Configuration des VLANs sous Cisco IOS

Ce chapitre a pour objectif d'exposer les commandes de configuration des VLANs en Cisco IOS, la configuration du protocole DTP (Dynamic Trunking Protocol) et VTP (VLAN Trunking Protocol) ainsi que les bonnes pratiques associées.

Téléchargez le PDF du guide CCNA 200-301 (https://leanpub.com/b/cisco-ccna-200-301)

Crédit photo: https://flic.kr/p/FTS1q3 (https://flic.kr/p/FTS1q3)

Objectifs de certification

CCNA 200-301

- 2.1 Configurer et vérifier les VLANs (normal range) couvrant plusieurs switches
  - 2.1.a Access ports (data et voice)
  - 2.1.b Default VLAN
  - 2.1.c Connectivity
- 2.2 Configurer et vérifier la connectivité interswitch
  - 2.2.a Trunk ports
  - 2.2.b 802.1Q
  - 2.2.c Native VLAN

Configuration des VLANs sous Cisco IOS®

Ce chapitre a pour objectif d'exposer les commandes de configuration des VLANs en Cisco IOS, la configuration du protocole DTP (Dynamic Trunking Protocol) et VTP (VLAN Trunking Protocol) ainsi que les bonnes pratiques associées.

1. VLAN et paramètres switchport par défaut

Par défaut, un port physique d'un commutateur Cisco est un "switchport", un port de commutation.

Il est configuré par défaut dans le mode "dynamic auto" mais il est en mode opérationnel "access". Il est associé au VLAN 1 (default).

S'il devait être monté trunk, le VLAN natif serait le VLAN 1 et l'encapsulation "Trunk" serait négociée par DTP.

Un port dynamique est un port qui restera un port "access" ou qui se montera en port "trunk" en fonction des messages Dynamic Trunk Protocol (DTP, protocole propriétaire Cisco) reçus par l'interface.

```
#show interfaces Fa0/21 switchport
Name: Fa0/21
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
...
```

2. Création des VLANs et des interfaces SVI

2.1. Création des VLANs

Les VLANs doivent d'abord être créés sur chaque commutateur. Par exemple, pour le VLAN 10 et pour chaque VLAN, en mode de configuration globale :

```
(config)#vlan 10
(config-vlan)#name TEST
(config-vlan)#exit
(config)#
```

Vérification

```
#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   TEST                             active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```


2.2. Suppression d'un VLAN

```
(config)#no vlan 10
(config-vlan)#exit
```

2.3. L'interface VLANx de gestion (SVI)

L'interface VLANx de gestion (SVI) correspond aux interfaces physiques appartenant à ce VLAN (le numéro 10 dans l'exemple) pour le joindre en IPv4 à des fins de gestion (en Telnet, SSH, HTTP ou SNMP). Comme tout périphérique joignable sur le réseau, le commutateur doit posséder une adresse IPv4, un masque et une passerelle.

```
(config)#interface vlan 10
(config-if)#ip address 192.168.10.1 255.255.255.0
(config-if)#no shutdown
(config-if)#exit
(config)#ip default-gateway 192.168.10.254
```

Si le VLAN qui correspond à l'interface créée a déjà été instancié (voir juste avant), l'interface se monte et le commutateur nous le dit avec un message de log :

```
%LINK-5-CHANGED: Interface Vlan10, changed state to up
```

Vérification :

```
#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
...
Vlan1                  unassigned      YES manual administratively down down
Vlan10                 192.168.10.1    YES manual up                    down
```

Mais la colonne "Protocol" reste "down" ce qui signifie un problème de couche 2 (L2).

3. Configuration et vérification des port "Access"

3.1. Configuration des ports "Access"

Sous Cisco IOS un port Access est un port qui appartient à un seul VLAN. En option, on peut activer "spanning-tree portfast" qui fait passer le port directement à l'état STP "forwarding" vu qu'il connectera des périphériques de terminaison (qui ne créent pas de boucles).

