

**Ministère de l'Enseignement Supérieur
Et de la recherche Scientifique**

REPUBLIQUE DE CÔTE D'IVOIRE



THEME :

IMPLEMENTATION DU VLAN TRUNKING PROTOCOL (VTP)



Auteur :
WOEKPO KOMLAN JEAN BAPTISTE

Date 05 / 03 / 2025

Introduction

Le protocole VTP (VLAN Trunking Protocol) est un protocole de gestion de VLAN utilisé dans les réseaux informatiques. Il permet la propagation des informations VLAN à tous les équipements du réseau, facilitant ainsi la gestion des VLAN dans un réseau étendu. VTP est un sujet clé pour les professionnels de la gestion de réseau, car il offre une solution pratique pour centraliser et simplifier la gestion des VLAN. Il permet aux administrateurs de configurer et modifier les VLAN sur un seul commutateur, puis de diffuser ces informations à tous les autres, ce qui simplifie la configuration dans les grands réseaux, fait gagner du temps et réduit les erreurs. Cependant, il est essentiel de suivre les bonnes pratiques de configuration pour éviter les problèmes de sécurité et de performance.

Scénario

Dans une infrastructure réseau de grande envergure comprenant 500 switches, la gestion manuelle des VLAN devient rapidement une tâche complexe et chronophage. Chaque ajout, suppression ou modification de VLAN nécessiterait une intervention sur l'ensemble des équipements pour mettre à jour la base de données VLAN (fichier vlan.dat).

*Pour répondre à cette problématique, Cisco a développé le **VLAN Trunking Protocol (VTP)**, un protocole propriétaire permettant la gestion centralisée des VLANs. Grâce à VTP, il est possible de :*

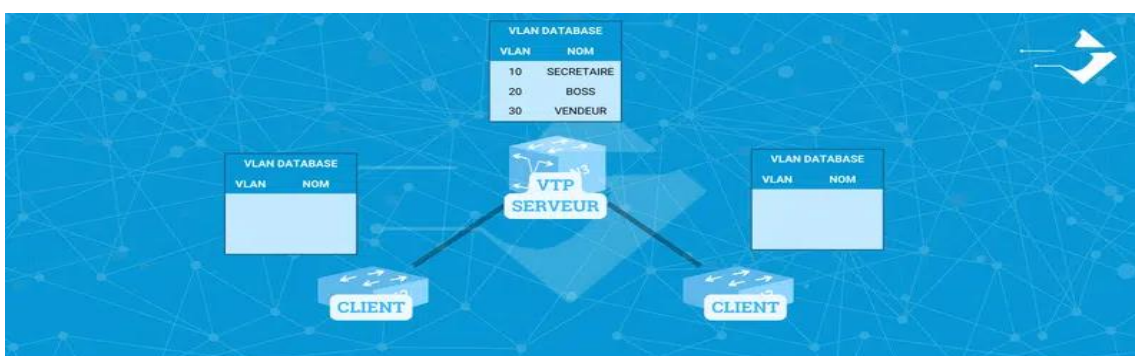
- Ajouter, supprimer et renommer les VLANs sur l'ensemble des switches d'un même domaine*
- Assurer une synchronisation automatique des VLANs sans intervention manuelle sur chaque équipement*
- Réduire les erreurs de configuration et garantir une cohérence dans l'architecture réseau.*

VTP fonctionne en mode client/serveur et repose sur l'échange de messages publicitaires (advertisements) pour propager les mises à jour des VLANs.

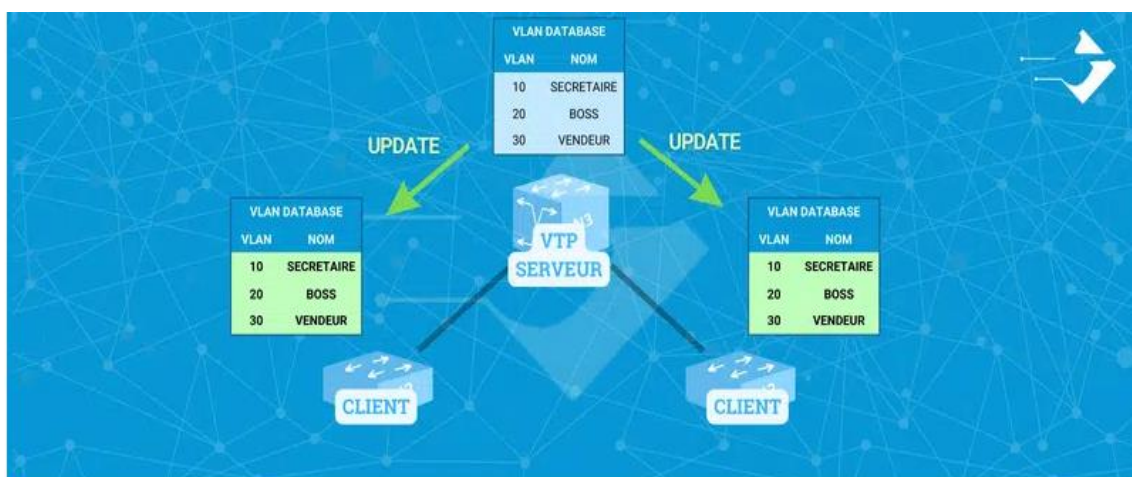
Bien que ce protocole facilite grandement l'administration réseau, il doit être utilisé avec précaution pour éviter les pertes de configuration en cas de mauvaise gestion des versions VTP.

