

Travaux pratiques 4.4.1 : Configuration de base du protocole VTP

Schéma de topologie

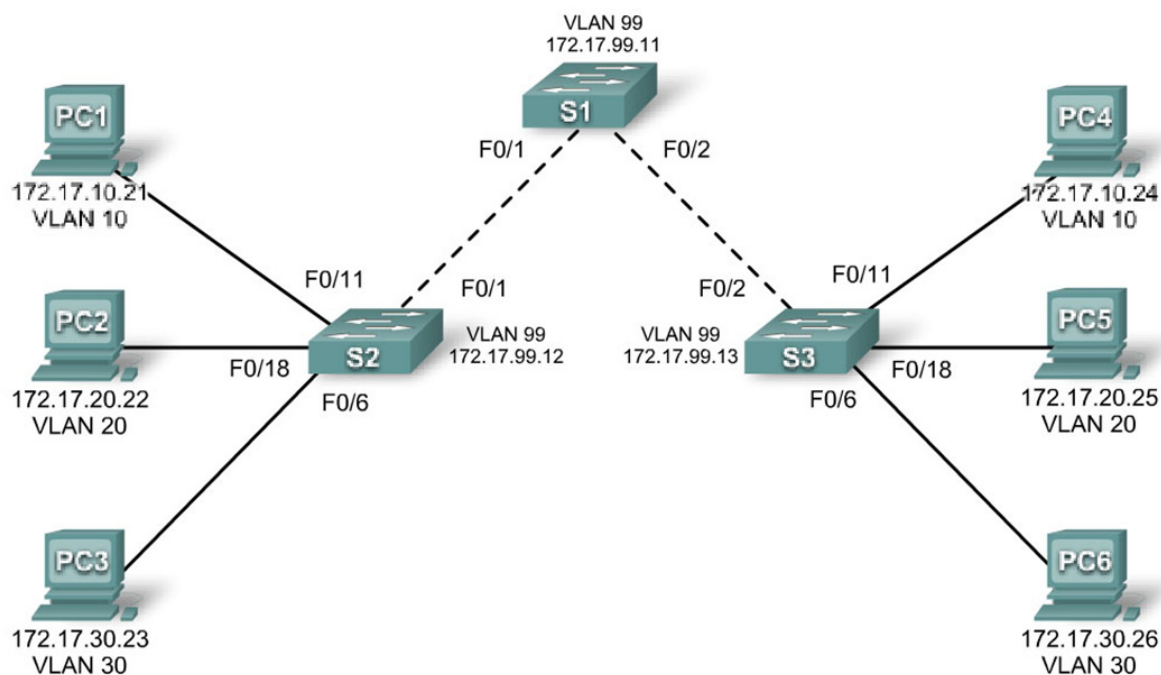


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
S1	VLAN 99	172.17.99.11	255.255.255.0	S/O
S2	VLAN 99	172.17.99.12	255.255.255.0	S/O
S3	VLAN 99	172.17.99.13	255.255.255.0	S/O
PC1	Carte réseau	172.17.10.21	255.255.255.0	172.17.10.1
PC2	Carte réseau	172.17.20.22	255.255.255.0	172.17.20.1
PC3	Carte réseau	172.17.30.23	255.255.255.0	172.17.30.1
PC4	Carte réseau	172.17.10.24	255.255.255.0	172.17.10.1
PC5	Carte réseau	172.17.20.25	255.255.255.0	172.17.20.1
PC6	Carte réseau	172.17.30.26	255.255.255.0	172.17.30.1

Affectation des ports (Commutateurs 2 et 3)

Ports	Affectation	Réseau
Fa0/1 – 0/5	Agrégations 802.1q (VLAN 99 natif)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Installer un réseau conformément au schéma de topologie
- Supprimer la configuration initiale et recharger un commutateur pour revenir aux paramètres par défaut
- Exécuter des tâches de configuration de base sur un commutateur
- Configurer le protocole VTP (VLAN Trunking Protocol) sur tous les commutateurs
- Activer l'agrégation sur les connexions entre commutateurs
- Vérifier la configuration de l'agrégation
- Modifier les modes VTP et en observer les conséquences
- Créer des réseaux locaux virtuels sur le serveur VTP et distribuer ces informations VLAN aux commutateurs du réseau
- Expliquer les différences de fonctionnement entre le mode transparent, le mode serveur et le mode client VTP
- Attribuer des ports de commutateur aux réseaux locaux virtuels
- Enregistrer la configuration VLAN
- Activer l'élagage VTP sur le réseau
- Expliquer la manière dont l'élagage réduit le trafic de diffusion inutile sur le réseau local

