

Exonet N°78

Description

Propriétés	Description
Intitulé long	Comprendre les principes de base des VLAN
Formation concerné	BTS Services informatiques aux organisations
Public concerné	BTS Services informatiques aux organisations
Matière	SISR2 – Conception des infrastructures réseaux
Compétences	Configurer les éléments d'interconnexion permettant de séparer les flux
Savoirs	Modèles de référence associés aux architectures réseaux
Objectifs	Comprendre les principes de base des VLAN
Pré-requis	Commutation routage VLAN
Mots-clés	VLAN ARP ICMP 802.1d 802.1q
Auteur(es)	Roger Sanchez
Version	1.1
Date de publication	14-09-2004
Date de mise à jour	02-05-2005

Énoncé

L'administrateur du réseau d'une entreprise souhaite optimiser l'utilisation de la bande passante.

L'entreprise est répartie sur différents étages d'un bâtiment. Chaque étage est consacré à une fonction particulière.

Le réseau de l'entreprise est un réseau Ethernet commuté à 100Mb/s. A chaque étage correspond un commutateur et une adresse de sous-réseau IP.

Les commutateurs sont reliés par des liens fibres optiques. Deux routeurs placés à l'étage 1 et 2 permettent d'interconnecter les différents réseaux IP.

Les commutateurs permettent de définir des VLAN de niveau 1, 2 ou 3. Ils peuvent gérer, si nécessaire, le protocole 802.1d et le protocole 802.1q sur les ports fibres optiques (*trunking*). On peut dupliquer sur un port du commutateur les flux circulants sur un autre port (port *mirroring*).

L'administrateur dispose d'un ordinateur portable sur lequel il a installé un analyseur de trames qui lui permet de capturer toutes les trames parvenant à sa carte réseau. Cet analyseur est couplé avec un logiciel d'étude des flux réseaux. Il va étudier ceux-ci avant de mettre en œuvre une solution basée sur des VLAN.

Lorsque l'étude de l'administrateur commence il n'y a pas de dysfonctionnement sur le réseau, tous les postes communiquent entre eux dans un réseau IP ou entre les réseaux IP.

L'[annexe 1](#) représente un schéma non exhaustif du réseau.

L'[annexe 2](#) présente les choix de l'administrateur pour répondre à ses objectifs.

L'[annexe 3](#) rappelle succinctement les concepts utilisés par cet exercice.

Questions

Première partie : étude des flux

Pour étudier les flux l'administrateur va connecter successivement son portable sur chaque commutateur

L'administrateur a installé son portable sur le port C3e3 du commutateur C3 et activé son analyseur. Il demande à un collègue d'exécuter la commande suivante à partir du poste 192.168.1.1 :

```
ping 192.168.3.1
```

A l'issue de cette commande l'analyseur de trames a capturé trois trames ARP "request", aucune trame ARP "reply" et aucun échange ICMP.

1. Quels sont les entêtes MAC des trois trames ARP (request) capturées par le poste de l'administrateur ?
2. Pourquoi les trames ARP "reply" et l'échange ICMP n'ont-ils pas été capturés ?
3. Proposer une solution qui permette de capturer tous les flux entrant sur le commutateur C3.
4. Quel serait l'en-tête MAC de la trame ICMP (echo) éventuellement capturée par la solution précédente ? Quelles seraient les adresses IP du paquet encapsulé dans cette trame ?

Rappel : 0806 est le code hexa correspondant au type d'une trame ARP. Le protocole ICMP est encapsulé dans un paquet IP dont la trame est de type 0800.

Deuxième partie : choix d'une solution VLAN

A l'issue de l'étude de flux, l'administrateur constate que 90% des flux se font à l'intérieur d'un même réseau IP et seulement 10% concerne des flux inter-réseaux IP.

Les étages sont organisés par fonction dans l'entreprise et il n'y a pas de mobilité des postes informatiques entre les étages.

L'administrateur décide donc de mettre en place une solution simple basée sur des VLAN de niveau 1, et de ne pas activer les protocoles 802.1d et 802.1q sur les commutateurs

1. L'administrateur n'a pas mis en œuvre le protocole 802.1d. Pourquoi ?
2. L'administrateur n'a pas mis en œuvre le protocole 802.1q. Pourquoi ?

Troisième partie : mise en œuvre d'un VLAN par port (niveau 1)

L'affectation des différents ports des commutateurs aux VLAN est décrite par l'[annexe 2](#).

L'administrateur décide de tester sa configuration. Son portable est connecté au commutateur 3 et capture tous les flux arrivant sur le port c3f1.

Il demande à un collègue d'exécuter la commande suivante à partir tout d'abord du poste **192.168.2.1**:

```
ping 192.168.3.1
```

Cette commande s'exécute parfaitement.

