Chap. VI Les réseaux locaux virtuels

Une des technologies qui permet de parvenir à de bonnes performances réseau consiste à diviser les vastes domaines de diffusion en domaines plus petits à l'aide de **réseaux locaux virtuels (VLAN : Virtual Local Area Network).** Avec des domaines de diffusion plus petits, le nombre de périphériques participant aux diffusions est limité et les périphériques peuvent être divisés en groupes fonctionnels.

Les VLAN reposent sur des connexions logiques, et non des connexions physiques. Un VLAN crée un domaine de diffusion logique qui peut s'étendre sur plusieurs segments de réseau local physique.

VI.1 Présentation des réseaux locaux virtuels

Un VLAN permet à un administrateur réseau de créer des groupes de périphériques en réseau logique qui se comportent comme s'ils se trouvaient sur un réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres réseaux locaux virtuels.

À l'aide de réseaux locaux virtuels, vous pouvez segmenter de manière logique des réseaux commutés selon des fonctions ou des services.

Dans la figureVI.1, un VLAN a été créé pour les étudiants (VLAN10) et un autre pour le personnel enseignant (VLAN20). Ces réseaux locaux virtuels permettent à l'administrateur réseau d'implémenter des stratégies d'accès et de sécurité pour des groupes d'utilisateurs spécifiques. Par exemple, il peut autoriser le personnel enseignant, mais pas les étudiants, à accéder aux serveurs de gestion d'e-learning pour élaborer des supports de cours en ligne.

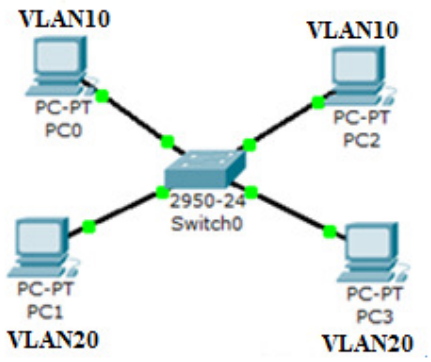


Figure VI.1 Un Switch et plusieurs Vlan

Les VLAN permettent à plusieurs réseaux et sous-réseaux IP de coexister sur le même réseau commuté. Pour que les ordinateurs communiquent sur le même VLAN, chacun d'entre eux doit avoir une adresse IP et un masque de sous-réseau compatible avec ce VLAN. Le VLAN doit être configuré sur le commutateur et

chaque port du commutateur doit être affecté au VLAN. Un port de commutateur sur lequel un seul VLAN est configuré s'appelle un « **port d'accès** ».

VI.1.1 Avantages d'un réseau local virtuel

L'implémentation de la technologie VLAN permet à un réseau d'assurer une prise en charge plus souple des objectifs de l'entreprise. Les principaux avantages des VLAN sont les suivants :

- **Sécurité** : les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité.
- **Réduction des coûts** : des économies sont réalisées grâce à une diminution des mises à niveau du réseau et à l'utilisation plus efficace de la bande passante.
- **Meilleures performances** : le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.
- **Atténuation des tempêtes de diffusion** : le fait de diviser un réseau en plusieurs réseaux locaux virtuels réduit le nombre de périphériques susceptibles de participer à une tempête de diffusion.
- **Efficacité accrue du personnel informatique** : les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN. Lorsque vous configurez un nouveau commutateur, toutes les stratégies et procédures déjà configurées pour le VLAN correspondant sont implémentées lorsque les ports sont affectés. Le personnel informatique peut identifier facilement la fonction d'un VLAN en lui donnant un nom approprié.
- **Gestion simplifiée de projets ou d'applications** : les VLAN rassemblent des utilisateurs et des périphériques réseau pour prendre en charge des impératifs commerciaux ou géographiques. La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application spécialisée.

VI.1.2 Plages d'ID de VLAN

Les réseaux locaux virtuels d'accès sont divisés selon une plage normale ou une plage étendue.

Réseaux locaux virtuels à plage normale

- Utilisés dans les réseaux de petites, moyennes et grandes entreprises.
- Identifiés par un **ID de VLAN** compris entre **1 et 1005.**
- Les ID de 1002 à 1005 sont réservés aux VLAN Token Ring et aux VLAN à interface de données distribuées sur fibre (FDDI).
- Les ID **1** et **1002 à 1005** sont automatiquement créés et ne peuvent pas être supprimés.