Principe de fonctionnement

Le protocole VTP a pour objectif de synchroniser les informations VLAN entre les différents switches d'un réseau étendu ; en mettant à jour le fichier vlan.dat. Le protocole VTP facilite la gestion des VLAN en permettant la création, la modification et la suppression de VLAN de manière centralisée.



Après avoir configuré le protocole VTP sur les différents switches, la création de nouveaux VLAN se fait sur le serveur VTP. Ce dernier va ensuite diffuser la mise à jour des informations VLAN aux clients VTP.



Les différents mode VTP

1. Mode SERVEUR

- *Permet la création, suppression et modification des VLANs dans un réseau étendu.*
- *Les switches en mode server propagent les mises à jour VTP aux autres équipements du même domaine.*
- *Plusieurs switches peuvent être configurés en **server** pour assurer une gestion centralisée et redondante des VLANs.*

2. Mode CLIENT

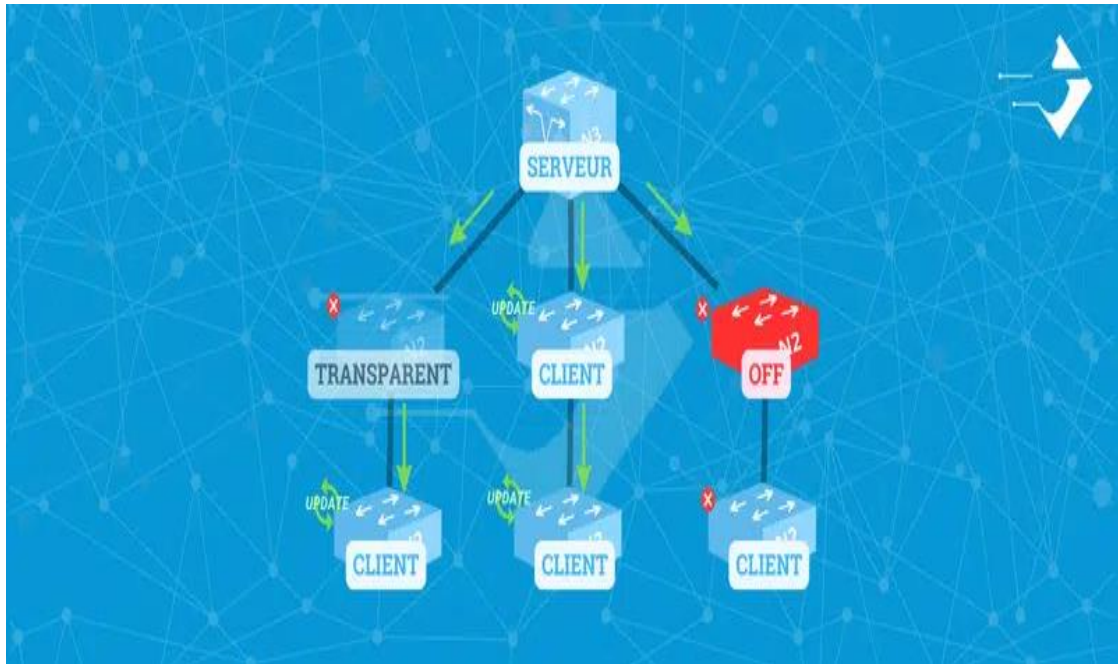
- *Ne permet ni la création, ni la suppression, ni la modification des VLANs.*
- *Apprend les VLANs configurés sur un switch en mode server et met à jour sa base de données VLAN en conséquence.*
- *Relaye les trames VTP vers les autres switches via ses ports trunks.*

3. Mode TRANSPARENT

- *N'applique pas les mises à jour VTP et conserve une base de données VLAN locale.*
- *Relaye les trames VTP vers ses ports trunks, sous certaines conditions selon la version de VTP :*
 - *VTP version 1 : ne relaie les trames que si le domaine et la version VTP correspondent.*
 - *VTP version 2 et 3 : relaie les informations VTP sans condition.*

4. Mode OFF (disponible uniquement en VTP version 3)

- *Ignore totalement les messages VTP.*
- *N'apprend ni ne relaie les mises à jour VTP, assurant une isolation complète.*
- *Utile pour des raisons de sécurité ou lorsque le VTP n'est pas nécessaire.*



Les échanges VTP

Le protocole VTP (VLAN Trunking Protocol) utilise trois types de trames pour échanger des informations et maintenir la synchronisation des VLANs sur l'ensemble du réseau.

