2
configure vrrp vlan admin vrid 100 version v3-v2
configure vrrp vlan vlan1 vrid 10 priority 150
save config

Pour SW4

configure snmp sysName SW4
configure vlan default delete port all
create vlan VLAN1
configure vlan VLAN1 tag 10
configure vlan VLAN1 add port 2 untagged
create vlan VLAN2
configure vlan VLAN2 tag 11
configure vlan VLAN2 add port 7 untagged
create vlan VLAN3
configure vlan VLAN3 tag 12
configure vlan VLAN3 add port 8 untagged
create vlan ADMIN

```
configure vlan  ADMIN tag 1001
configure vlan ADMIN add port 4,6 tagged
configure vlan VLAN2 add port 4,6 tagged
configure vlan VLAN1 add port 4,6 tagged
configure vlan VLAN3 add port 4,6 tagged
configure vlan VLAN1 ipaddress 192.9.200.4 255.255.255.0
enable ipforwarding vlan VLAN1
configure vlan VLAN2 ipaddress 192.9.201.4 255.255.255.0
enable ipforwarding vlan VLAN2
configure vlan VLAN3 ipaddress 192.9.202.4 255.255.255.0
enable ipforwarding vlan VLAN3
configure vlan ADMIN ipaddress 192.168.0.4 255.255.255.0
enable ipforwarding vlan ADMIN
configure stpd s0 delete vlan default ports all
create stpd s10
configure stpd s10 mode dot1w
configure stpd s10 default-encapsulation pvst-plus
configure stpd s10 add vlan VLAN1 ports 6 pvst-plus
configure stpd s10 add vlan VLAN1 ports 4 pvst-plus
configure stpd s10 ports mode pvst-plus 6
configure stpd s10 ports mode pvst-plus 4
configure stpd s10 tag 10
enable stpd s10
create stpd s11
configure stpd s11 mode dot1w
configure stpd s11 default-encapsulation pvst-plus
configure stpd s11 add vlan VLAN2 ports 6 pvst-plus
configure stpd s11 add vlan VLAN2 ports 4 pvst-plus
configure stpd s11 ports mode pvst-plus 6
configure stpd s11 ports mode pvst-plus 4
configure stpd s11 tag 11
enable stpd s11
create stpd s12
configure stpd s12 mode dot1w
configure stpd s12 default-encapsulation pvst-plus
configure stpd s12 add vlan VLAN3 ports 6 pvst-plus
configure stpd s12 add vlan VLAN3 ports 4 pvst-plus
configure stpd s12 ports mode pvst-plus 6
configure stpd s12 ports mode pvst-plus 4
configure stpd s12 tag 12
enable stpd s12
```

create stpd s1001
configure stpd s1001 mode dot1w
configure stpd s1001 default-encapsulation pvst-plus
configure stpd s1001 add vlan ADMIN ports 6 pvst-plus
configure stpd s1001 add vlan ADMIN ports 4 pvst-plus
configure stpd s1001 ports mode pvst-plus 6
configure stpd s1001 ports mode pvst-plus 4
configure stpd s1001 tag 1001
enable stpd s1001
create vrrp vlan VLAN1 vrid 10
create vrrp vlan VLAN2 vrid 11
create vrrp vlan VLAN3 vrid 12
create vrrp vlan ADMIN vrid 100
configure vrrp vlan VLAN1 vrid 10 add 192.9.200.8
configure vrrp vlan VLAN2 vrid 11 add 192.9.201.8
configure vrrp vlan VLAN3 vrid 12 add 192.9.202.8
configure vrrp vlan ADMIN vrid 100 add 192.168.0.8
enable vrrp vlan VLAN1 vrid 10
enable vrrp vlan VLAN2 vrid 11
enable vrrp vlan VLAN3 vrid 12
enable vrrp vlan ADMIN vrid 100
configure vrrp vlan vlan1 vrid 10 version v3-v2
configure vrrp vlan vlan2 vrid 11 version v3-v2
configure vrrp vlan vlan3 vrid 12 version v3-v2
configure vrrp vlan admin vrid 100 version v3-v2
save config

VRRP Attention au VRID de 100 pour l'admin incompatible avec les extrems à modifier
Modifier les numéros de vrid pour extreme 1 en 10 2 en 11 3 en 12 1001 en 100
Attention à la compatibilité v3-v2
A voir pour l'adresse du port de management le serveur SNMP peut il être joint sur les VLANS ?
Virtual Router Identifier (VRID). Values range from ***1 to 255***.

- **<u>Sécurisation de l'accès du switch à distance</u> :**

Pour cela, il faut créer un access-list. II faut créer une règle et l'appliquer à une interface.

- <u>Création de la règle</u> :
  - SwitchX#**conf t**
  - SwitchX(config)#**ip access-list standard** « *numéro de la règle de l à 99>>*
  - SwitchX(config-std-nacl)#**permit host** « *@IP du poste qui peul administrer à distance »*
  - SwitchX(config-std-nacl)#**deny any**
  - SwitchX(config-std-nacl)#**exit**

  <u>Application de la règle à une interface</u> :

  - SwitchX(config)#**int** vlan 1
  - SwitchX(config-if)#**ip access-group** « *numéro de la règle n>>*

  Pour supprimer cet access-list, il faut taper les lignes de commandes suivantes : SwitchX(config)#**no ip access-list standard** « *numéro de la règle n>>*

  SwitchX(config-it)#**no ip access-group** « *numéro de la règle>>* in

- **Les commandes CISCO pour l'agrégation de liens**

conf t (sur le premier switche en mode actif)
Switch#conf t
Switch(config)#port-channel load-balance src-mac
Switch(config)#int gi0/1
Switch(config-if)#channel-protocol lacp
Switch(config-if)#channel-group 1 mode active
Switch(config)#int gi0/2
Switch(config-if)#channel-protocol lacp
Switch(config-if)#channel-group 2 mode active

Switch#conf t (sur le deuxième switche en mode passif)
Switch(config)#port-channel load-balance src-mac
Switch(config)#int gi0/1
Switch(config-if)#channel-protocol lacp
Switch(config-if)#channel-group 1 mode passive
Switch(config)#int gi0/2
Switch(config-if)#channel-protocol lacp
Switch(config-if)#channel-group 2 mode passive