```
(config)#interface range f0/1 - 20
(config-if-range)#switchport mode access
(config-if-range)#switchport access vlan 10
(config-if-range)#spanning-tree portfast
(config-if-range)#exit
```

Dès que des ports sont configurés dans le VLAN 10, l'interface Vlan 10 se monte en "Protocol up" :

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
```

Vérification :

```
#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
...
Vlan1                  unassigned      YES manual administratively down down
Vlan10                 192.168.10.1    YES manual up                    up
```


3.2. Vérification des ports “Access”

Vérification du VLAN associé à un port “access”

```
#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   TEST                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
...
```

4. Configuration et vérification des ports “Trunk”

4.1. Configuration d’un port “Trunk”

Un port dit “Trunk” est un port qui transporte le trafic appartenant à plusieurs VLANs, tous par défaut sur du matériel Cisco.

```
(config)#int G0/1
(config-if)#switchport mode trunk
(config-if)#exit
```

4.2. Vérification d’un port “Trunk”

```
#show interfaces G0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none


#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10
```

Dans cette sortie fournie par la commande `show interfaces trunk`, on prendra connaissance du mode DTP de l'interface ("on", "dynamic auto", "desirable", "nonegociate"), du protocole d'encapsulation ("802.1q" ou "isl"), le statut et le numéro du VLAN natif sur le Trunk.

4.3. Encapsulation sur le port "trunk"

```
(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk"
mode.


(config-if)#switchport trunk encapsulation ?
  dot1q      Interface uses only 802.1q trunking encapsulation when trunking
  isl        Interface uses only ISL trunking encapsulation when trunking
  negotiate  Device will negotiate trunking encapsulation with peer on
             interface


(config-if)#switchport trunk encapsulation dot1q
(config-if)#switchport mode trunk


(config-if)#do show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1
```


4.4. Rétablir la négociation de l'encapsulation sur le "trunk"

Pour rétablir la négociation de l'encapsulation (via DTP) :

```
(config-if)#switchport trunk encapsulation negotiate
Command rejected: A port which is configured to "trunk" mode can not be configured to negotiate the
encapsulation.


(config-if)#no switchport mode trunk
(config-if)#switchport trunk encapsulation negotiate
```

4.5. Autoriser certains VLANs sur le port "trunk"

Pour autoriser certains VLANs sur le port “trunk” :

```
(config)#int G0/1
(config-if)#switchport trunk allowed vlan 10, 20
```

Pour ne pas placer d’étiquette 802.1q sur un VLAN (VLAN natif) :

```
(config-if)#switchport trunk native vlan 100
(config-if)#exit
```

5. Routage Inter-VLAN

5.1. Configuration du Trunk sur le routeur (Router-on-A-Stick)

Pour que différents VLANs communiquent entre eux, le routage est nécessaire. Le routage peut être assuré par un routeur ou un commutateur de niveau 3. Ici la configuration sur un routeur (configuration Router-on-A-Stick).

```
(config)#interface G0/0
(config-if)#no ip address
(config-if)#no shut
(config-if)#interface G0/0.1
(config-subif)#encapsulation dot1q 10
(config-subif)#ip address 192.168.10.254 255.255.255.0
(config-subif)#exit
(config)#...
(config)#interface G0/0.4
(config-subif)#encapsulation dot1q 100 native
(config-subif)#exit
```

5.2. Routage avec un commutateur L3

Vérifier que votre commutateur est capable de remplir des tâches de routage.

Activer le routage IPv4 :

```
(config)#ip routing
```

Créer les VLANs et les ports Trunks vers les commutateurs d’accès.

Pour chaque VLAN à router, création d’une interface VLAN.

Éventuellement, activation d'un protocole de routage

6. Dynamic Trunking Protocol (DTP)

6.1. Dynamic Trunking Protocol (DTP)

Dynamic Trunking Protocol (DTP) est un protocole propriétaire Cisco (activé par défaut sur les ports des commutateurs Cisco) qui négocie aussi bien :

- le statut des ports "trunk" ou "access"
- l'encapsulation des ports "trunk"

DTP gère la négociation "trunk" seulement si le port sur l'autre commutateur est configuré dans un mode trunk supporté par DTP.

6.2. DTP mode "dynamic auto"

Par défaut, tous les ports du commutateur sont configurés en `switchport mode dynamic auto` ; le commutateur local annonce qu'il est capable de se monter en trunk mais ne demande pas à son correspondant de passer en mode trunk. Après la négociation DTP, le port local termine en mode trunk uniquement si le port correspondant est "on" (trunk) ou "desirable". Si le port correspondant est en "auto" ou "access", la négociation aboutit localement en mode "access".