- Les configurations sont stockées dans un fichier de base de données VLAN, appelé **vlan.dat**. Le fichier vlan.dat se trouve dans la mémoire flash du commutateur.
- Le protocole VTP (VLAN Trunking Protocol), qui permet de gérer des configurations de VLAN entre des commutateurs, ne peut apprendre que les VLAN à plage normale et les stocke dans le fichier de base de données VLAN.

Réseaux locaux virtuels à plage étendue

- Permettent aux fournisseurs de services d'étendre leur infrastructure à un plus grand nombre de clients.
- Sont identifiés par un ID de VLAN compris entre 1006 et 4094.
- Prennent en charge moins de fonctionnalités VLAN que les VLAN à plage normale.
- Sont enregistrés dans le **fichier de configuration en cours.**
- Le protocole VTP ne prend pas en compte les VLAN à plage étendue.

VI.2 Types de réseaux locaux virtuels

Aujourd'hui, la méthode d'implémentation des VLAN est presque toujours la même : il s'agit de VLAN basés sur le port. Ce type de VLAN est associé à un port appelé ' ***réseau local virtuel d'accès*** ' .

Dans le réseau, il existe plusieurs termes pour désigner les VLAN. Certains termes définissent **le type de trafic** réseau transporté, tandis que d'autres décrivent **une fonction spécifique** remplie par le VLAN. Voici certains des termes les plus couramment utilisés pour désigner les VLAN :

VI.2.1 VLAN de données

Un VLAN de données est un réseau local virtuel qui est configuré pour ne transporter que le trafic généré par l'utilisateur.

Un VLAN acheminant du trafic de voix ou de gestion ne fait pas partie d'un VLAN de données. Il est d'usage de séparer le *trafic de voix* et *de gestion* du *trafic de données*. Un VLAN de données est parfois appelé un *VLAN utilisateur*. Les VLAN de données sont utilisés pour diviser un réseau en groupes d'utilisateurs ou de périphériques.

VI.2.2 VLAN par défaut

Tous les ports du commutateur deviennent membres du VLAN par défaut après le démarrage initial du commutateur. Étant donné que tous les ports du commutateur participent au VLAN par défaut, ils appartiennent tous au même

domaine de diffusion. Cela permet à n'importe quel périphérique connecté à n'importe quel port du commutateur de communiquer avec d'autres périphériques sur d'autres ports du commutateur. Le VLAN par défaut des commutateurs Cisco est le VLAN 1. Le VLAN 1 possède les mêmes caractéristiques que n'importe quel autre VLAN, sauf que vous ne pouvez ni le renommer, ni le supprimer.

Par défaut, tout le trafic de contrôle de couche 2 est associé au VLAN 1.

VI.2.3 VLAN natif

Un VLAN natif est affecté à un port d'agrégation 802.1Q. Un port d'agrégation 802.1Q prend en charge le trafic provenant de nombreux VLAN (trafic étiqueté ou « tagged traffic »), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté ou « untagged traffic »). Le port d'agrégation (ou trunk) 802.1Q place le trafic non étiqueté sur le VLAN natif, qui par défaut est le VLAN 1.

VI.2.4 VLAN de gestion

Un VLAN de gestion est un réseau local virtuel que vous configurez pour accéder aux fonctionnalités de gestion d'un commutateur. C'est le VLAN 1 qui fait office de VLAN de gestion si vous ne définissez pas explicitement un VLAN distinct pour remplir cette fonction. Il faut attribuer au VLAN de gestion une adresse IP et un masque de sous-réseau. Un commutateur peut être géré par le biais de HTTP, de Telnet, de SSH ou de SNMP. Étant donné que le VLAN 1 est déjà le VLAN par défaut dans la configuration initiale d'un commutateur Cisco, il ne doit pas servir en plus de VLAN de gestion. Il faut en effet éviter qu'un utilisateur arbitraire qui se connecte à un commutateur ne se retrouve par défaut sur le VLAN de gestion.

VI.2.5 VLAN voix

Le trafic de voix sur IP requiert les éléments suivants :

- bande passante consolidée pour garantir la qualité de la voix ;
- priorité de transmission par rapport aux autres types de trafic réseau ;
- possibilité de routage autour des zones encombrées du réseau ;
- délai inférieur à 150 millisecondes (ms) sur le réseau.

Pour remplir ces conditions, le réseau entier doit être conçu pour prendre en charge la voix sur IP.

VI.3 Types de trafic réseau

Étant donné qu'un VLAN possède toutes les caractéristiques d'un LAN, il doit accueillir le même trafic réseau qu'un LAN.

