Exonet - Ressources mutualisées en réseau

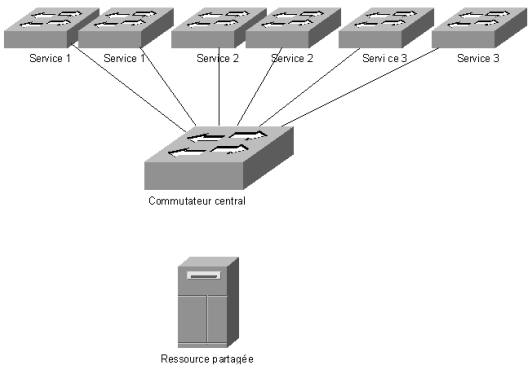
Description du thème

Propriétés	Description
Intitulé long	Ressources mutualisées dans une architecture de réseaux virtuels.
Formation concernée	BTS Informatique de gestion – option ARLE BTS services informatiques aux organisations, parcours SISR (solutions d'infrastructures, systèmes et réseaux)
Présentation	Étude de huit solutions pour partager l'accès à un serveur de fichiers dans une architecture optimisée et sécurisée par la mise en place de réseaux virtuels. Les dernières solutions sont réalisées avec des fonctions avancées : VLAN asymétriques ou solutions propriétaires.
Modules	SISR2 – Conception des infrastructures réseaux
Activités	A3.2.1 Installation et configuration d'éléments d'infrastructure
Compétences ; Savoir-faire	BTS SIO : Justifier le choix d'une solution technique Configurer les éléments d'interconnexion permettant de séparer les flux BTS IG : C22 Installer et configurer un réseau C33 Assurer la sécurité d'un réseau C35 Actualiser une solution informatique et améliorer ses performances
Pré-requis	Commutation VLAN routage filtrage
Mots-clés	VLAN, 802.1q, Vlan asymétrique, filtrage, routage, interface virtuelle
Durée	1h30 à 2h
Auteur(es)	Daniel Régnier (avec la précieuse relecture de Freddy Didier)
Version	v 1.0
Date de publication	Avril 2011

Contexte de travail

Une entreprise souhaite mutualiser un serveur de fichiers entre plusieurs services dans une architecture construite avec des VLAN. Toute communication entre les services est interdite, mais les postes de chaque service doivent accéder à ce serveur partagé (ressource mutualisée).Les commutateurs des services sont reliés à un commutateur central.

Schéma simplifié du réseau :



L'affectation des ports sur le commutateur central est la suivante :

Ports	Affectation
1 à 2	Service 1
3 à 4	Service 2
5 à 6	Service 3
7 à 12	libres

L'administrateur veut étudier plusieurs solutions pour réaliser cette mutualisation. Ces solutions varient en fonction du type de commutateur central, de l'interface réseau de la ressource partagée et de l'utilisation éventuelle d'un routeur. Des fonctionnalités avancées de certains commutateurs pour la gestion des vlan sont présentées dans certaines solutions.

A partir de ces différents matériels, l'administrateur a déterminé huit configurations différentes. Il vous demande de les compléter.

Les contraintes :

- Interdire la communication entre les services.
- Tous les services accèdent à la ressource mutualisée (un serveur de fichiers).
- La communication au sein même d'un service n'est pas obligatoire.
- Les réseaux IP éventuels seront : 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16, 10.4.0.0/16, 10.5.0.0/16, 10.6.0.0/16

Travail à faire :

Pour chaque solution présentée dans les pages 3 à 7, compléter la partie configuration en spécifiant le nombre de Vlan nécessaires, l'affectation des ports du commutateur central, la ou les adresses des réseaux IP utilisés, la configuration IP de la ressource mutualisée et la configuration IP des éléments spécifiés (postes des services, routeur éventuel).

Chaque solution présente des caractéristiques différentes en termes d'évolutivité, de configuration, d'administration et de performance.

Travail à faire :

Pour chaque solution présentée dans les pages 3 à 7, définir les éventuels avantages et/ou inconvénients.

1) Solution N°1

Matériel disponible :

- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose de trois interfaces non compatibles 802.1q.