1. Summary Advertisements

- *Toutes les 300 secondes pour informer les switches du domaine VTP.*
- *À chaque mise à jour du fichier vlan.dat sur un switch en mode server.*

Elles contiennent les informations suivantes :

- *Version VTP (1, 2 ou 3).*

- **Nom du domaine VTP.**
- **Numéro de révision** (indiquant la version de la base de données VLAN)
- **Time Stamp** (horodatage des modifications)
- **Hash MD5** (pour l'intégration et la vérification des messages)
- **Nombre de trames Subset advertisements qui suivent.**

2. Subset Advertisements

Ces trames sont envoyées lorsqu'un changement est effectué sur un VLAN :

- **Création ou suppression d'un VLAN.**
- **Activation ou désactivation d'un VLAN.**
- **Modification du nom d'un VLAN.**
- **Changement de la taille MTU d'un VLAN.**

3. Client Request Advertisement (Demande de mise à jour du client)

Un switch en mode client envoie cette trame lorsqu'il :

- **Supprime son fichier *vlan.dat* et a besoin de récupérer la base VLAN à jour.**
- **Reçoit un Summary Advertisement avec un numéro de révision trop élevé, ce qui signifie qu'il a une base VLAN obsolète et doit se resynchroniser.**

VTP PRUNNING

Lorsqu'un PC dans un vlan envoie un broadcast, il sera transmis sur toutes les interfaces TRUNK du réseau. Cela peut causer des congestions de trafic inutiles, en particulier pour le VLAN qui ne sont pas présent partout dans l'architecture.



Pour éviter cela, le protocole VTP a intégré l'option "Pruning". Cette fonctionnalité permet de limiter la propagation des broadcasts aux vlan qui sont présents sur chaque lien du réseau. Les switches de chaque vlan échangent des messages pour déterminer quels vlan sont présents sur chaque lien et ajoute automatiquement leurs configurations de pruning en conséquence.

Lorsqu'on active l'option pruning avec le scénario précédent, on obtient l'image suivante :



En utilisant l'option de pruning, les administrateurs peuvent améliorer les performances et l'efficacité de leur réseau, tout en évitant les problèmes de congestion de trafic inutiles.

Configuration de l'option Pruning

Switch(config)# vtp pruning

Configuration du protocole VTP

Afin que le protocole VTP soit opérationnel, il faut que les équipements actifs ai en commun ses propriétés :

- *Domaine VTP.*
- *Mot de passe MD5*
- *Numéro de révision*
- *La même date de dernière modification*
- *Source de la dernière modification*

→ Etape 1 : Choix de la version VTP

Switch(config)# vtp version {1 | 2 | 3}

→ Etape 2 : Spécifier le nom de domaine VTP

Switch(config)# vtp domain <nom_domaine_vtp>

→ Etape 3 : Choisir le mode de notre switch

Switch(config)# vtp mode {server | client | transparent | off }

→ Etape 4 : Sécuriser le protocole VTP

Switch(config)# vtp password < mot de passe >

→ **Etape 5 : Créer les VLANs sur le serveur VTP :**

L'administrateur réseau devra créer manuellement les VLANs sur le switch en mode VTP server :

```
VTP_SERVER (config)# vlan <vlan_ID>  
VTP_SERVER (config-vlan) # name <name_VLAN>  
VTP_SERVER (config)# exit
```

Vérification de la création du vlan :

```
VTP_SERVER(config)# show vlan
```

→ **Etape 6 : Vérification sur un switch en mode VTP client**

```
VTP_CLIENT (config)# show vlan
```

A ce niveau, les vlans créés dans le switch en mode server VTP devraient être répliqués sur tous les switches clients.

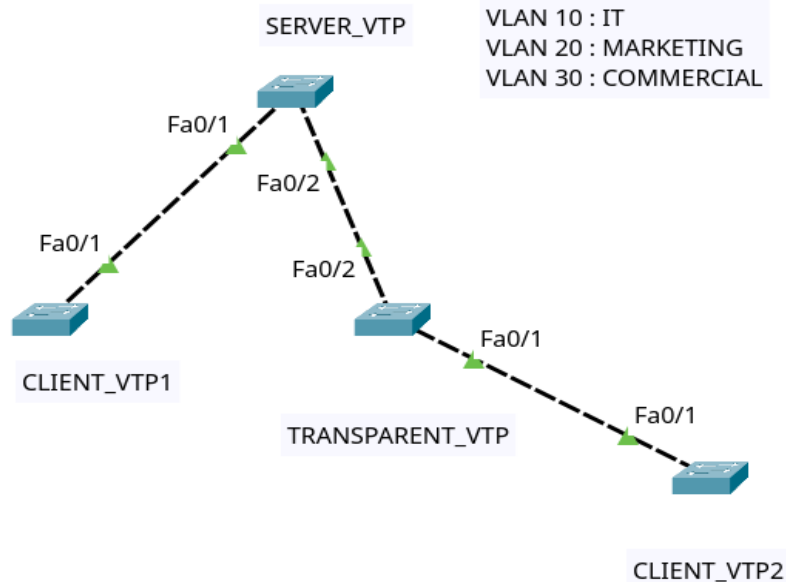
Résumé des commandes

```
Switch(config)# vtp version {1 | 2 | 3}  
Switch(config)# vtp domain <domain_vtp>  
Switch(config)# vtp mode {server | client | transparent | off}  
Switch(config)# vtp password <mot de passe >
```