VI.3.1Trafic de contrôle et de gestion du réseau

De nombreux types de trafic de contrôle et de gestion du réseau peuvent être présents sur le réseau, notamment les mises à jour CDP (Cisco Discovery Protocol), le trafic SNMP (Simple Network Management Protocol) et le trafic RMON (Remote Monitoring).

VI.3.2 Téléphonie sur IP

Les types de trafic de téléphonie sur IP sont le trafic de signalisation et le trafic vocal. Le trafic de signalisation est chargé de l'établissement, de la progression et de l'arrêt des appels, et traverse le réseau d'un bout à l'autre. L'autre type de trafic de téléphonie se compose de paquets de données de la conversation vocale proprement dite.

VI.3.3 Données normales

Le trafic de données normales est lié à la création et au stockage de fichiers, aux services d'impression, à l'accès à la base de données de messagerie et à d'autres applications réseau partagées d'usage professionnel. Les VLAN sont une solution évidente pour ce type de trafic, car vous pouvez segmenter les utilisateurs d'après leur fonction ou leur emplacement géographique pour gérer plus facilement leurs besoins spécifiques.

VI.4 Modes d'appartenance des ports de commutateur

Les ports de commutateur sont des interfaces de couche 2 uniquement qui sont associées à un port physique. Les ports de commutateur appartiennent à un ou plusieurs VLAN.

VI.4.1 Modes de port de commutateur de VLAN

Lorsque vous configurez un VLAN, vous devez lui affecter un numéro d'identification et vous pouvez éventuellement lui donner un nom. L'objectif des implémentations de réseaux locaux virtuels est d'associer judicieusement des ports à des VLAN donnés. Un port peut être configuré pour prendre en charge les types de VLAN suivants :

- **VLAN statique** : les ports d'un commutateur sont affectés manuellement à un VLAN.

- **VLAN dynamique** : ce mode n'est pas couramment utilisé dans les réseaux de production. L'appartenance d'un port à un VLAN dynamique se configure à l'aide d'un serveur spécial appelé serveur VMPS (VLAN Membership Policy Server). Avec le serveur VMPS, vous affectez dynamiquement les ports de commutateur aux VLAN, en fonction de l'adresse MAC source du périphérique connecté au port. L'avantage de ce mode apparaît lorsque vous

déplacez un hôte à partir d'un port se trouvant sur un commutateur du réseau vers un port se trouvant sur un autre commutateur du réseau : le commutateur affecte dynamiquement le nouveau port au VLAN correspondant à cet hôte.

- **VLAN voix** : un port est configuré en mode voix pour qu'il puisse prendre en charge un téléphone IP qui est connecté dessus. Avant de configurer un VLAN voix sur le port, vous devez d'abord configurer un VLAN pour le trafic vocal et un VLAN pour les données.

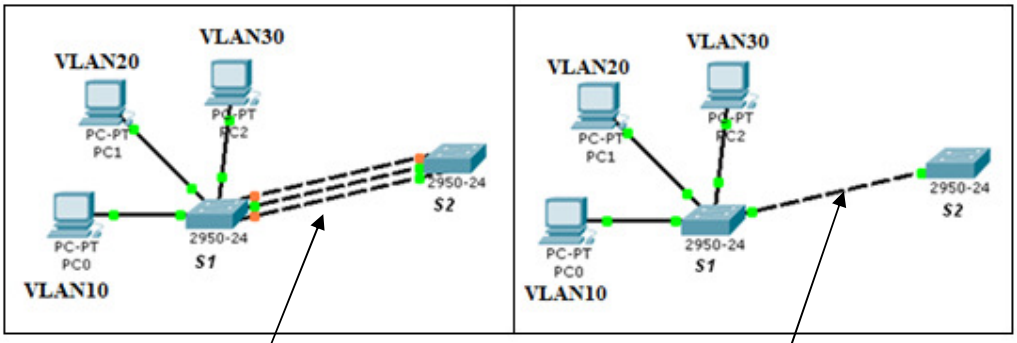
VI.5 Agrégation de VLAN

Une agrégation (trunk) est une liaison point à point entre deux périphériques réseau qui porte plusieurs VLAN (figure VI.2.b). Une agrégation de VLAN vous permet d'étendre les VLAN à l'ensemble d'un réseau. Cisco prend en charge la norme IEEE 802.1Q pour coordonner les agrégations sur les interfaces Fast Ethernet et Gigabit Ethernet.

Les trunks de VLAN permettent à tout le trafic VLAN de se propager entre les commutateurs, de sorte que les périphériques du même VLAN connectés à différents commutateurs puissent communiquer sans l'intervention d'un routeur.