6.3. DTP mode "on"

Si le port du commutateur est configuré en `switchport mode trunk` , il est en mode DTP "on", le port du commutateur envoie régulièrement des messages DTP selon lesquels il est inconditionnellement en mode "trunk"

6.4. DTP mode "auto desirable"

Si le commutateur est configuré en `switchport dynamic desirable` , le commutateur local annonce qu'il est capable de se monter en trunk et demande à son correspondant de passer en mode "trunk". Après la négociation DTP, le port local termine en mode "trunk" si le port correspondant est "on" (trunk) ou "desirable" ou "auto". Si le port correspondant est en "access", la négociation aboutit localement en mode "access". Si le port distant est en mode "non-negociate", le port local reste en mode "access".

6.5. DTP mode "nonegociate"

Si le commutateur est en `switchport nonegotiate`, le port local reste inconditionnellement en mode trunk. Il n'y a aucune négociation. On utilise cette commande pour intégrer au trunking des commutateurs d'autres constructeurs.

6.6. Désactiver DTP sur un port

Configurer administrativement un port en `switchport mode access` désactive DTP sur le port.

6.7. DTP tableau récapitulatif

-	Dynamic auto	Dynamic desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	-
Access	Access	Access	-	Access

6.8 Modes DTP et commandes associées

Mode DTP	Commande (config-if)#
On	`switchport mode trunk`
Desirable	`switchport mode dynamic desirable`
Auto	`switchport mode dynamic auto`
Nonegotiate	`switchport mode nonegotiate`
Off	`no switchport mode trunk` ou `switchport mode access`

7. Virtual Trunking Protocol (VTP)

7.1. Virtual Trunking Protocol

VTP (Virtual Trunking Protocol) est un protocole propriétaire Cisco servant à maintenir la base de données de VLANs sur plusieurs commutateurs de manière cohérente.

Tout au plus VTP va-t-il ajouter, modifier ou supprimer des ID VLAN et leurs noms de manière cohérente à travers une infrastructure constituée de commutateurs.

VTP ne permettra en aucun cas de configurer les ports de manière centralisée !