Configuration à compléter :

Principe :

Nombre de vlan :

Affectation des ports du commutateur dans un vlan

Ports	Vlan	802.1q activé	Affectation
1 à 2			Service 1
3 à 4			Service 2
5 à 6			Service 3
7			
8			
9			
10			
11			

Réseaux IP utilisés :

Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) :

Passerelle éventuelle des postes de chaque service :

2) Solution N°2

Matériel disponible :

- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface compatible 802.1q.

Configuration à compléter :

Principe :

Nombre de vlan :

Affectation des ports du commutateur dans un vlan

Ports	Vlan	802.1q activé	Affectation
1 à 2			Service 1
3 à 4			Service 2
5 à 6			Service 3
7			
8			
9			
10			
11			

Réseaux IP utilisés :

Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) :

Passerelle éventuelle des postes de chaque service :

3) Solution N°3

Matériel disponible :

- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.
- Routeur filtrant avec quatre interfaces.

Configuration à compléter :
Principe :

Nombre de vlan :

Affectation des ports du commutateur dans un vlan

Ports	Vlan	802.1q activé	Affectation
1 à 2			Service 1
3 à 4			Service 2
5 à 6			Service 3
7			
8			
9			
10			
11			

Réseaux IP utilisés :
Configuration IP du Routeur filtrant :
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) :
Passerelle éventuelle des postes de chaque service :

Règles de filtrage du routeur :

Interface	Ip source	Port source	Ip destination	Port dest.	Protocole	Action

4) Solution N°4

Matériel disponible :

- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.
- Routeur filtrant avec une interface compatible 802.1q.

Configuration à compléter :
Principe :

Nombre de vlan :
Affectation des ports du commutateur dans un vlan

Ports	Vlan	802.1q activé	Affectation
1 à 2			Service 1
3 à 4			Service 2
5 à 6			Service 3
7			
8			
9			
10			
11			

Réseaux IP utilisés :
Configuration IP du Routeur filtrant :
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) :
Passerelle éventuelle des postes de chaque service :

Règles de filtrage du routeur :

Interface	Ip source	Port source	Ip destination	Port dest.	Protocole	Action

5) Solution N°5

Matériel disponible :

- Commutateur de niveau 3 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.

Configuration à compléter :
Principe :

Nombre de vlan :

Affectation des ports du commutateur dans un vlan

Ports	Vlan	802.1q activé	Affectation
1 à 2			Service 1
3 à 4			Service 2
5 à 6			Service 3
7			
8			
9			
10			
11			

Réseaux IP utilisés :
Configuration IP du commutateur routeur :
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) :
Passerelle éventuelle des postes de chaque service :

Règles de filtrage du commutateur de niveau 3 :

Interface	Ip source	Port source	Ip destination	Port dest.	Protocole	Action

6) Solution N°6

Matériel disponible :

- Commutateur de niveau 2, gère les vlan asymétriques.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.

Vlan asymétriques : Les trames reçues sur un port appartiennent à un seul et même VLAN ; par contre, un port peut émettre des trames de différents VLAN. Les trames ne sont pas étiquetées. Exemple : un port reçoit une trame et l'affecte toujours au vlan 1; il peut diffuser des trames des vlan 1, 10 ou 20.

Configuration à compléter :
Principe :

Nombre de vlan :

Affectation des ports du commutateur dans un vlan

Ports	Vlan affecté	Vlan diffusé	Affectation
1 à 2			Service 1
3 à 4			Service 2
5 à 6			Service 3
7			
8			
9			
10			
11			

Réseaux IP utilisés :
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) :
Passerelle éventuelle des postes de chaque service :

7) Solution N°7

Matériel disponible :

- Commutateur de niveau 2, gère les ports "isolated" et "promiscuous" (solution propriétaire Cisco : PVLAN).
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.

Ports "isolated" : ils ne peuvent émettre des trames que vers des ports "promiscuous" du même vlan.
Ports "promiscuous" : ils peuvent émettre des trames vers tous les ports ("isolated" et "promiscuous") du même vlan.

Configuration à compléter :
Principe :

Nombre de vlan :

Affectation des ports du commutateur dans un vlan

Ports	Vlan	Type port	Affectation
1 à 2			Service 1
3 à 4			Service 2
5 à 6			Service 3
7			
8			
9			
10			
11			

Réseaux IP utilisés :
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) :
Passerelle éventuelle des postes de chaque service :

8) Solution N°8

Matériel disponible :

- Commutateur de niveau 3, gère les vlan "protected" (solution propriétaire Allied Telesyn).
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.