Une agrégation de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour les VLAN entre les commutateurs et les routeurs.

La figure VI.2.a présente une liaison distincte pour chaque sous-réseau. Trois (03) liaisons distinctes connectent les commutateurs S1 et S2, ce qui laisse trois ports de moins aux périphériques utilisateur. À chaque fois qu'un nouveau sous-réseau est pris en compte, une nouvelle liaison est requise pour chaque commutateur du réseau.



a. Liaisons distinctes pour chaque sous-réseau (VLAN) **b. Agrégation**

Figure VI.2 VLAN et agrégation

Dans la figure VI.3, la topologie du réseau contient une agrégation de VLAN qui connecte les commutateurs S1 et S2 (S1 et S3) au moyen d'une seule liaison physique. C'est de cette manière qu'un réseau doit être configuré.

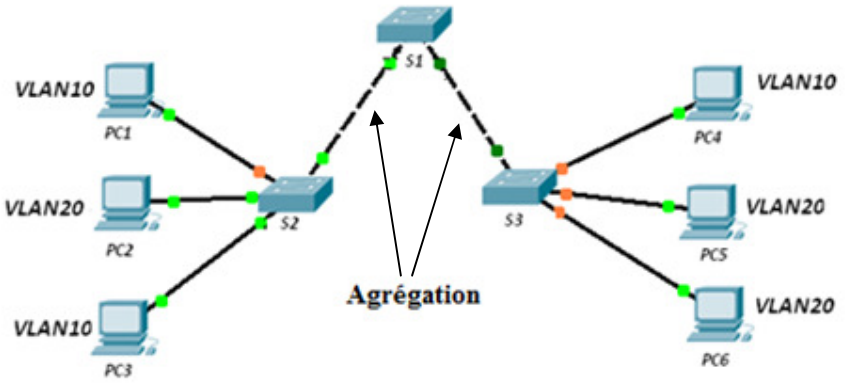


Figure VI.3 Plusieurs Switch, plusieurs Vlan et Agrégation

VI.5.1 Étiquetage des trames Ethernet pour l'identification des VLAN

Les commutateurs (de la gamme Catalyst 2960) sont des périphériques de couche 2. Ils utilisent les informations de l'en-tête des trames Ethernet pour transférer les paquets. L'en-tête des trames Ethernet standard ne contient pas d'informations sur le VLAN auquel appartiennent les trames. Par conséquent, lorsque celles-ci sont placées sur une agrégation, il convient d'ajouter les informations relatives au VLAN dont elles dépendent. Ce processus, appelé ***étiquetage***, s'effectue à l'aide de l'en-tête IEEE 802.1Q. Cette étiquette de 4 octets est insérée dans l'en-tête d'origine de la trame Ethernet, indiquant le VLAN auquel la trame appartient (figure VI.5), entre le *champ adresse Mac source* et le *champ longueur/Type*.

Lorsque le commutateur reçoit une trame sur un port configuré en mode d'accès et associé à un VLAN, il insère une étiquette VLAN dans l'en-tête de trame, recalcule la séquence de contrôle de trame (CRC), puis envoie la trame étiquetée par un port trunk.

Type	Priorité	CFI	VID

Figure VI.5 L'étiquette VLAN

L'étiquette VLAN se compose d'*un champ Type*, d'*un champ Priorité*, d'*un champ CFI (Canonical Format Identifier)* et d'*un champ d'ID de VLAN :*

- Type (2 octets) : appelée ID de protocole d'étiquette (TPID). Pour Ethernet, elle est définie sur une valeur hexadécimale 0x8100.
- Priorité utilisateur (3 bits) : prend en charge l'implémentation de niveaux ou de services.
- CFI (Canonical Format Identifier, 1 bit) : identificateur qui active les trames Token Ring à transmettre sur des liaisons Ethernet.

- ID de VLAN (VID, 12 bits) : numéro d'identification VLAN qui prend en charge jusqu'à 4 096 ID de VLAN.