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du schéma de topologie

Vous pouvez utiliser n'importe quel commutateur durant les travaux pratiques, pourvu qu'il soit équipé des interfaces indiquées dans la topologie. Les résultats présentés dans ces travaux pratiques proviennent des commutateurs 2960. Les autres types de commutateur peuvent produire des résultats différents. Si vous utilisez des commutateurs plus anciens, certaines commandes peuvent être différentes ou indisponibles.

Vous remarquerez dans le tableau d'adressage que les ordinateurs ont été configurés avec une adresse IP de passerelle par défaut. Cette adresse peut correspondre à l'adresse IP du routeur local qui n'est pas inclus dans ce scénario des travaux pratiques. La passerelle par défaut et le routeur sont nécessaires pour que les ordinateurs de différents réseaux locaux virtuels puissent communiquer. Ce point est traité dans un prochain chapitre.

Configurez les connexions console pour les trois commutateurs.

Étape 2 : suppression des configurations actuelles des commutateurs

Si nécessaire, reportez-vous aux Travaux pratiques 2.5.1, Annexe 1, pour consulter la procédure de suppression des configurations des commutateurs et des réseaux locaux virtuels. Utilisez la commande **show vlan** pour confirmer que seuls les réseaux locaux virtuels par défaut existent et que tous les ports sont affectés au VLAN 1.

```
Switch#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 Gig1/1, Gig1/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Étape 3 : désactivation de tous les ports à l'aide de la commande shutdown

Répétez ces commandes pour chaque commutateur dans la topologie.

```
Switch(config)#interface range fa0/1-24  
Switch(config-if-range)#shutdown  
Switch(config-if-range)#interface range gi0/1-2  
Switch(config-if-range)#shutdown
```

Tâche 2 : configuration de base des commutateurs

Étape 1 : configuration de base des commutateurs S1, S2 et S3

Configurez les commutateurs S1, S2 et S3 conformément aux instructions suivantes et enregistrez toutes vos configurations :

- Configurez le nom d'hôte du commutateur comme indiqué dans la topologie.
- Désactivez la recherche DNS.
- Configurez le mot de passe **class** pour le mode d'exécution.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.

(Résultats pour S1)

```
Switch>enable  
Switch#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#hostname S1  
S1(config)#enable secret class  
S1(config)#no ip domain-lookup  
S1(config)#line console 0  
S1(config-line)#password cisco
```

```
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Étape 2 : réactivation des ports utilisateur sur S2 et S3

Configurez les ports utilisateur en mode d'accès. Consultez le diagramme de la topologie pour déterminer les ports qui sont connectés aux périphériques de l'utilisateur final.

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
```

```
S3(config)#interface fa0/6
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/11
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/18
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
```

Étape 3 : réactivation des ports agrégés sur S1, S2 et S3

```
S1(config)#interface fa0/1
S1(config-if)#no shutdown
S1(config)#interface fa0/2
S1(config-if)#no shutdown
```

```
S2(config)#interface fa0/1
S2(config-if)#no shutdown
```

```
S3(config)#interface fa0/2
S3(config-if)#no shutdown
```

Tâche 3 : configuration des interfaces Ethernet sur les ordinateurs hôtes

Configurez les interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 et PC6 avec les adresses IP et les passerelles par défaut indiquées dans le tableau d'adressage au début des travaux pratiques.

Vérifiez que PC1 peut envoyer une requête ping à PC4, que PC2 peut envoyer une requête ping à PC5, et que PC3 peut faire de même à PC6.

Tâche 4 : configuration du protocole VTP sur les commutateurs

Le protocole VTP permet à l'administrateur réseau de contrôler les instances des réseaux locaux virtuels sur le réseau en créant des domaines VTP. Dans chaque domaine VTP, un ou plusieurs commutateurs sont configurés en tant que serveurs VTP. Les réseaux locaux virtuels sont alors créés sur le serveur VTP et élargis aux autres commutateurs du domaine. La définition du mode de fonctionnement, du domaine et du mot de passe font partie des tâches de configuration VTP courantes. Au cours de ces travaux pratiques, vous utiliserez S1 comme serveur VTP, S2 et S3 étant configurés comme clients VTP ou en mode transparent VTP.

Étape 1 : vérification des paramètres VTP courants sur les trois commutateurs

S1#**show vtp status**