Puis il demande à un autre collègue d'exécuter la commande suivante à partir du poste **192.168.1.1**:

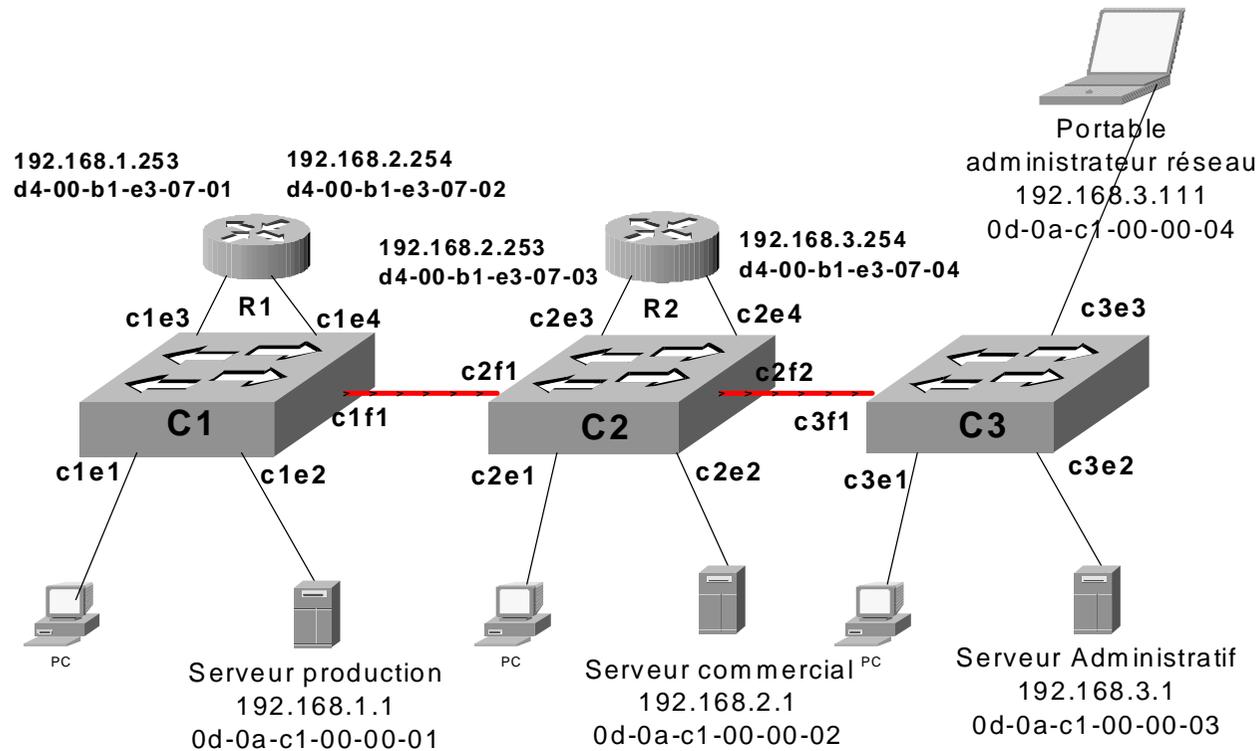
```
ping 192.168.3.1
```

La réponse à cette commande est : "délai d'attente dépassé".

1. Quelles sont les trames capturées par le portable de l'administrateur lors de la première commande ?
2. Quelle est la cause de l'échec de la deuxième commande ? Proposer une solution.

Annexes

Annexe 1 : schéma non exhaustif du réseau



Légende : c1e1 signifie : premier port Ethernet du commutateur C1. c1f1 signifie premier port fibre optique du commutateur c1.

Configuration :

Tous les masques de sous-réseau sont égaux à 255.255.255.0

Les postes du réseau production ont comme passerelle par défaut : 192.168.1.253.

Les postes du réseau commercial ont comme passerelle par défaut : 192.168.2.253.

Les postes du réseau administratif ont comme passerelle par défaut : 192.168.3.254.

Annexe 2 : Affectation des ports aux VLAN

L'administrateur a déclaré trois VLAN identifiés par les chiffres 1 2 et 3. Il a réparti les ports sur ce VLAN comme le montre le tableau suivant.

VLAN 1	VLAN 2	VLAN 3
C1e1	C2e1	C2e4
C1e2	C2e2	C2f2
C1e3	C2e3	C3f1
C1f1	C2f1	C3e1
	C1e4	C3e2
		C3e3

Annexe 3 : Rappels sur les VLAN

Définition : un VLAN permet de créer des domaines de diffusion gérés par les commutateurs. Il y a trois méthodes pour créer des VLAN :

- VLAN de niveau 1 : on affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN.
- VLAN de niveau 2 : on affecte chaque adresse MAC à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par son adresse MAC. En fait il s'agit à partir de l'association Mac/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.
- VLAN de niveau 3 : on affecte un protocole de niveau 3 ou de niveau supérieur à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par le protocole de niveau 3 ou supérieur qu'elle utilise. En fait il s'agit à partir de l'association protocole/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

Une carte réseau ne peut-être associée qu'à un seul VLAN. Une carte réseau associée à un VLAN par une de ces trois méthodes ne peut communiquer qu'avec une carte réseau associée à un même VLAN. Une trame de diffusion (broadcast) émise par une carte réseau associée à un VLAN sera transmise à toutes les cartes réseaux composant ce VLAN et **uniquement celles-ci**.