VI.5.2 Problèmes courants avec les agrégations

Lorsque vous configurez des VLAN et des agrégations sur une infrastructure commutée, voici les types d'erreurs de configuration les plus courants par ordre d'importance :

- **Non-concordance du VLAN natif** : les ports d'agrégation sont configurés avec des VLAN natifs différents, par exemple si un port d'agrégation a défini le VLAN 99 en tant que VLAN natif alors que l'autre port a défini le VLAN 100 en tant que VLAN natif. Cette erreur de configuration génère l'affichage de notifications sur la console, entraîne le mauvais acheminement du trafic de contrôle et de gestion et représente un risque pour la sécurité.
- **Non-concordance du mode d'agrégation :** le mode d'agrégation est « désactivé » sur l'un des ports d'agrégation et « actif » sur l'autre. En présence de cette erreur de configuration, la liaison agrégée cesse de fonctionner.
- **VLAN et sous-réseaux IP** : les périphériques d'utilisateurs finaux configurés avec des adresses IP incorrectes ne bénéficient pas de la connectivité réseau. Chaque réseau local virtuel est un sous-réseau IP logique distinct. Les périphériques du VLAN doivent être configurés avec les paramètres IP appropriés.
- **VLAN autorisés sur les agrégations** : la liste des VLAN autorisés sur une agrégation n'a pas été mise à jour pour tenir compte des critères d'agrégation de VLAN actuels. Dans ce cas, l'agrégation transporte un trafic imprévu ou aucun trafic.

VI.6 Le protocole VTP

À mesure que le nombre de commutateurs augmente sur un réseau de petite ou moyenne entreprise, l'administration globale requise pour gérer des réseaux locaux virtuels (VLAN) et des agrégations en réseau devient très compliquée.

Le protocole VTP (VLAN Trunking Protocol) permet à un administrateur réseau de configurer un commutateur pour qu'il propage des configurations VLAN à d'autres commutateurs du réseau. Le protocole VTP mémorise les configurations VLAN dans la base de données VLAN appelée **vlan.dat**

VI.6.1 Avantages du protocole VTP

- Configuration VLAN homogène sur le réseau
- Surveillance et suivi précis des VLAN
- Signalement dynamique des VLAN ajoutés à l'ensemble du réseau

- Configuration dynamique d'agrégations lors de l'ajout de VLAN au réseau

VI.6.2 Composants VTP

- **Domaine VTP** : composé d'un ou de plusieurs commutateurs interconnectés. Tous les commutateurs d'un domaine partagent les détails de configuration VLAN à l'aide d'annonces VTP. Un routeur ou commutateur de couche 3 définit la limite de chaque domaine.
  Le protocole VTP vous permet de séparer votre réseau en domaines de gestion plus petits pour vous aider à réduire la gestion des réseaux locaux virtuels.
  Un domaine VTP se compose d'un ou plusieurs commutateurs interconnectés partageant le même nom de domaine VTP. Un commutateur peut être membre d'un seul domaine VTP à la fois. Tant que le nom de domaine VTP n'est pas spécifié, vous ne pouvez pas créer ni modifier de réseaux locaux virtuels sur un serveur VTP, et les informations VLAN ne sont pas propagées sur le réseau.
  Pour qu'un commutateur client ou serveur VTP participe à un réseau compatible VTP, il doit faire partie du même domaine. Lorsque les commutateurs se trouvent dans des domaines VTP différents, ils n'échangent pas de messages VTP. Un serveur VTP propage le nom de domaine VTP à tous les commutateurs à votre place.

- **Annonces VTP** : le protocole VTP utilise une hiérarchie d'annonces pour distribuer et synchroniser les configurations VLAN sur le réseau.
  Les annonces (ou messages) VTP distribuent le nom de domaine VTP et les modifications de configuration VLAN aux commutateurs compatibles VTP.

- **Modes VTP** : un commutateur peut être configuré dans un des trois modes : ***serveur, client*** ou ***transparent.*** Ces modes diffèrent dans leur utilisation pour gérer et annoncer les domaines VTP et les réseaux locaux virtuels.

- **Serveur VTP** : les serveurs VTP annoncent les paramètres VLAN de domaine VTP aux autres commutateurs compatibles dans le même domaine VTP. Les serveurs VTP stockent les informations VLAN pour l'ensemble du domaine dans la mémoire vive non volatile. Le serveur est l'emplacement sur lequel vous pouvez créer, supprimer ou renommer des réseaux locaux virtuels pour le domaine. Le mode serveur VTP constitue le mode par défaut d'un commutateur Cisco. Les serveurs VTP annoncent leurs configurations VLAN aux autres commutateurs du même domaine VTP et les synchronisent avec eux en fonction des annonces reçues sur les liaisons agrégées. Les serveurs effectuent le suivi des mises à jour via un numéro de révision de configuration. Les autres commutateurs du même domaine VTP comparent leurs numéros de

révision de configuration avec celui reçu d'un serveur VTP pour voir s'ils doivent synchroniser leurs bases de données VLAN.