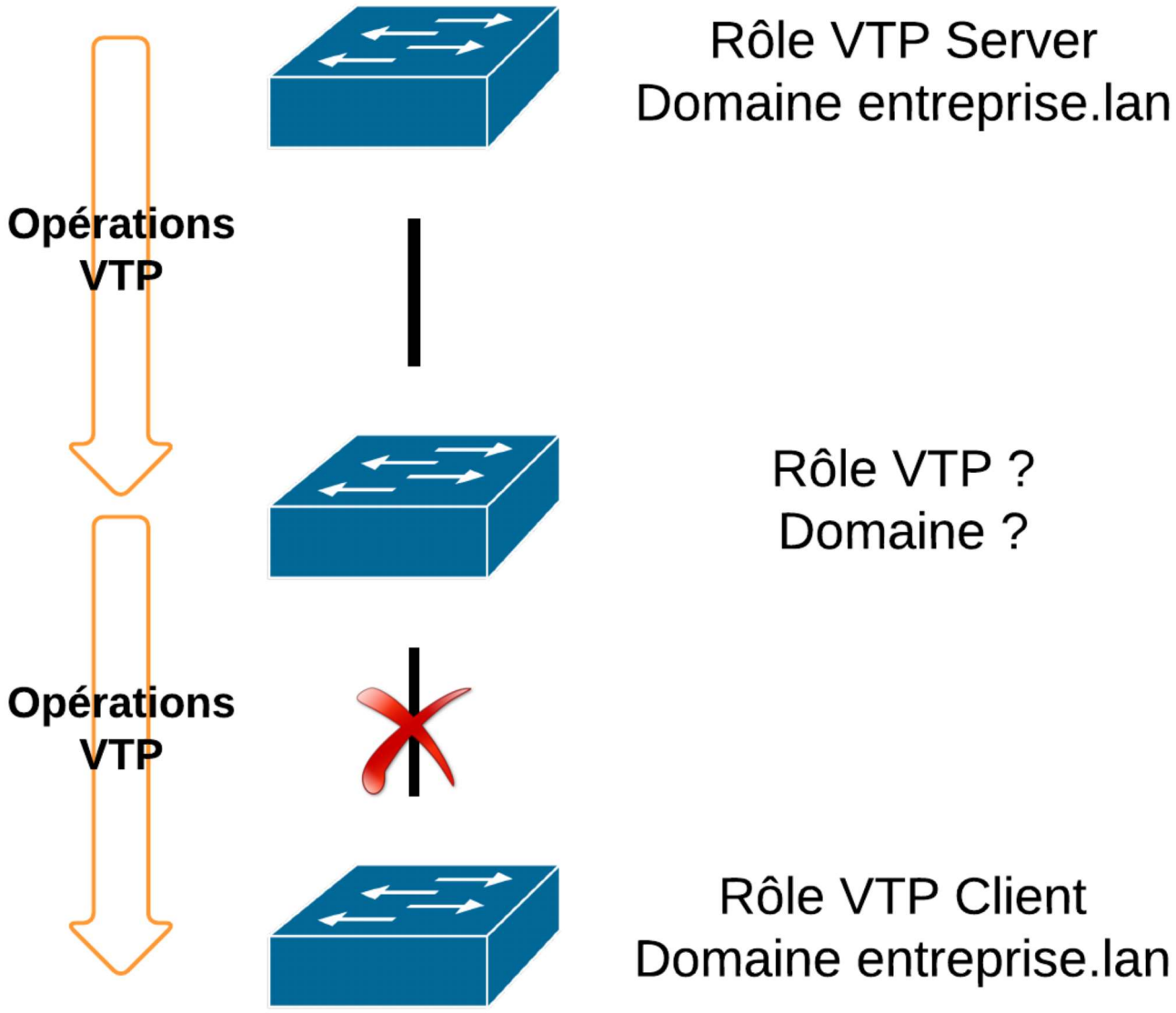
7.2. Domaine et rôles

Deux éléments sont nécessaires au bon fonctionnement de VTP :

- Définir un nom de domaine VTP (appelé aussi domaine de gestion). Ne participent à cette gestion que les commutateurs qui appartiennent à un même domaine.
- Définir pour chaque commutateur un rôle :
  - soit `client` ,
  - soit `transparent` ,
  - soit, pour un seul d'entre eux, `server` .

Il ne peut y avoir qu'un seul commutateur "server" dans un domaine VTP.

7.3. Rôles VTP



Rôles VTP

Chaque opération à partir du “server” VTP sera répercutée sur les “clients” VTP.

Le mode “transparent” laissera le commutateur indifférent à toutes ces opérations. Mais à quoi sert-il de ce cas ? Il assure la connectivité VTP du “server” vers les “clients”.

7.4. Messages VTP et numéros de révision

Les messages VTP sont appelés “VTP Advertisements”. Ceux-ci sont identifiés par un numéro de révision de configuration.

Le numéro de révision le plus élevé sera celui qui modifiera la base de données VLAN.

Ce mécanisme maintient les informations VTP à jour dans un domaine.

7.5. Configuration de VTP

Configurer le rôle VTP du commutateur :

```
(config)#vtp mode ?
  client       Set the device to client mode.
  off          Set the device to off mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
```

Définir le domaine VTP :

```
(config)#vtp domain ?
  WORD  The ascii name for the VTP administrative domain.
```

Pour configurer un mot de passe (identique sur tous les commutateurs du domaine) :

```
(config)#vtp password ?
  WORD  The ascii password for the VTP administrative domain.
```

Avant d’intégrer un nouveau commutateur dans un domaine, on prendra garde d’effacer sa base de données VLAN (`flash:/vlan.dat`) et de le redémarrer en mode client. Manipuler VTP dans un environnement en production est déconseillé !

7.6. Vérification de VTP

(paramètres par défaut)

```
#show vtp status
VTP Version                     : 2
Configuration Revision          : 9
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x13 0xBC 0x6D 0xC9 0xF0 0xF1 0x46 0xC3
Configuration last modified by 0.0.0.0 at 3-1-93 01:03:40
Local updater ID is 192.168.1.1 on interface Vl30 (lowest numbered VLAN interface found)
```

7.7. Mode transparent

Configuration en mode “transparent” :

```
(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

```
(config)#vtp domain mydomain
Changing VTP domain name from NULL to mydomain
```

Vérification :

```
#show vtp status
```

7.8. Désactiver VTP sur un commutateur Cisco

On désactive globalement VTP avec la commande `vtp mode off`