Vérification du protocole VTP

```
Switch(config)# show vtp status
```

Test du protocole VTP sur Packet Tracer



Nous allons donc configurer le protocole VTP sur ces switches et vérifié s'il fonctionne correctement .

➤ SERVER VTP :

- Configuration du protocole VTP

```
switch(config)# hostname SERVER_VTP
SERVER_VTP(config)# vtp version 2
SERVER_VTP(config)# vtp domain CCNA
SERVER_VTP(config)# vtp mode server
SERVER_VTP(config)# vtp password CCNA
```

- Création des vlans 10, 20, 30

```
SERVER_VTP(config)# vlan 10
SERVER_VTP(config-vlan)# name IT
SERVER_VTP(config-vlan)# exit
```

```
SERVER_VTP(config)# vlan 20
SERVER_VTP(config-vlan)# name MARKETING
SERVER_VTP(config-vlan)# exit
SERVER_VTP(config)# vlan 30
SERVER_VTP(config-vlan)# name COMMERCIAL
SERVER_VTP(config-vlan)# exit
```

- **Liason trunk**

```
SERVER_VTP(config)# interface range FastEthernet 0/1-2
SERVER_VTP(config-if-range)# switchport mode trunk
SERVER_VTP(config-if-range)# switchport trunk allowed vlan
10,20,30
```

➤ **CLIENT_VTP1 :**

- **Configuration du protocole VTP**

```
switch(config)# hostname CLIENT_VTP
CLIENT_VTP1(config)# vtp version 2
CLIENT_VTP1(config)# vtp domain CCNA
CLIENT_VTP1(config)# vtp mode client
CLIENT_VTP1(config)# vtp password CCNA
```

- **Liason trunk**

```
CLIENT_VTP(config)# interface range FastEthernet 0/1
CLIENT_VTP(config-if-range)# switchport mode trunk
CLIENT_VTP(config-if-range)# switchport trunk allowed vlan
10,20,30
```

➤ **CLIENT_VTP2 :**

- **Configuration du protocole VTP**

```
switch(config)# hostname CLIENT_VTP2
CLIENT_VTP2(config)# vtp version 2
CLIENT_VTP2(config)# vtp domain CCNA
CLIENT_VTP2(config)# vtp mode client
CLIENT_VTP2(config)# vtp password CCNA
```

- **Liason trunk**

```
CLIENT_VTP2(config)# interface range FastEthernet 0/1
CLIENT_VTP2(config-if-range)# switchport mode trunk
CLIENT_VTP2(config-if-range)# switchport trunk allowed vlan
10,20,30
```

➤ **TRANSPARENT VTP:**

- **Configuration du protocole VTP**

```
switch(config)# hostname TRANSPARENT_VTP
TRANSPARENT_VTP(config)# vtp version 2
TRANSPARENT_VTP(config)# vtp domain CCNA
TRANSPARENT_VTP(config)# vtp mode transparent
TRANSPARENT_VTP(config)# vtp password cisco
```