- **Client VTP** : les clients VTP fonctionnent de la même manière que les serveurs VTP, sauf que vous ne pouvez pas créer, modifier, ni supprimer des réseaux locaux virtuels sur un client VTP. Un client VTP stocke uniquement les informations VLAN pour l'ensemble du domaine pendant que le commutateur est sous tension. Une réinitialisation du commutateur entraîne la suppression des informations VLAN. Vous devez configurer le **mode client VTP** sur un commutateur. En cas d'arrêt et de redémarrage, un client VTP envoie une annonce de type requête à un serveur VTP pour obtenir les informations de configuration VLAN mises à jour.

- **VTP transparent** : Les réseaux locaux virtuels créés, renommés ou supprimés sur un commutateur transparent sont uniquement associés à ce commutateur. Les commutateurs configurés en mode transparent transmettent les annonces VTP reçues sur des ports agrégés aux autres commutateurs du réseau. Les commutateurs en mode transparent VTP n'annoncent pas leur configuration VLAN et ne la synchronisent pas avec un autre commutateur. Configurez un commutateur en mode transparent VTP lorsque vous possédez des configurations VLAN qui ont une signification locale et ne doivent pas être partagées avec le reste du réseau.
  En mode transparent, les configurations VLAN sont enregistrées dans la mémoire vive non volatile (mais pas annoncées à d'autres commutateurs), de sorte que la configuration est disponible après un rechargement du commutateur. Ceci signifie que quand un commutateur en mode transparent VTP redémarre, il ne revient pas à un mode serveur VTP par défaut, mais reste en mode transparent VTP.

- **Élagage VTP** : l'élagage VTP augmente la bande passante disponible sur le réseau en limitant les transmissions diffusées sur les liaisons agrégées que le trafic doit utiliser pour atteindre les périphériques de destination. Sans élagage VTP, un commutateur répand le trafic de diffusion, de multidiffusion et de monodiffusion inconnue sur toutes les liaisons agrégées au sein d'un domaine VTP même si les commutateurs de réception peuvent les ignorer.
  L'élagage VTP évite l'inondation superflue d'informations de diffusion provenant d'un réseau local virtuel sur toutes les agrégations d'un domaine VTP. Cet élagage permet aux commutateurs de négocier les réseaux locaux virtuels affectés à des ports à l'autre extrémité d'une agrégation et, par conséquent, d'élaguer les réseaux locaux virtuels qui ne sont pas affectés à des ports sur le commutateur distant. L'élagage est désactivé par défaut. ***Vous devez activer l'élagage sur* un seul *commutateur serveur VTP du domaine.***

VI.6.3 Annonces VTP

1. Annonces de type résumé

L'annonce de type résumé contient le ***nom de domaine VTP***, ***le numéro de révision actuel***, ainsi que d'autres détails sur la configuration VTP.
Les annonces de type résumé sont envoyées :

- toutes les 5 minutes par un serveur ou client VTP pour informer les commutateurs voisins compatibles VTP du numéro de révision de configuration VTP actuel pour son domaine VTP,
- immédiatement après une configuration

2. Annonces de type sous-ensemble

Une annonce de type sous-ensemble contient des informations VLAN. Les modifications qui déclenchent l'annonce de type sous-ensemble comprennent :

- création ou suppression d'un VLAN
- arrêt ou activation d'un VLAN
- modification du nom d'un VLAN
- modification de la MTU d'un VLAN

Plusieurs annonces de type sous-ensemble peuvent être nécessaires pour mettre entièrement à jour les paramètres VLAN.

3. Annonces de type requête

Lorsqu'une annonce de type requête est envoyée à un serveur VTP du même domaine VTP, le serveur VTP répond en envoyant une annonce de type résumé, puis une annonce de type sous-ensemble.
Des annonces de type requête sont envoyées si :

- le nom de domaine VTP a été changé
- le commutateur reçoit une annonce de type résumé avec un numéro de révision de configuration supérieur au sien
- pour une raison quelconque, il manque un message d'annonce de type sous-ensemble
- le commutateur a été réinitialisé

VI.7 Le protocole STP

Dans la mesure où les réseaux sont de plus en plus importants pour les entreprises, la disponibilité de l'infrastructure réseau, qui constitue désormais un critère primordial, doit être assurée. ***La redondance*** est la solution qui permet d'obtenir la disponibilité nécessaire (figure VI.5).

La redondance de couche 2 améliore la disponibilité du réseau grâce à la mise en place de chemins alternatifs via l'ajout d'équipements et de câbles. Si les données ont la possibilité d'emprunter plusieurs chemins pour traverser le réseau, un chemin peut être coupé sans aucune incidence sur la connectivité des périphériques du réseau.

