Comment faire des VLANs et un routage inter-VLANs ?

* Créé [28 février 2018](https://labo-tech.fr/base-de-connaissance/comment-faire-des-vlans-et-un-routage-inter-vlans/)
* Autheur [Mickael Asseline](https://labo-tech.fr/author/papamica/)
* Catégorie [Cisco Packet Tracer](https://labo-tech.fr/article-categories/cisco-packet-tracer/)

VLANs et routage inter-VLANs

Présentation :

mise en place un réseau simple composé de :  
 4 postes de travail,   
 deux switchs et   
 un routeur.

Les deux switchs partageront des VLANS et le routeur se chargera des tâches de routage inter-VLANs.

Nous aborderons divers fonction et manipulation sous des éléments de marques Cisco. Ainsi, nous régulerons plus facilement le flux

Intérêt des vlan :   
Segmenter le réseau physique en réseau logique plus petit et facilement manageables  
bloquer les adresses de diffusions optimiser la bande passante  
créer des espaces de travail indépendants et   
Accroite la sécurité en isolant les flux réseau

Schéma du réseau

Pour illustrer le tutoriel, j’utiliserais ce schéma fait sous Packet Tracer :

[Une image contenant diagramme, ligne, capture d’écran

Description générée automatiquement](https://i2.wp.com/labo-tech.fr/wp-content/uploads/2018/02/RoutageInterVLAN01-550x271.png)

Configuration des VLANs

La première étape à suivre une fois que le cablage est en place est de créer les deux VLANS sur nos deux switchs. Pour faire simple, nous allons supposer que nous aurons deux VLANS (10 et 20) avec une liaison par port trunk entre le switch 2 et le switch 3. Le reste de la configuration sera détaillée et expliquée plus tard.

Note : A faire sur les deux Switchs

//Passer en mode configuration :

Switch>enable

Switch#conf t

//Création des VLANs : 10, 20 et 99

Switch(config)#vlan 10

Switch(config-vlan)#name vlan\_10

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name vlan\_20

Switch(config-vlan)#vlan 99

Switch(config-vlan)#name Native

Switch(config-vlan)#exit

Nous créons également un VLAN natif dont l’explication sera faite un peu plus bas dans le tutoriel.

Nous allons maintenant **créer nos ports trunk sur les interfaces Fa0/1 de nos deux switchs.**

Le port trunk va permettre, au travers des trames 802.1q de faire transiter des trames tagguées (ou étiquetées) selon un Vlan ou un autre afin que tous les Vlan autorisés puissent passer au travers d’un même lien. Plus clairement, c’est un port qui peut faire passer plusieurs VLAN vers un autre élément actif.

Cela permet, dans notre cas, de faire communiquer les VLANS 10 et 20 entres des éléments connectés à deux switchs différents. Sans port trunk, il faudrait une liaison entre les switchs par VLANs.

**créer nos ports trunk sur les interfaces Fa0/1 de nos deux switchs**

//Création des ports trunk

Switch(config)#interface fa0/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 20,30,99

Switch(config-if)# switchport trunk native vlan 99

Switch(config-if)#no shutdown

Switch(config-if)#exit

Faisons un petit point sur le terme « native vlan »sur ce lien : vlan natif

Par défaut, un trunk laisse passer tous les VLANs.

Une bonne pratique est de **décrire explicitement les VLANs permis**.

Par exemple :

switchport trunk allowed vlan 10, 20-29

**bonnes pratiques du VLAN**

Une bonne pratique est de **décrire explicitement les VLANs permis**. Par exemple :

switchport trunk allowed vlan 10, 20-29

En plus, un trunk laisse passer les trames Ethernet natives (sans étiquette de VLAN).   
Le switch place ces trames dans un VLAN spécial, c’est le VLAN natif de l’interface.

Par défaut, le VLAN natif est le VLAN 1 : les trames natives vont dans le VLAN 1.   
Et le VLAN 1 est toujours actif.

En général, quand il y a une interface trunk, c’est pour échanger des trames avec une étiquette de VLAN.

**Dès lors, les trames sans étiquettes de VLAN doivent être écartées**. Pour cela, il suffit de spécifier, pour chaque trunk, un VLAN natif exclusif. Quoi qu’il en soit, sur un trunk, il faut toujours **spécifier le VLAN natif**.

En plus, un trunk laisse passer les trames Ethernet natives (sans étiquette de VLAN).   
Le switch place ces trames dans un VLAN spécial, c’est le VLAN natif de l’interface.