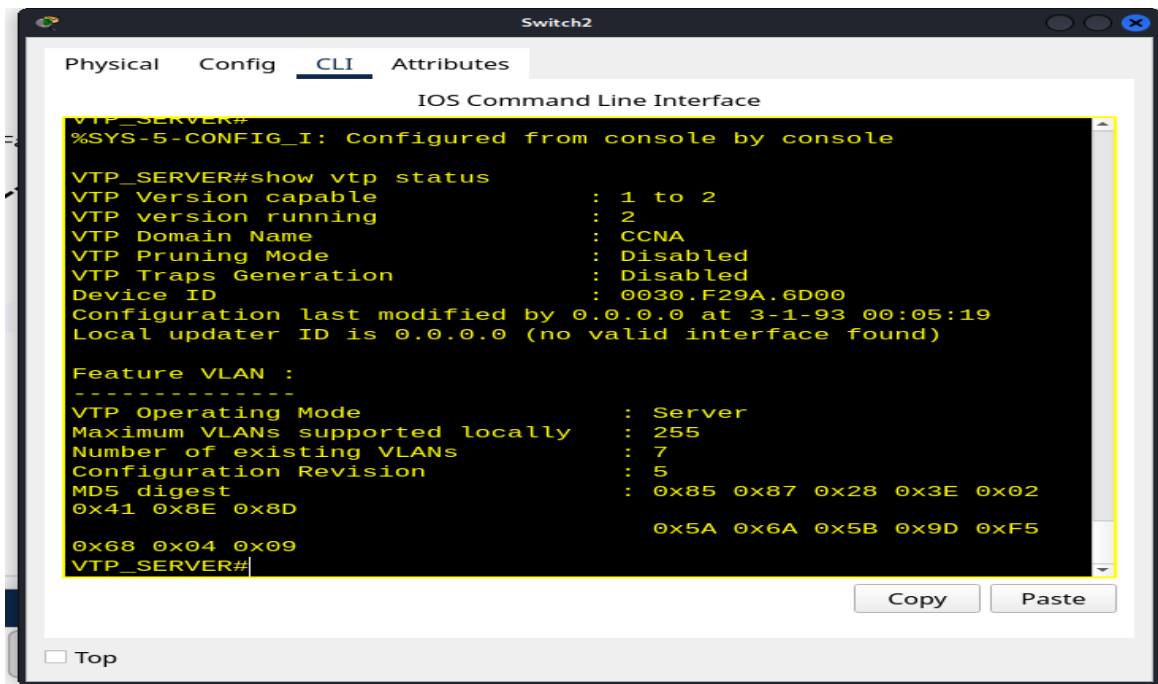
- **Liaison Trunk**

```
TRANSPARENT_VTP(config)# interface range FastEthernet 0/1-2
TRANSPARENT_VTP(config-if-range)# switchport mode trunk
TRANSPARENT_VTP(config-if-range)# switchport trunk allowed
vlan 10,20,30
```

Vérification de l'implémentation du protocole VTP

Une fois le VTP implémenté avec un **serveur VTP**, deux **clients VTP** et un **switch en mode transparent**, il est crucial de vérifier que la propagation des VLANs fonctionne correctement et que chaque switch applique les mises à jour conformément à son mode de fonctionnement. Cette vérification permet de s'assurer de la synchronisation des bases VLAN et d'identifier d'éventuelles anomalies.

SERVER_VTP



Switch2

Physical Config CLI Attributes

IOS Command Line Interface

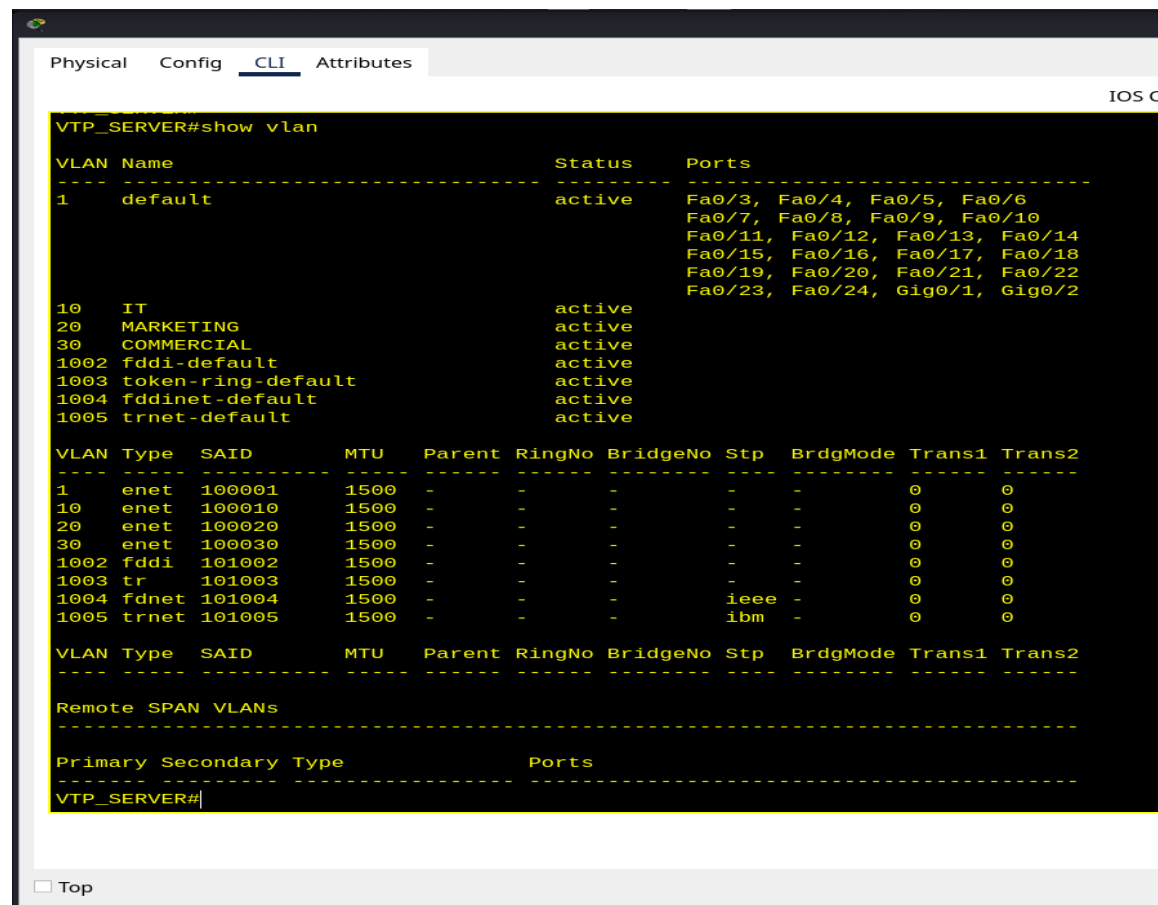
```
VTP_SERVER#
%SYS-5-CONFIG_I: Configured from console by console

VTP_SERVER#show vtp status
VTP Version capable           : 1 to 2
VTP version running          : 2
VTP Domain Name               : CCNA
VTP Pruning Mode              : Disabled
VTP Traps Generation          : Disabled
Device ID                     : 0030.F29A.6D00
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:19
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
-----
VTP Operating Mode            : Server
Maximum VLANs supported locally : 255
Number of existing VLANs      : 7
Configuration Revision        : 5
MD5 digest                   : 0x85 0x87 0x28 0x3E 0x02
                              0x41 0x8E 0x8D
                              0x5A 0x6A 0x5B 0x9D 0xF5
                              0x68 0x04 0x09
VTP_SERVER#
```