```
(config)#vtp mode off
```

8. Bonnes pratiques

- Faire tomber tous les ports inutilisés.
- Déplacer tous les ports du VLAN 1 dans un autre VLAN.
- Séparer le trafic de gestion de celui des utilisateurs.
- Changer l'ID du VLAN de gestion dans un autre VLAN que le VLAN 1.
- Changer l'ID du VLAN natif dans un autre VLAN que le VLAN 1.
- S'assurer que seuls les périphériques du VLAN de gestion peuvent se connecter aux commutateurs.
- Connexion distante au commutateur uniquement en SSH.
- Désactiver l'autonégociation sur les ports Trunk.
- Ne pas utiliser les modes DTP "dynamic desirable" ou "dynamic auto" sur les ports.
- Désactiver VTP et CDP

Tags : ccna | cisco | commutateur | dtp | icnd1 | icnd2 | inter-vlan | ios | router | routeur | switch | vlan | vtp

Catégories : Switching | VLANs

Mis à jour : Lundi 10 août 2020

État d'avancement du document : 80 %

LAISSER UN COMMENTAIRE

S'IDENTIFIER AVEC OU INSCRIVEZ-VOUS SUR DISQUS ?

Nom

totor20 • il y a 5 mois

Bonjour,
concernant les vlan, ils sont stockés dans vlan.dat? j'ai un stack de switch cisco ou je dois restaurer le startup config a une version antérieur. J'ai bien le fichier txt du startup config. Par contre, si je fais juste ça, le vlan.dat lui restera à sa configuration actuelle? En plus le stack en question est vtp server (ce qui n'apparait pas non plus, je crois dans la conf?)
Quel est la méthode pour restorer mon stack à une version antérieur (en incluant tout les vlans et la conf vtp server)?

^ | v • Répondre • Partager ›

Goffinet Modo → totor20 • il y a 5 mois

Bonjour mon seul conseil est faire appel au support TAC de Cisco Systems.

^ | v • Répondre • Partager ›

totor20 → Goffinet • il y a 5 mois

Nous n'avons pas de support tac

^ | v • Répondre • Partager ›

Khalil Moustafa • il y a 9 mois

Le site est bien fait, on y trouve des résumés du cours donnée par l'académie Cisco

^ | v • Répondre • Partager ›

le_facteur_100 • il y a un an

Bonjour,

Nous n'arrivons pas à ouvrir la connexion vers un CISCO 2960-L avec un PC sous windows10
Nous sommes connecté via ethernet au port ethernet de configuration notre carte réseau est confiigurée en IP 10.0.0.2/255.255.255.0
La carte est desactivée/activée... mais sur firefox impossible de se connecter à l'@ 10.0.0.1
Seriez vous nous proposer une solution ou nous expliquer ce qu'il manque nous manque?
Cordialement

^ | v • Répondre • Partager ›

Goffinet Modo → le_facteur_100 • il y a un an

Bonjour, vous devriez vous connecter au commutateur avec un port console. Voyez l'article https://cisco.goffinet.org/.... Vous êtes ici sur un site de formation à la certification Cisco. Merci.

^ | v • Répondre • Partager ›

le_facteur_100 → Goffinet • il y a un an • edited

Mais sur un autre site (officiel) il était indiqué que nous pouvions utiliser le mini port usb-usb à la place du port console...
Donc finalement cela ne fonctionne pas et il faut absolument connecter ce

Donc finalement cela ne fonctionne pas et il faut absolument connecter ce fameux(...!!) port console couplé à un usb-DSB9pt
Moi je ne comprend pas la raison pour laquelle un simple câble Ethernet n'est pas suffisant...pourquoi ce compliquer la vie...
Bref oui finalement cela fonctionne avec le port console... avec une ou deux astuces quand même, mais bon c'est un site de formation donc je n'en dis pas plus.
Merci

Répondre • Partager ›

mpoukali ngobana nydeirch • il y a un an

Bonjour
je demande votre aide; pour changer le port d'un vlan vers un autre vlan sur le switch ou routeur CISCO.

Répondre • Partager ›

Goffinet Modo ➚ mpoukali ngobana nydeirch • il y a un an

```
(config)#vlan 10
(config-vlan)#name TEST
(config-vlan)#exit
(config)#interface range f0/1 - 20
(config-if-range)#switchport mode access
(config-if-range)#switchport access vlan 10
```

Répondre • Partager ›

mpoukali ngobana nydeirch • il y a un an

bonsoir ; j'ai aimé ce que vous faites mais je tiens à vous dire cela

Répondre • Partager ›