Vlan "protected" : Un port d'un Vlan "protected" ne peut communiquer avec un autre port du même Vlan. La communication ne peut se faire qu'au niveau 3, vers un autre Vlan.

Configuration à compléter :

Principe :

Nombre de vlan :

Vlan "protected" :

Vlan non "protected" :

Affectation des ports du commutateur dans un vlan

Ports	Vlan	Affectation
1 à 2		Service 1
3 à 4		Service 2
5 à 6		Service 3
7		
8		
9		
10		
11		

Réseaux IP utilisés :

Configuration IP du commutateur routeur :

Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) :

Passerelle éventuelle des postes de chaque service :

Règles de filtrage du commutateur de niveau 3 :

Interface	Ip source	Port source	Ip destination	Port dest.	Protocole	Action

Corrigé

Pour information, des extraits de documents sur les fonctionnalités avancées des commutateurs pour la gestion des vlan, vues dans les solutions 7,8 et 9, sont présentés dans les annexes 1, 2 et 3 du corrigé.

Pour chaque solution présentée dans les pages 3 à 7, compléter la partie configuration en spécifiant le nombre de Vlan nécessaires, l'affectation des ports du commutateur central, la ou les adresses des réseaux IP utilisés, la configuration IP de la ressource mutualisée et la configuration IP des éléments spécifiés (postes des services, routeur éventuel).

1) Solution N°1

Matériel disponible :

- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose de trois interfaces non compatibles 802.1q.

Configuration à compléter :

Principe : La ressource est dans chaque Vlan. Chaque interface physique de la ressource est connectée sur un port du commutateur et associée à un vlan différent. La ressource possède une adresse IP compatible avec chaque service.

Nombre de vlan : 3

Affectation des ports du commutateur dans un vlan

Ports	Vlan	802.1q activé	Affectation
1 à 2	1	Non	Service 1
3 à 4	2	Non	Service 2
5 à 6	3	Non	Service 3
7	1	Non	Interface 1 Ressource mutualisée
8	2	Non	Interface 2 Ressource mutualisée
9	3	Non	Interface 3 Ressource mutualisée
10		Non	
11		Non	

Réseaux IP utilisés : 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16

Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) :10.1.0.1/16, 10.2.0.1/16, 10.3.0.1/16

Passerelle éventuelle des postes de chaque service : Non

2) Solution N°2

Matériel disponible :

- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface compatible 802.1q.

Configuration à compléter :

Principe : La ressource est dans chaque Vlan. L'interface physique de la ressource est connectée sur un port 802.1q, elle est associée à trois interfaces virtuelles (802.1q). La ressource possède une adresse IP compatible avec chaque service.

Nombre de vlan : 3

Affectation des ports du commutateur dans un vlan

Ports	Vlan	802.1q activé	Affectation
1 à 2	1	Non	Service 1
3 à 4	2	Non	Service 2
5 à 6	3	Non	Service 3
7	1,2,3	Oui	Ressource mutualisée
8		Non	
9		Non	
10		Non	
11		Non	

Réseaux IP utilisés : 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) : 10.1.0.1/16, 10.2.0.1/16, 10.3.0.1/16
Passerelle éventuelle des postes de chaque service : Non

3) Solution N°3

Matériel disponible :

- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.
- Routeur filtrant avec quatre interfaces.

Configuration à compléter :
Principe : La ressource est dans un vlan différent. La communication avec les services est réalisée via le routeur. Chaque interface du routeur est connectée sur un port du commutateur et associée à un vlan différent. Il a une adresse IP compatible avec chaque Vlan. Le trafic entre les services est bloqué par les règles de filtrage.

Nombre de vlan : 4

Affectation des ports du commutateur dans un vlan

Ports	Vlan	802.1q activé	Affectation
1 à 2	1	Non	Service 1
3 à 4	2	Non	Service 2
5 à 6	3	Non	Service 3
7	4	Non	Ressource mutualisée
8	1	Non	Interface 1 routeur
9	2	Non	Interface 2 routeur
10	3	Non	Interface 3 routeur
11	4	Non	Interface 4 routeur

Réseaux IP utilisés : 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16, 10.4.0.0/16
Configuration IP du Routeur filtrant : 10.1.0.1/16, 10.2.0.1/16, 10.3.0.1/16, 10.4.0.1/16
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) : 10.4.0.2/16 (passerelle : 10.4.0.1)
Passerelle éventuelle des postes de chaque service : 10.1.0.1, 10.2.0.1, 10.3.0.1

Règles de filtrage du routeur :

Interface	Ip source	Port source	Ip destination	Port dest.	Protocole	Action
*	*	*	10.4.0.2/32	*	*	Autorisé
*	10.4.0.2/32	*	*	*	*	Autorisé
*	*	*	*	*	*	Bloqué

4) Solution N°4

Matériel disponible :

- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.
- Routeur filtrant avec une interface compatible 802.1q.