Bien sûr, **il ne faut jamais utiliser le VLAN 1 pour véhiculer le trafic de données**. En effet, ce VLAN est utilisé par de nombreux protocoles de niveau 2.

Ah, j’allais oublier aussi ISL. Il s’agit d’un protocole propriétaire créé avant que les étiquettes de VLAN ne soient normalisées. A n’utiliser qu’en présence d’équipements CISCO obsolètes, qui gèrent uniquement ISL. Certains équipements récents ne gèrent plus ISL.

**en résumé, un trunk bien propre du point de vue des VLAN donne :**

* switchport trunk encapsulation dot1q
* switchport trunk native vlan 801
* switchport trunk allowed vlan 10,20-29
* switchport mode trunk
* switchport nonegotiate

Vos remarques, questions et autres interventions sont les bienvenues.

Pascal BONNARD

Le vlan natif est le vlan qui n’est pas balisé avec un ID de vlan sur une jonction 802.1q. Tous les autres vlan traversant le trunk sont marqués avec un ID de vlan.

L’utilisation de la commande trunk allowed vous permet de spécifier exactement quels vlan sont autorisés sur la liaison trunk, s’ils ne sont pas dans la liste, le trafic vlan ne passera pas par le lien. un trunk est une liaison ayant pour but de véhiculer le trafic de plusieurs vlans.

HTH (en anglais seulement)

On spécifie les VLANS que nous souhaitons laisser passer sur notre trunk à savoir les trames étiquetées sur les VLAN 20,30 et 99. Par défaut, toutes les VLANS peuvent passer sur un port trunk. Si nous spécifions l’autorisation de certaines VLANs, les autres ne seront pas acceptés à transiter.

[Le vlan natif est le vlan qui n’est pas balisé avec un ID de vlan sur une jonction 802.1q. Tous les autres vlan traversant le trunk sont marqués avec un ID de vlan.](https://www.bing.com/ck/a?!&&p=66ac5af89131ebc6JmltdHM9MTcwODY0NjQwMCZpZ3VpZD0wYTM2ODllMy05ZWZjLTY4YmQtM2Q1ZS05ZGY2OWZmYTY5ODYmaW5zaWQ9NTAxMg&ptn=3&ver=2&hsh=3&fclid=0a3689e3-9efc-68bd-3d5e-9df69ffa6986&u=a1aHR0cHM6Ly9jb21tdW5pdHkuY2lzY28uY29tL3Q1L3N3aXRjaGluZy90cnVuay1hbGxvd2VkLXZsYW4tdnMtbmF0aXZlLXZsYW4vdGQtcC83MzMwNzUjOn46dGV4dD1UaGUlMjBuYXRpdmUlMjB2bGFuJTIwaXMlMjB0aGUlMjB2bGFuLGFyZSUyMHRhZ2dlZCUyMHdpdGglMjBhJTIwdmxhbiUyMElELiZ0ZXh0PVRoZSUyMG5hdGl2ZSUyMHZsYW4lMjBpcyx3aXRoJTIwYSUyMHZsYW4lMjBJRC4mdGV4dD12bGFuJTIwaXMlMjB0aGUlMjB2bGFuLGFyZSUyMHRhZ2dlZCUyMHdpdGglMjBh&ntb=1" \t "_blank)

**Nous allons maintenant affecter les ports voulus à nos différentes VLANS.**

On présume que nous souhaitons affecter les ports Fa0/10 des deux switchs sur la VLAN 20 et les ports Fa0/11 sur le VLAN 30, on exécute donc ces commandes sur nos deux switchs :

//Affectation des ports au VLANs :

Switch(config)#interface fa0/10

Switch(config-if)#switchport access vlan 20

Switch(config-if)#no shutdown

Switch(config-if)#exit

Switch(config)#interface fa0/11

Switch(config-if)#switchport access vlan 30

Switch(config-if)#no shutdown

Switch(config-if)#exit

* Re-play
* Copy to Clipboard
* Pause
* Full View

Voici à présent le schéma de notre réseau, j’ai juste ajouté des détails sur les postes pour savoir sur quel VLAN ils sont :

[Une image contenant diagramme, ligne, capture d’écran, texte

Description générée automatiquement](https://i2.wp.com/labo-tech.fr/wp-content/uploads/2018/02/RoutageInterVLAN02-550x242.png)

J’ai également ajouté des IPs à mes postes. Ceux sur la VLAN 20 appartient au réseau « **192.168.20.0/24** » et ceux sur le VLAN 30 appartiennent au réseau « **192.168.30.0/24** » (pour faire simple  ).