Copy Paste

Top



Physical Config CLI Attributes

IOS C

```
VTP_SERVER#show vlan

VLAN Name                Status    Ports
-----
1    default                active    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   IT                      active
20   MARKETING              active
30   COMMERCIAL             active
1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001    1500  -     -     -     -     -         0       0
10   enet  100010    1500  -     -     -     -     -         0       0
20   enet  100020    1500  -     -     -     -     -         0       0
30   enet  100030    1500  -     -     -     -     -         0       0
1002 fddi  101002    1500  -     -     -     -     -         0       0
1003 tr   101003    1500  -     -     -     -     -         0       0
1004 fdnet 101004    1500  -     -     -     -     -         0       0
1005 trnet 101005    1500  -     -     -     -     -         0       0

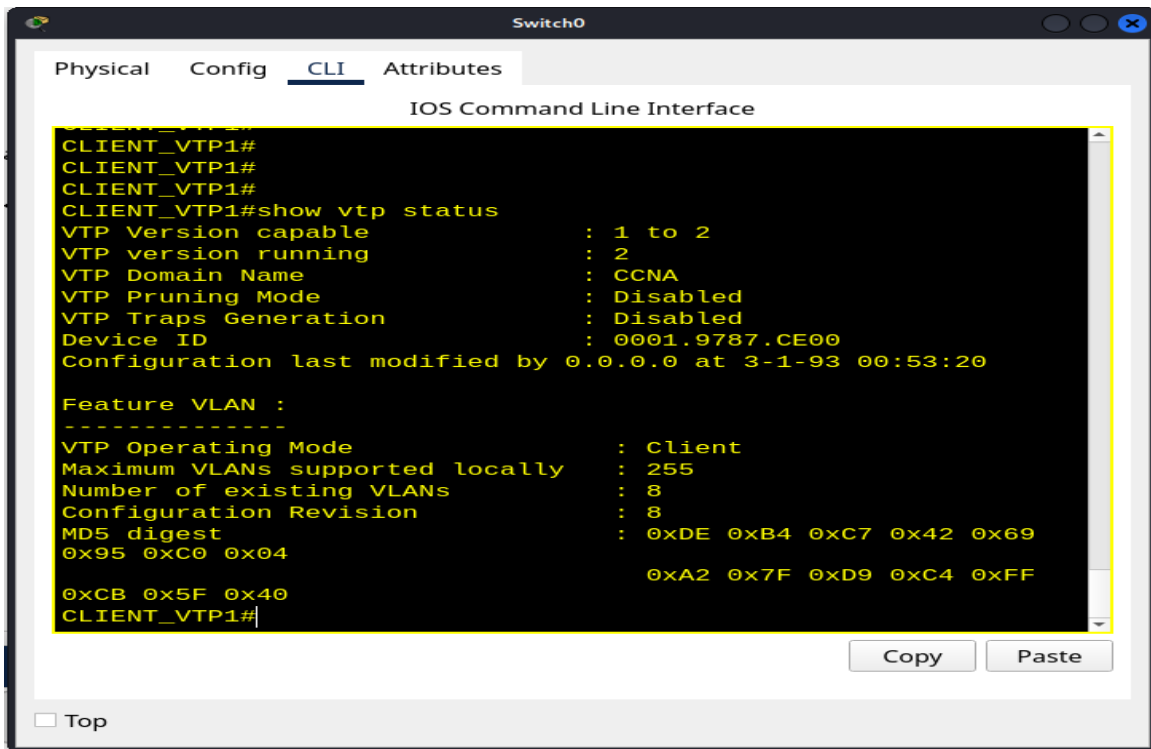
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----

Remote SPAN VLANs
-----

Primary Secondary Type          Ports
-----
VTP_SERVER#
```