Configuration à compléter :

Principe : La ressource est dans un vlan différent. La communication avec les services est réalisée via le routeur. L'interface du routeur est connectée sur un port 802.1q, elle est associée à quatre interfaces virtuelles en activant 802.1q. Le routeur possède une adresse IP compatible avec chaque Vlan. Le trafic entre les services est bloqué par les règles de filtrage.

Nombre de vlan : 4

Affectation des ports du commutateur dans un vlan

Ports	Vlan	802.1q activé	Affectation
1 à 2	1	Non	Service 1
3 à 4	2	Non	Service 2
5 à 6	3	Non	Service 3
7	4	Non	Ressource mutualisée
8	1,2,3,4	Oui	Interface routeur
9		Non	
10		Non	
11		Non	

Réseaux IP utilisés : 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16, 10.4.0.0/16
Configuration IP du Routeur filtrant : 10.1.0.1/16, 10.2.0.1/16, 10.3.0.1/16, 10.4.0.1/16
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) : 10.4.0.2/16 (passerelle : 10.4.0.1)
Passerelle éventuelle des postes de chaque service : 10.1.0.1, 10.2.0.1, 10.3.0.1

Règles de filtrage du routeur :

Interface	Ip source	Port source	Ip destination	Port dest.	Protocole	Action
*	*	*	10.4.0.2/32	*	*	Autorisé
*	10.4.0.2/32	*	*	*	*	Autorisé
*	*	*	*	*	*	Bloqué

5) Solution N°5

Matériel disponible :

- Commutateur de niveau 3 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.

Configuration à compléter :

Principe : La ressource est dans un vlan différent. La communication avec les services est réalisée via le commutateur- routeur. Le commutateur-routeur a une interface virtuelle pour chaque Vlan et une adresse IP compatible avec chaque Vlan. Le trafic entre les services est bloqué par les règles de filtrage.

Nombre de vlan : 4

Affectation des ports du commutateur dans un vlan

Ports	Vlan	802.1q activé	Affectation
1 à 2	1	Non	Service 1
3 à 4	2	Non	Service 2
5 à 6	3	Non	Service 3
7	4	Non	Ressource mutualisée
8		Non	
9		Non	
10		Non	
11		Non	

Réseaux IP utilisés : 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16, 10.4.0.0/16
Configuration IP du commutateur routeur : 10.1.0.1/16, 10.2.0.1/16, 10.3.0.1/16, 10.4.0.1/16
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) : 10.4.0.2/16 (passerelle : 10.4.0.1)
Passerelle éventuelle des postes de chaque service : 10.1.0.1, 10.2.0.1, 10.3.0.1

Règles de filtrage du commutateur de niveau 3 :

Interface	Ip source	Port source	Ip destination	Port dest.	Protocole	Action
*	*	*	10.4.0.2/32	*	*	Autorisé
*	10.4.0.2/32	*	*	*	*	Autorisé
*	*	*	*	*	*	Bloqué

6) Solution N°6
Matériel disponible :

- Commutateur de niveau 2, gère les vlan asymétriques.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.

Vlan asymétriques : Les trames reçues sur un port appartiennent à un seul et même VLAN ; par contre, un port peut émettre des trames de différents VLAN. Les trames ne sont pas étiquetées. Exemple : un port reçoit une trame et l'affecte toujours au vlan 1; il peut diffuser des trames des vlan 1, 10 ou 20.

Voir annexe 1: Extrait de IEEE Std 802.1Q, Standards for Local and metropolitan area networks—Virtual Bridged Local Area Networks, Annex B.1.3 Asymmetric VLANs.