```
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             :
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

S2#**show vtp status**

```
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             :
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

S3#**show vtp status**

```
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             :
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Notez que les trois commutateurs sont en mode serveur. Le mode serveur est le mode VTP par défaut pour la plupart des commutateurs Catalyst.

Étape 2 : configuration du mode de fonctionnement, du nom de domaine et du mot de passe VTP sur les trois commutateurs

Configurez le nom de domaine VTP **Lab4** et le mot de passe VTP **cisco** pour les trois commutateurs. Configurez S1 en mode serveur, S2 en mode client et S3 en mode transparent.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end
```

```
S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end
```

```
S3(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
S3(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Remarque : le nom de domaine VTP peut être appris par un commutateur client à partir d'un commutateur serveur, mais uniquement si le domaine du commutateur client a l'état Null. Il n'apprend pas de nouveau nom si un nom a déjà été défini. Pour cela, il est recommandé de configurer manuellement le nom de domaine sur tous les commutateurs pour s'assurer qu'il est correctement configuré. Les commutateurs de différents domaines VTP n'échangent pas les informations VLAN.

Étape 3 : configuration de l'agrégation et du réseau local virtuel natif pour les ports agrégés sur les trois commutateurs

Utilisez la commande **interface range** en mode de configuration globale pour simplifier cette tâche.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
```

```
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Étape 4 : configuration de la sécurité des ports sur les commutateurs de couche d'accès S2 et S3

Configurez les ports fa0/6, fa0/11 et fa0/18 afin qu'ils autorisent uniquement un seul hôte et qu'ils apprennent l'adresse MAC de l'hôte de manière dynamique.

```
S2(config)#interface fa0/6
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/11
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#end
```

```
S3(config)#interface fa0/6
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/11
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/18
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#end
```

Étape 5 : configuration des réseaux locaux virtuels sur le serveur VTP

Quatre réseaux locaux virtuels supplémentaires sont requis dans ces travaux pratiques :

- VLAN 99 (management)
- VLAN 10 (faculty/staff)
- VLAN 20 (students)
- VLAN 30 (guest)

Configurez ces réseaux sur le serveur VTP.

```
S1(config)#vlan 99
S1(config-vlan)#name direction
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name personnel enseignant/administratif
S1(config-vlan)#exit
S1(config)#vlan 20
```

```
S1(config-vlan)#name participants
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name invité
S1(config-vlan)#exit
```

Vérifiez que les réseaux locaux virtuels ont été créés sur S1 via la commande **show vlan brief**.

Étape 6 : vérification de la distribution sur S2 et S3 des réseaux locaux virtuels créés sur S1

Utilisez la commande **show vlan brief** sur S2 et S3 pour déterminer si le serveur VTP a élargi la configuration des réseaux locaux virtuels à tous les commutateurs.

S2#**show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, 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, Gi0/1 Gi0/2
10	faculty/staff	active	
20	students	active	
30	guest	active	
99	management	active	

S3#**show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, 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, Gi0/1 Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Les mêmes réseaux locaux virtuels sont-ils configurés sur tous les commutateurs ? _____

Expliquez ici pourquoi S2 et S3 ont des configurations de réseaux locaux virtuels différentes.

Étape 7 : création d'un réseau local virtuel sur les commutateurs 2 et 3

```
S2(config)#vlan 88
```

La configuration d'un réseau local virtuel %VTP n'est pas autorisée lorsque le périphérique est en mode CLIENT.

```
S3(config)#vlan 88
```

```
S3(config-vlan)#name test
```

```
S3(config-vlan)#
```

Pourquoi est-il impossible de créer un réseau local virtuel sur S2, alors que cela est possible sur S3 ?