Top

CLIENT_VTP1



Switch0

Physical Config CLI Attributes

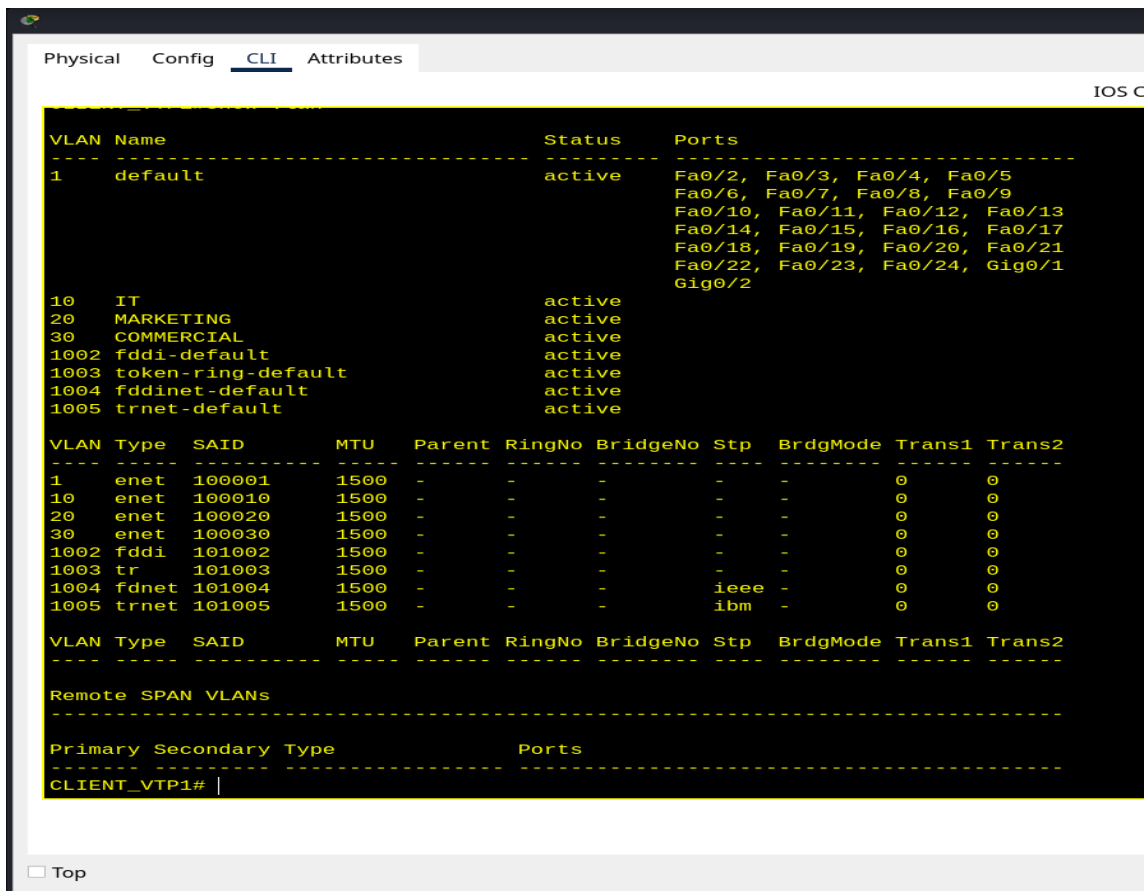
IOS Command Line Interface

```
CLIENT_VTP1#
CLIENT_VTP1#
CLIENT_VTP1#
CLIENT_VTP1#show vtp status
VTP Version capable      : 1 to 2
VTP version running     : 2
VTP Domain Name         : CCNA
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 0001.9787.CE00
Configuration last modified by 0.0.0.0 at 3-1-93 00:53:20

Feature VLAN :
-----
VTP Operating Mode      : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 8
Configuration Revision  : 8
MD5 digest              : 0xDE 0xB4 0xC7 0x42 0x69
                        0x95 0xC0 0x04
                        0xA2 0x7F 0xD9 0xC4 0xFF
0xCB 0x5F 0x40
CLIENT_VTP1#
```