Configuration à compléter :
Principe : La ressource est dans un vlan différent. Le port sur lequel est connectée la ressource est affecté au Vlan 4 et peut diffuser les vlan 1, 2, 3 et 4. Les ports des services sont affectés à leur vlan et peuvent diffuser aussi sur le vlan 4. Un seul réseau IP est suffisant.

Nombre de vlan : 4

Affectation des ports du commutateur dans un vlan

Ports	Vlan affecté	Vlan diffusé	Affectation
1 à 2	1	1,4	Service 1
3 à 4	2	2,4	Service 2
5 à 6	3	3,4	Service 3
7	4	1,2,3,4	Ressource mutualisée
8			
9			
10			
11			

Réseaux IP utilisés : 10.1.0.0/16
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) : 10.1.0.1/16 (passerelle : Non)
Passerelle éventuelle des postes de chaque service : Non

7) Solution N°7
Matériel disponible :

- Commutateur de niveau 2, gère les ports "isolated" et "promiscuous" (solution propriétaire Cisco : PVLAN).
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.

Ports "isolated" : ils ne peuvent émettre des trames que vers des ports "promiscuous" du même vlan.
Ports "promiscuous" : ils peuvent émettre des trames vers tous les ports ("isolated" et "promiscuous") du même vlan.

Voir annexe 2 : Extrait de la documentation Cisco, PVLAN

Configuration à compléter :
Principe : Un seul Vlan est utilisé et un seul réseau IP. Le port sur lequel est connectée la ressource est de type "promiscuous", il peut émettre vers tous les services, les ports sur lesquels sont connectés les services sont de type "isolated", ils ne peuvent émettre que vers la ressource.

Nombre de vlan : 1

Affectation des ports du commutateur dans un vlan

Ports	Vlan	Type port	Affectation
1 à 2	1	isolated	Service 1
3 à 4	1	isolated	Service 2
5 à 6	1	isolated	Service 3
7	1	promiscuous	Ressource mutualisée
8			
9			
10			
11			

Réseaux IP utilisés : 10.1.0.0/16
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) : 10.1.0.1/16 (passerelle : Non)
Passerelle éventuelle des postes de chaque service : Non

8) Solution N°8
Matériel disponible :

- Commutateur de niveau 3, gère les vlan "protected" (solution propriétaire Allied Telesyn).
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.

Vlan "protected" : Un port d'un Vlan "protected" ne peut communiquer avec un autre port du même Vlan. La communication ne peut se faire qu'au niveau 3, vers un autre Vlan.

Voir annexe 3 : Extrait de la documentation Allied Telesyn

Configuration à compléter :
Principe : Les services sont dans le même Vlan "protected". La ressource est dans un autre Vlan. La communication avec la ressource est réalisée via le commutateur- routeur. Le commutateur-routeur a une interface virtuelle pour chaque Vlan et une adresse IP compatible avec chaque Vlan. La communication entre les services étant impossible, il n'y a pas de règles de filtrage.

Nombre de vlan : 2
Vlan "protected" : 1
Vlan non "protected" : 2

Affectation des ports du commutateur dans un vlan

Ports	Vlan	Affectation
1 à 2	1	Service 1
3 à 4	1	Service 2
5 à 6	1	Service 3
7	2	Ressource mutualisée
8		
9		
10		
11		

Réseaux IP utilisés : 10.1.0.0/16, 10.2.0.0/16
Configuration IP du commutateur routeur : 10.1.0.1/16, 10.2.0.1/16
Configuration IP de la ressource mutualisée (IP et passerelle éventuelle) : 10.2.0.2/16 (passerelle : 10.2.0.1)
Passerelle éventuelle des postes de chaque service : 10.1.0.1

Règles de filtrage du commutateur de niveau 3 : AUCUNE

TRAVAIL A FAIRE :
Pour chaque solution présentée dans les pages 3 à 7, définir les éventuels avantages et/ou inconvénients.

1) Solution N°1
Matériel disponible :
- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose de trois interfaces non compatibles 802.1q.

Principe : La ressource est dans chaque Vlan. Chaque interface physique de la ressource est connectée sur un port du commutateur et associée à un vlan différent. La ressource possède une adresse IP compatible avec chaque service.

Avantages :
- Très performant, la ressource a un lien direct commuté avec chaque service, pas de routage.