Protocole 802.1q : Un commutateur peut gérer plusieurs VLAN et un VLAN peut être géré par plusieurs commutateurs. L'appartenance à un VLAN, d'une trame circulant entre les commutateurs est déterminée par un marquage de la trame qui rajoute à celle-ci l'identifiant du VLAN. 802.1q marque les trames en modifiant l'en-tête MAC de la trame. Il rajoute notamment dans cette entête un identifiant de VLAN qui permet rapidement au commutateur d'associer la trame à un VLAN sans consulter ses tables. Cette modification du format de la trame est généralement faite par les commutateurs sur les liaisons inter-commutateurs (trunk link) en utilisant des ports spéciaux, les ports 802.1q (port *trunk link*). En effet, la modification de l'entête implique que les éléments recevant la trame marquée (*taggée*) disposent du protocole 802.1q. Ce n'est généralement pas le cas des cartes réseaux. Les ports *trunk link* associés à ce type de lien ajoutent ou enlèvent le PDU (Protocole Data Unit) 802.1q selon qu'ils transmettent ou non la trame à un commutateur. Remarque : 802.1q est basé sur un protocole propriétaire CISCO ISL (Inter Switch Linking) et permet également de gérer la qualité de service (QoS) par la même technique de marquage de la trame.

Protocole 802.1d : Pour gérer la tolérance de pannes dans les liaisons inter-commutateurs on met en place des liaisons redondantes. Les liaisons redondantes doivent être invalidées quand elles ne sont pas utiles et validées en cas de rupture d'une liaison. Cette gestion de la redondance est prise en charge par le protocole 802.1d (spanning tree).

Proposition de corrigé :

Première partie

1. Les fibres optiques sont sur les commutateurs et non sur les routeurs. Les commutateurs propagent les broadcast. Le protocole ARP est basé sur une trame de broadcast "request".

Lorsque le poste 192.168.1.1 exécute un ping 192.168.3.1 il génère une trame "ARP" pour récupérer l'adresse MAC de son routeur par défaut R1 (192.168.1.253). Une fois qu'il a son adresse MAC il utilise cette adresse pour lui transmettre les paquets "echo" destinés à 192.168.3.1 que le routeur R1 devra relayer.

Le routeur R1 doit transmettre les paquets au routeur R2 (192.168.2.253). Il générera donc une requête ARP pour récupérer l'adresse MAC de celui-ci. Comme précédemment, une fois obtenue l'adresse MAC il utilise cette adresse pour transmettre les paquets "echo" destinés à 192.168.3.1 que le routeur R2 devra relayer.

Enfin le routeur R2 génère une requête ARP pour récupérer l'adresse MAC du poste 192.168.3.1, adresse qu'il utilisera ensuite pour transmettre les paquets ICMP.

Toutes les trames de broadcast ARP parviennent au portable de l'administrateur. Les trois entêtes sont en format ETHERNET II (ou DIX Digital Intel Xerox):

Adresse MAC destination	Adresse MAC source	Type
FF-FF-FF-FF-FF-FF	0d-0a-c1-00-00-01	0806
FF-FF-FF-FF-FF-FF	d4-00-b1-e3-07-02	0806
FF-FF-FF-FF-FF-FF	d4-00-b1-e3-07-04	0806

2. Les trames ARP "reply" et l'échange ICMP ne sont pas basés sur des trames de broadcast. Le commutateur ne les diffuse pas au portable de l'administrateur mais commute directement vers le bon port.
3. Il faut établir un "mirroring" entre le port c3f1 et le port c3e3.
4. Les trames capturées seraient celles envoyées par le routeur R2.

Adresse MAC destination	Adresse MAC source	Type
0d-0a-c1-00-00-03	d4-00-b1-e3-07-04	0800

Les adresse IP correspondent à celles de l'émetteur et du destinataire réels

Adresse IP source	Adresse IP destination
192.168.1.1	192.168.3.1

Deuxième partie

1. Il n'y a pas de liaison redondante ou de circuit établi entre les commutateurs donc il n'y a pas de tolérance aux pannes. Ceci explique pourquoi l'administrateur n'a pas mis en œuvre le protocole 802.1d (spanning tree) qui permet d'invalider les chemins redondants et de les réactiver en cas de besoin. Ce protocole est donc inutile dans ce cas.
2. Le protocole 802.1q permet de gérer des VLAN distribués sur plusieurs commutateurs, ce qui n'est pas le cas ici puisqu'on a un VLAN par commutateur.

Troisième partie

1. Le poste capturera l'échange ARP et l'échange ICMP entre le Routeur R2 et le serveur administratif. Il ne capturera pas les autres échanges ARP car les VLAN constituent des domaines de diffusion.
2. Le port c1f1 n'est pas affecté au bon VLAN il faut l'affecter au VLAN numéro 2.