Copy Paste

Top



Physical Config CLI Attributes

IOS C

```
VLAN Name                Status    Ports
-----
1    default                active    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   IT                      active
20   MARKETING              active
30   COMMERCIAL             active
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active

VLAN Type  SAID          MTU   Parent  RingNo BridgeNo  Stp    BrdgMode Trans1 Trans2
-----
1    enet  100001      1500  -       -       -       -         0       0
10   enet  100010      1500  -       -       -       -         0       0
20   enet  100020      1500  -       -       -       -         0       0
30   enet  100030      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

VLAN Type  SAID          MTU   Parent  RingNo BridgeNo  Stp    BrdgMode Trans1 Trans2
-----

Remote SPAN VLANs
-----

Primary Secondary Type          Ports
-----
CLIENT_VTP1#
```

Top

CLIENT_VTP2

```
Switch3
Physical Config CLI Attributes
IOS Command Line Interface
CLIENT_VTP2#
CLIENT_VTP2#
CLIENT_VTP2#
CLIENT_VTP2#show vtp st
CLIENT_VTP2#show vtp status
VTP Version capable      : 1 to 2
VTP version running     : 2
VTP Domain Name         : CCNA
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : 0090.2140.6C00
Configuration last modified by 0.0.0.0 at 3-1-93 00:53:20

Feature VLAN :
-----
VTP Operating Mode      : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 8
Configuration Revision  : 8
MD5 digest              : 0xDE 0xB4 0xC7 0x42 0x69
                        0x95 0xC0 0x04
                        0xA2 0x7F 0xD9 0xC4 0xFF
                        0xCB 0x5F 0x40
CLIENT_VTP2#
```

```
Physical Config CLI Attributes
IOS Con
VLAN Name                Status    Ports
-----
1    default                active    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   IT                       active
20   MARKETING               active
30   COMMERCIAL              active
1002 fddi-default           active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active

VLAN Type SAID      MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
1    enet  100001  1500  -     -     -     -     -     0     0
10   enet  100010  1500  -     -     -     -     -     0     0
20   enet  100020  1500  -     -     -     -     -     0     0
30   enet  100030  1500  -     -     -     -     -     0     0
1002 fddi  101002  1500  -     -     -     -     -     0     0
1003 tr   101003  1500  -     -     -     -     -     0     0
1004 fdnet 101004  1500  -     -     -     -     -     0     0
1005 trnet 101005  1500  -     -     -     -     -     0     0

VLAN Type SAID      MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
Remote SPAN VLANs
-----
Primary Secondary Type          Ports
-----
CLIENT_VTP2#
```

TRANSPARENT_VTP

```
Switch1
Physical Config CLI Attributes
IOS Command Line Interface
TRANSPARENT_VTP>en
TRANSPARENT_VTP#
TRANSPARENT_VTP#
TRANSPARENT_VTP#
TRANSPARENT_VTP#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name         : CCNA
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0060.7035.4900
Configuration last modified by 0.0.0.0 at 3-1-93 00:49:07

Feature VLAN :
-----
VTP Operating Mode       : Transparent
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
Configuration Revision   : 0
MD5 digest               : 0x6C 0x46 0x56 0x15 0x30
                          0xC8 0x34 0x8E
                          0xF6 0xD4 0xC8 0x7C 0x4F
                          0x16 0x52 0xFB
TRANSPARENT_VTP#
```

```
Physical Config CLI Attributes
IOS Comr
MD5 digest : 0x6C 0x46 0x56 0x15 0x30 0xC8 0x34 0x8E
           0xF6 0xD4 0xC8 0x7C 0x4F 0x16 0x52 0xFB
TRANSPARENT_VTP#
TRANSPARENT_VTP#
TRANSPARENT_VTP#
TRANSPARENT_VTP#
TRANSPARENT_VTP#show vlan

VLAN Name                Status      Ports
-----
1    default                active     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

1002 fddi-default          active
1003 token-ring-default    active
1004 fdnet-default         active
1005 trnet-default         active

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

VLAN Type SAID      MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----

Remote SPAN VLANs
-----

Primary Secondary Type      Ports
-----
TRANSPARENT_VTP#
```

Conclusion

Le VTP (VLAN Trunking Protocol) est un protocole puissant et pratique développé par Cisco pour simplifier la gestion des VLANs dans un réseau étendu. Il permet une administration centralisée, réduisant ainsi le temps de configuration et le risque d'erreurs. Grâce aux différents modes de fonctionnement (Server, Client, Transparent et Off), VTP s'adapte aux besoins et aux architectures réseau variées.

Cependant, malgré ses avantages, VTP doit être utilisé avec précaution. Une mauvaise gestion des révisions de configuration peut entraîner la suppression involontaire des VLANs sur l'ensemble du réseau, causant ainsi des interruptions de service majeures. De plus, les failles de sécurité associées à VTP peuvent être exploitées si le protocole n'est pas correctement sécurisé.

Ainsi, bien que VTP facilite grandement l'administration des VLANs, il est essentiel de maîtriser ses mécanismes, d'adopter les bonnes pratiques de configuration et de sécuriser les échanges VTP afin d'éviter toute perturbation réseau.