Inconvénients :
- Très peu évolutif, si le nombre de services (Vlan) augmente, la ressource sera limitée en nombre d'interface et le nombre de ports du commutateur limite aussi cette solution.

2) Solution N°2
Matériel disponible :
- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface compatible 802.1q.

Principe : La ressource est dans chaque Vlan. L'interface physique de la ressource est connectée sur un port 802.1q, elle est associée à trois interfaces virtuelles (802.1q). La ressource possède une adresse IP compatible avec chaque service.

Avantages :
- Très évolutif, le nombre de services (Vlan) n'est pas un problème, pas de routage.

Inconvénients :
- Le lien (ressource-commutateur) est très sollicité, attention aux performances.

3) Solution N°3
Matériel disponible :
- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.
- Routeur filtrant avec quatre interfaces.

Principe : La ressource est dans un vlan différent. La communication avec les services est réalisée via le routeur. Chaque interface du routeur est connectée sur un port du commutateur et associée à un vlan différent. Il a une adresse IP compatible avec chaque Vlan. Le trafic entre les services est bloqué par les règles de filtrage.

Avantages :
- Permet de conserver un commutateur de niveau 2 !

Inconvénients :
- Nécessite de mettre en place le routage et les règles de filtrage pour la contrainte N°1.
- Très peu évolutif, si le nombre de services (Vlan) augmente, le routeur sera limité en nombre d'interface et le nombre de ports du commutateur limite aussi cette solution.

4) Solution N°4

Matériel disponible :

- Commutateur de niveau 2 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.
- Routeur filtrant avec une interface compatible 802.1q.

Principe : La ressource est dans un vlan différent. La communication avec les services est réalisée via le routeur. L'interface du routeur est connectée sur un port 802.1q, elle est associée à quatre interfaces virtuelles en activant 802.1q. Le routeur possède une adresse IP compatible avec chaque Vlan. Le trafic entre les services est bloqué par les règles de filtrage.

Avantages :

- Permet de conserver un commutateur de niveau 2 !

Inconvénients :

- Nécessite de mettre en place le routage et les règles de filtrage pour la contrainte N°1,
- Le lien (routeur-commutateur) est très sollicité, attention aux performances.

5) Solution N°5

Matériel disponible :

- Commutateur de niveau 3 qui gère les Vlan compatibles 802.1q.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.

Principe : La ressource est dans un vlan différent. La communication avec les services est réalisée via le commutateur- routeur. Le commutateur-routeur a une interface virtuelle pour chaque Vlan et une adresse IP compatible avec chaque Vlan. Le trafic entre les services est bloqué par les règles de filtrage.

Avantages :

- Très évolutif, beaucoup moins limité par le nombre de services (Vlan), pas de ports utilisés par le routage.

Inconvénients :

- Nécessite de mettre en place le routage et les règles de filtrage pour la contrainte N°1,

6) Solution N°6

Matériel disponible :

- Commutateur de niveau 2, gère les vlan asymétriques.
- Ressource à mutualiser dispose d'une interface non compatible 802.1q

Principe : La ressource est dans un vlan différent. Le port sur lequel est connecté la ressource est affecté au Vlan 4 et peut diffuser les vlan 1, 2 et 3. Les ports des services sont affectés à leur vlan et peuvent diffuser sur le vlan 4. Un seul réseau IP est suffisant.

Avantages :

- Un seul réseau IP (pas de routage).

Inconvénients :

- Semble plus complexe à comprendre, la configuration du commutateur est plus délicate.

7) Solution N°7

Matériel disponible :

- Commutateur de niveau 2, gère les ports "isolated" et "promiscuous" (solution propriétaire Cisco : PVLAN).
- Ressource à mutualiser dispose d'une interface non compatible 802.1q.

Configuration à compléter :

Principe : Un seul Vlan est utilisé et un seul réseau IP. Le port sur lequel est connectée la ressource est de type "promiscuous", il peut émettre vers tous les services, les ports sur lesquels sont connectés les services sont de type "isolated", ils ne peuvent émettre que vers la ressource.

Avantages :

- Un seul réseau IP (pas de routage).
- Un seul Vlan, quelque soit le nombre de service à segmenter.

Inconvénients :

- Semble plus complexe à comprendre. La communication au sein d'un même service est impossible via les ports du commutateur central (nouvelle contrainte).