Test des VLANs

Nous allons maintenant tester la connectivité des postes situées sur la même VLAN. On prend pas exemple le poste « Laptop2 » sur le VLAN 30 et avec l’IP 192.168.30.2 pour pinger le poste « Laptop1 » située sur la VLAN 30 de l’autre switch et avec l’IP 192.168.30.1 :

[Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement](https://i1.wp.com/labo-tech.fr/wp-content/uploads/2018/02/RoutageInterVLAN03-550x248.png)

On peut faire la même chose en pingant du poste « PC1 » au poste « PC2 » qui sont également tout deux sur le même VLAN(20 cette fois ci). Les plus curieux aurons remarqué que le « PC1 » ou « PC2 » ne peuvent pinger « Laptop1 » et « Laptop2 » qui sont sur des VLANS différentes (20 et 30). C’est justement la problématique que nous venons de nous créer est que les VLANS isolent correctement les groupes de postes/d’utilisateur mais bloquent complétement la communication entres elles.

**Pourquoi ?**

Les VLANs sont des LAN virtuelle (d’où leur nom  ) et comme chaque LAN, nous ne pouvons les interconnectés que par l’intermédiaire de routeur (d’élément gérant la couche 3 – réseau plus spécifiquement). Nous avons maintenant besoin de router nos différentes VLANS entre elles pour qu’elles puissent communiquer. Nous abordons donc la deuxième partie du tutoriel qui est donc le routage inter-vlan.

Routage inter-VLAN

Il se peut qu’un besoin de communication se fasse entre les deux groupes de travail. Il est alors possible de faire communiquer deux Vlans sans pour autant compromettre leur sécurité.

Pour cela nous utilisons un routeur relié à un des deux switchs. Nous appelons ce type de routage inter-vlan un Router-on-stick. Cela signifie que le router va, par intermédiaire d’un seul lien physique router et faire transiter un ensemble de VLAN. On aurait également pu mettre en place un switch de niveau trois qui aurai été capable d’effectuer les tâches de routage inter-vlan.

Plusieurs Vlans peuvent avoir pour passerelle un même port physique du routeur qui sera « découpé » en plusieurs interfaces virtuelles. Nous pouvons en effet diviser un port du routeur selon les Vlans à router et ainsi créer une multitude de passerelles virtuelles avec des adresses IP différentes.

Configuration du routeur

Nous allons donc créer nos interface virtuelles sur le port Fa0/0 de notre routeur. Il faut tout d’abord absolument activer l’interface physique pour que les interfaces virtuelles soient opérationnelles :

//Activation de l’interface physique :

Router>enable

Router#configuration terminal

Router(config)#interface fa0/0

Router(config-if)#no shutdown

Router(config-if)#exit

* Re-play
* Copy to Clipboard
* Pause
* Full View

Nous allons ensuite créer l’interface **fa0/0.1** (interface virtuelle 1 de l’interface physique fa0/0),nous dirons que ce port virtuel sur la passerelle des postes du VLAN 20 :

//Création de l’interface virtuelle fa0/01 pour le VLAN 20 :

Router(config)#interface fa0/0.1

Router(config-subif)#encapsulation dot1Q 20

Router(config-subif)#ip address 192.168.20.254 255.255.255.0

Router(config-subif)#no shutdown

Router(config-subif)#exit

* Re-play
* Copy to Clipboard
* Pause
* Full View

Nous faisons pareil pour l’interface fa0/0.2 et les postes du réseau du vlan 30

//Création de l’interface virtuelle fa0/0.2 pour le VLAN 30 :

Router(config)#interface fa0/0.2

Router(config-subif)#encapsulation dot1Q 30

Router(config-subif)#ip address 192.168.30.254 255.255.255.0

Router(config-subif)#no shutdown

Router(config-subif)#exit

* Re-play
* Copy to Clipboard
* Pause
* Full View

Un petit mot de la commande **« encapsulation dot1q ».** La norme de trame **802.1q** indique que les trames sont étiquetées pour contenir le numéro de vlan à laquelle elles sont destinées/attribuées. La commande « **encapsulation dot1q 30** » permet donc d’encapsuler une trame pour transiter sur le vlan 30 si elle est destinée à celui ci. Le routeur a besoin de cette information par exemple quand il voit une trame venant du vlan 20 (étiquetée vlan 20) qui souhaite se diriger sur le vlan 30. Il change donc à ce moment la son étiquetage 802.1q pour que les switchs puissent correctement acheminé la trame vers le ou les postes du vlan 30. N’oublions pas notre switch ! Il faut également mettre le port **fa0/24** de notre **« Switch2 »** (qui fait la liaison avec le routeur) en mode trunk pour que lui aussi puisse acheminer toutes les VLANs vers et depuis le routeur :