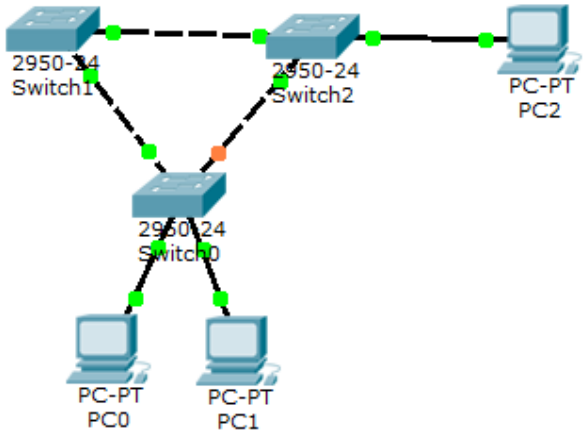


Figure VI.5 Topologie redondante

VI.7.1 Boucles de couche 2

La redondance est une composante importante de la conception hiérarchique. Bien que la redondance soit importante pour la disponibilité du réseau, il est essentiel de prendre en compte certains facteurs avant de pouvoir envisager la mise en œuvre d'une architecture redondante dans un réseau.

Lorsqu'il existe plusieurs chemins entre deux périphériques du réseau et que le protocole STP a été désactivé sur ces commutateurs, une boucle de couche 2 peut se former. Si le protocole STP est activé sur ces commutateurs (paramètre par défaut), aucune boucle de couche 2 ne se forme.

Les trames Ethernet n'ont pas de durée de vie (TTL) comme les paquets IP qui traversent les routeurs. Par conséquent, si elles ne sont pas arrêtées correctement dans un réseau commuté, elles continuent de circuler indéfiniment d'un commutateur à un autre ou jusqu'à ce qu'une liaison soit interrompue et mette fin à la boucle.

VI.7.2 Tempêtes de diffusion

Une tempête de diffusion est inévitable sur un réseau comportant des boucles. Avec la multiplication des périphériques qui envoient des trames de diffusion sur le réseau, le trafic inclus dans la boucle est de plus en plus important. À terme, il se produit une tempête de diffusion qui provoque une panne du réseau.

VI.7.3 Trames de monodiffusion en double

Les boucles ne concernent pas uniquement les trames de diffusion : lorsque des trames de monodiffusion (unicast) sont envoyées sur un réseau comportant des boucles, des trames en double peuvent parvenir à la destination finale.

VI.7.4 Algorithme Spanning Tree

La redondance améliore la disponibilité de la topologie du réseau en supprimant le risque de points de défaillance uniques dans un réseau ; par exemple, une panne d'un commutateur ou d'un câble du réseau. Lorsqu'une architecture redondante est introduite dans une conception de couche 2, des boucles et des trames en double peuvent apparaître, et les conséquences peuvent être dramatiques pour le réseau. Le protocole STP (Spanning Tree Protocol) a été conçu afin de résoudre ces problèmes.

Le protocole STP garantit l'unicité du chemin logique entre toutes les destinations sur le réseau en procédant intentionnellement au blocage des chemins redondants susceptibles d'entraîner la formation d'une boucle. Un port est considéré comme bloqué lorsqu'aucune donnée ne peut être envoyée ou reçue sur ce port, à l'exception des trames BPDU (Bridge Protocol Data Unit) qui sont employées par le protocole STP pour empêcher la formation de boucles. Le blocage des chemins redondants est essentiel pour empêcher la formation de boucles sur le réseau. Les chemins physiques sont préservés pour assurer la redondance, mais ils sont désactivés afin d'empêcher la création de boucles. Si le chemin est amené à être utilisé en cas de panne d'un commutateur ou d'un câble réseau, l'algorithme Spanning Tree (STA) recalcule les chemins et débloque les ports nécessaires pour permettre la réactivation du chemin redondant.

VI.8 Routage entre VLAN

Chaque VLAN forme un domaine de diffusion unique, de sorte que les ordinateurs de VLAN distincts ne sont pas, par défaut, en mesure de communiquer. Il existe un moyen de permettre à ces stations de communiquer ; il s'agit du routage entre VLAN.

Le routage LAN utilise généralement des routeurs avec plusieurs interfaces physiques. Chaque interface doit être connectée à un réseau distinct et configurée pour un sous-réseau différent (figure VI.6).