Supprimez le VLAN 88 de S3.

```
S3(config)#no vlan 88
```

Étape 8 : configuration manuelle des réseaux locaux virtuels

Configurez les quatre réseaux locaux virtuels identifiés à l'étape 5 sur le commutateur S3.

```
S3(config)#vlan 99
```

```
S3(config-vlan)#name management
```

```
S3(config-vlan)#exit
```

```
S3(config)#vlan 10
```

```
S3(config-vlan)#name faculty/staff
```

```
S3(config-vlan)#exit
```

```
S3(config)#vlan 20
```

```
S3(config-vlan)#name students
```

```
S3(config-vlan)#exit
```

```
S3(config)#vlan 30
```

```
S3(config-vlan)#name guest
```

```
S3(config-vlan)#exit
```

Un des avantages de VTP est illustré ici. La configuration manuelle est fastidieuse et présente des risques d'erreur, et toute erreur introduite ici peut empêcher la communication au sein du réseau local virtuel. En outre, ces types d'erreurs peuvent être difficiles à résoudre.

Étape 9 : configuration de l'adresse de l'interface de gestion sur les trois commutateurs

```
S1(config)#interface vlan 99
```

```
S1(config-if)#ip address 172.17.99.11 255.255.255.0
```

```
S1(config-if)#no shutdown
```

```
S2(config)#interface vlan 99
```

```
S2(config-if)#ip address 172.17.99.12 255.255.255.0
```

```
S2(config-if)#no shutdown
```

```
S3(config)#interface vlan 99
```

```
S3(config-if)#ip address 172.17.99.13 255.255.255.0
```

```
S3(config-if)#no shutdown
```

Vérifiez que les commutateurs sont configurés correctement en envoyant des requêtes ping entre eux. À partir de S1, envoyez une requête ping à l'interface de gestion sur S2 et S3. À partir de S2, envoyez une requête ping à l'interface de gestion sur S3.

Les requêtes ping ont-elles abouti ? _____

Dans le cas contraire, corrigez les configurations des commutateurs et réessayez.

Étape 10 : affectation des ports de commutateur aux réseaux locaux virtuels

Reportez-vous au tableau d'affectation des ports au début des travaux pratiques pour affecter les ports aux réseaux locaux virtuels. Utilisez la commande **interface range** pour simplifier cette tâche. Les affectations des ports ne sont pas configurées via VTP. Elles doivent être configurées sur chaque commutateur de manière manuelle ou dynamique via un serveur VMPS. Les commandes sont décrites pour S3 uniquement mais les commutateurs S2 et S1 doivent également être configurés de la même façon. Enregistrez la configuration lorsque vous avez terminé.

```
S3(config)#interface range fa0/6-10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11-17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18-24
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end
S3#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
S3#
```

Tâche 5 : configuration de l'élagage VTP sur les commutateurs

L'élagage VTP permet à un serveur VTP de supprimer le trafic de diffusion IP pour des réseaux locaux virtuels spécifiques et de le remplacer par des commutateurs ne présentant aucun port dans ce réseau local virtuel. Par défaut, toutes les monodiffusions et diffusions inconnues d'un réseau local virtuel sont transmises à l'ensemble du réseau local virtuel. Tous les commutateurs du réseau reçoivent l'ensemble des diffusions, même lorsque peu d'utilisateurs sont connectés à ce réseau local virtuel. L'élagage VTP est utilisé pour éliminer ou élaguer ce trafic inutile. L'élagage préserve la bande passante du réseau local car il est inutile de transmettre les diffusions aux commutateurs qui n'en ont pas besoin.

L'élagage est configuré sur le commutateur de serveur via la commande **vtp pruning** en mode de configuration globale. La configuration est élargie aux commutateurs client.

Confirmez la configuration de l'élagage VTP sur chaque commutateur à l'aide de la commande **show vtp status**. Le mode d'élagage VTP doit être activé sur chaque commutateur.

```
S1#show vtp status
VTP Version                : 2
Configuration Revision      : 17
Maximum VLANs supported locally : 255
Number of existing VLANs    : 9
VTP Operating Mode          : Server
VTP Domain Name             : Lab4
VTP Pruning Mode             : Enabled
<résultat omis>
```

Tâche 6 : remise en état

Supprimez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).