//Passage du port fa0.24 en mode trunk :

Switch(config)#interface fa0/24

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 20,30,99

Switch(config-if)# switchport trunk native vlan 99

Switch(config-if)#no shutdown

Switch(config-if)#exit

* Re-play
* Copy to Clipboard
* Pause
* Full View

Test du routage VLAN

Une fois que nous avons mis les bonnes passerelles à nos postes (par exemple 192.168.20.254 pour les postes du VLAN 20 dans le cas de notre schéma de test), nous pouvons tester la communication inter-VLAN par l’intermédiaire d’un simple ping par exemple du poste 192.168.20.2 vers 192.168.30.1

[Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement](https://i0.wp.com/labo-tech.fr/wp-content/uploads/2018/02/RoutageInterVLAN04-550x299.png)

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

vlan 10

Description Market

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

**Exemple de configuration de l’affectation VLAN basée sur l’interface (statiquement Type de lien configuré)**

**Configuration requise pour la mise en réseau**

Comme le montre [la figure 5-24](https://support.huawei.com/enterprise/en/doc/EDOC1000178168/d6b7bdf/example-for-configuring-interface-based-vlan-assignment-statically-configured-link-type#fig_dc_cfg_vlan_004601), de multiples Les terminaux utilisateur sont connectés aux commutateurs d’une entreprise. Les utilisateurs qui utilisent le même service accèdent à l’entreprise réseau à l’aide de différents appareils.

Pour s’assurer que la sécurité des communications et éviter les tempêtes de diffusion, l’entreprise permet aux utilisateurs qui utilisent le même service de communiquer avec et d’isoler les utilisateurs qui utilisent des services différents.

Configurer attributions VLAN basées sur l’interface sur le commutateur et ajouter des interfaces connectées aux terminaux des utilisateurs qui utilisent le même service vers le même VLAN. Les utilisateurs de différents VLAN communiquent à l’adresse suivante : Couche 2, et les utilisateurs du même VLAN peuvent communiquer directement.

**Graphique 5-24** Mise en réseau de l’affectation VLAN basée sur l’interface

**Graphique 5-24** Mise en réseau de l’affectation VLAN basée sur l’interface  
Une image contenant texte, capture d’écran, diagramme, ligne

Description générée automatiquement

**Feuille de route de configuration**

La configuration La feuille de route est la suivante :

1. Créer des VLAN et ajouter des interfaces se connectant aux terminaux des utilisateurs aux VLAN pour isoler le trafic de couche 2 entre les utilisateurs qui utilisent des services.
2. Configurer le type de liaison entre SwitchA et SwitchB et VLAN pour permettre aux utilisateurs qui utilisent le même service pour communiquer.

Exécutez la commande vlan batch dans la vue système pour créer des VLAN dans un lot.  
  
Créez 10 VLAN contigus : VLAN 11 à VLAN 20.  
<HUAWEI> system view  
[HUAWEI] vlan batch 11 à 20

Par exemple, la commande vlan batch 10 15 à 19 25 28 to 30 crée quatre plages VLAN non contiguës.

Vous pouvez créer un maximum de **10 VLANs contigus** ou de 10 plages de VLAN non contiguës.en une seule fois.

Vous pouvez créer un maximum de 10 VLAN contigus ou plages de VLAN non contigus à la fois. S’il y a plus de 10 VLAN, exécutez cette commande plusieurs fois.

Par exemple, la commande vlan batch 11 to 20 crée **10 VLANs contigus** allant de **VLAN 11 à VLAN 20**. [Si vous avez plus de 10 VLANs, vous pouvez exécuter cette commande plusieurs fois1](https://support.huawei.com/enterprise/en/knowledge/EKB1000379480).

**Procédure**

1. Créez le VLAN 2 et le VLAN 3 sur le commutateur A, et ajouter des interfaces connectées à des terminaux utilisateurs à différents VLAN. Le configuration du commutateur B est similaire à celle du commutateur A et n’est pas mentionné ici.