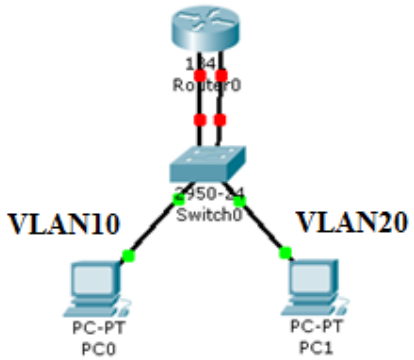


Figure VI.6 Routage inter-vlan avec plusieurs interfaces

Dans un réseau traditionnel qui utilise plusieurs VLAN pour segmenter le trafic en domaines de diffusion logiques, le routage s'effectue en connectant différentes interfaces de routeur physique à différents ports de commutateur physiques. Les ports de commutateur se connectent au routeur en mode d'accès ; dans ce mode, des VLAN statiques différents sont affectés à chaque interface de port. Chaque interface de commutateur serait ainsi attribuée à un VLAN statique différent. Chaque interface de routeur peut alors accepter le trafic du VLAN associé à l'interface de commutateur à laquelle elle est connectée, et le trafic peut être acheminé vers les autres VLAN connectés aux autres interfaces.

Le routage traditionnel entre VLAN exige plusieurs interfaces physiques sur le routeur et le commutateur. Cependant, toutes les configurations de routage entre VLAN ne nécessitent pas plusieurs interfaces physiques. Certains logiciels de routeur permettent de configurer des interfaces de routeur comme liaisons agrégées, créant ainsi de nouvelles possibilités pour le routage entre VLAN (figure VI.7).

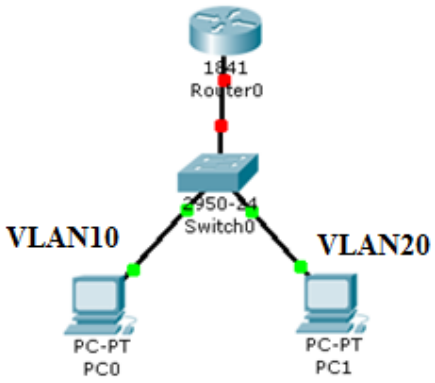


Figure VI.7 Routage en mode agrégation

L'interface du routeur est configurée pour fonctionner comme liaison agrégée et est connectée à un port du commutateur configuré en mode d'agrégation. Le routeur effectue le routage entre VLAN en acceptant le trafic étiqueté VLAN sur l'interface agrégée provenant du commutateur adjacent et en effectuant le routage en interne entre les VLAN à l'aide de sous-interfaces. Le routeur transfère alors le trafic acheminé (étiqueté VLAN pour le VLAN de destination) depuis la même interface physique.

Les sous-interfaces sont des interfaces virtuelles multiples, associées à une interface physique. Ces sous-interfaces sont configurées sur un routeur configuré de manière indépendante avec une adresse IP et une affectation VLAN pour fonctionner sur un VLAN spécifique. Les sous-interfaces sont configurées pour différents sous-réseaux correspondant à leur affectation VLAN afin de faciliter le routage logique avant que les trames de données soient étiquetées VLAN et renvoyées depuis l'interface physique.

Commutateur multicouche:

Certains commutateurs peuvent effectuer des fonctions de couche 3, remplaçant la nécessité pour des routeurs dédiés d'effectuer un routage de base sur un réseau. Les commutateurs multicouches sont en mesure d'effectuer un routage entre VLAN.

Pour permettre à un commutateur multicouche d'effectuer des fonctions de routage, les interfaces VLAN sur le commutateur doivent être configurées avec les adresses IP appropriées correspondant au sous-réseau auquel est associé le VLAN sur le réseau. Le routage IP doit également être activé sur le commutateur multicouche.

Remarque : La technologie d'interface virtuelle de commutateur (SVI, Switch Virtual Interface) permet à un commutateur de couche 3 de router des transmissions entre des VLAN.

Une interface SVI est une interface logique configurée pour un VLAN spécifique. Vous devez configurer une interface SVI pour un VLAN si vous voulez assurer le routage entre des VLAN ou fournir une connectivité d'hôte IP au commutateur. Par défaut, une interface SVI est créée pour le VLAN par défaut (VLAN 1) pour permettre l'administration à distance du commutateur.

Un commutateur de couche 3 a la capacité de router des transmissions entre des VLAN. La procédure est la même que pour la communication inter-VLAN utilisant un routeur distinct, à la différence que les interfaces SVI jouent le rôle des interfaces du routeur pour router les données entre des VLAN.