8) Solution N°8

Matériel disponible :

- Commutateur de niveau 3, gère les vlan "protected".
- Ressource à mutualiser dispose d'une interface non compatible 802.1q

Principe : Les services sont dans le même Vlan "protected". La ressource est dans un autre Vlan. La communication avec la ressource est réalisée via le commutateur- routeur. Le commutateur-routeur a une interface virtuelle pour chaque Vlan et une adresse IP compatible avec chaque Vlan. La communication entre les services étant impossible, il n'y a pas de règles de filtrage.

Avantages :

- Configuration rapide des ports affectés au Vlan "protected".
- Pas de règle de filtrage malgré le routage.
- Un seul Vlan et un seul réseau IP pour tous les services, quelque soit le nombre de services à segmenter.

Inconvénients :

- La communication au sein d'un même service est impossible via les ports du commutateur central (nouvelle contrainte).

Sources d'information complémentaires

Document 1 : Extrait de IEEE Std 802.1Q, Standards for Local and metropolitan area networks Virtual Bridged Local Area Networks (http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf)

Annex B.1.3 Asymmetric VLANs (informative), page 228
A primary example of the requirement for Shared VLAN Learning is found in "asymmetric" uses of VLANs. Under normal circumstances, a pair of devices communicating in a VLAN environment will both send and receive using the same VLAN; however, there are some circumstances in which it is convenient to make use of two distinct VLANs, one used for A to transmit to B: the other used for B to transmit to A. An example of such an application of VLANs is shown in Figure 11-1. Note that:
a) In the example, the server and both clients are assumed to be VLAN-unaware devices, i .e., they transmit and receive untagged frames only;
b) The ingress classification rules assumed by the example are as defined in this standard, i.e., Portbased classification only;
c) The configuration shown can only be achieved by management configuration of appropriate values in Static VLAN Registration Entries (8.11.9) in order to configure the indicated member sets and untagged sets.

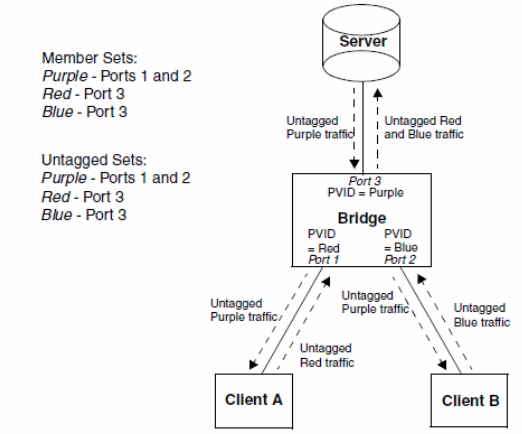


Figure B-4—Asymmetric VLAN use: "multi-netted server"

In the example, Port-based tagging and an asymmetric VLAN configuration is used in order to permit Clients A and B access to a common server, but to prohibit Clients A and B from talking to each other. Examples of where this type of configuration might be required are if the clients are on distinct IP subnets, or if there is some confidentiality-related need to segregate traffic between the clients.

Client A transmits to the server via Port 1, which will classify this traffic as belonging to VLAN Red; the Bridge therefore learns Client A's MAC Address on Port 1 in VLAN Red. The Server transmits its responses to Client A via Port 3, which classifies the return traffic as belonging to VLAN Purple.

Document 2 : Extrait de la documentation Cisco, PVLAN
(http://www.cisco.com/en/US/tech/tk389/tk814/tk840/tsd_technology_support_sub-protocol_home.html)

PVLANs provide layer 2 isolation between ports within the same broadcast domain. There are three types of PVLAN ports:
Promiscuous— A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.
Isolated— An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is forwarded only to promiscuous ports.
Community— Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

Annexe 3 : Extrait de la documentation Allied Telesyn (Allied Telesyn switch AT-8624T)

Protected VLANs : If a VLAN is protected, Layer 2 traffic between ports that are members of a protected VLAN is blocked. Traffic can be Layer 3 switched to another VLAN. This feature prevents members of a protected VLAN from communicating with each other yet still allows members to access another network. Layer 3 Routing between ports in a protected VLAN can be prevented by adding a Layer 3 filter. The protected VLAN feature also allows all of the members of the protected VLAN to be in the same subnet. A typical application is a hotel installation where each room has a port that can be used to access the Internet. In this situation it is undesirable to allow communication between rooms.