2-C : Réseaux Locaux Virtuels

Olivier GLÜCK
Université LYON 1 / Département Informatique
Olivier.Gluck@univ-lyon1.fr
http://perso.univ-lyon1.fr/olivier.gluck

1

Copyright

2

Remerciements

- Certains transparents sont basés sur des supports de cours de :
  - Danièle DROMARD (PARIS 6)
  - Andrzej DUDA (INP Grenoble/ENSIMAG)
  - Shivkumar KALYANARAMAN (RPI/ECSE)
  - Alain MILLE (LYON 1)
  - CongDuc PHAM (LYON 1)
  - Laurent Toutain (ENST Bretagne)
  - Michel RIVEILL (Université de Nice/ESSI)
  - L'Institut National des Télécommunications (INT)
  - Cisco Networking Acadamy
- Des figures sont issues des livres cités en bibliographie

3

Bibliographie

- « *Réseaux* », 4ième édition, Andrew Tanenbaum, Pearson Education, ISBN 2-7440-7001-7
- « *Réseaux et Télécoms* », Claude Servin, Dunod, ISBN 2-10-007986-7
- « *Analyse structurée des réseaux* », 2ième édition, J. Kurose et K. Ross, Pearson Education, ISBN 2-7440-7000-9
- « *TCP/IP Illustrated Volume 1, The Protocols* », W. R. Stevens, Addison Wesley, ISBN 0-201-63346-9
- « *TCP/IP, Architecture, protocoles, applications* », 4ième édition, D. Comer, Dunod, ISBN 2-10-008181-0
- « *An Engineering Approach to Computer Networking* », Addison-Wesley, ISBN 0-201-63442-6
- « Réseaux locaux et Internet, des protocoles à l'interconnexion », 3ième édition, Laurent Toutain, Hermes Science, ISBN 2-7462-0670-6
- Internet…

4

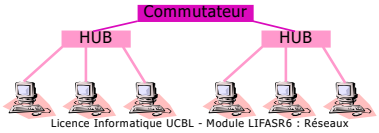
Réseaux Locaux Virtuels (VLAN)

Principe des VLAN
Intérêts
Appartenance à un VLAN
Etiquetage des trames (802.1p/Q)

5

Pourquoi les VLANs ? (1)

- Dans les réseaux locaux partagés
  - les sous-réseaux sont liés aux hubs
  - les utilisateurs sont groupés géographiquement
  - pas de sécurité sur un segment : n'importe quelle station du segment peut capturer l'ensemble du trafic réseau
  - la mobilité entraîne un changement d'adresse et/ou un re-câblage
  - les *broadcasts* interrompent tous les matériels réseau avec traitement au niveau du CPU



6

Pourquoi les VLANs ? (2)

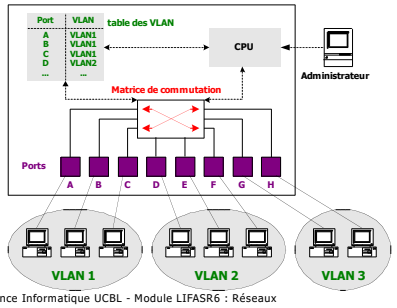
- Trois nécessités auxquelles un LAN commuté ne répond pas
  - Limitation des domaines de diffusion
  - Garantir la sécurité par isolement de certains trafics
  - Permettre la mobilité des utilisateurs
- Les VLANs : une nouvelle manière d'exploiter la technique de la commutation en donnant plus de flexibilité aux réseaux locaux
- -> segmentation du réseau un peu à la manière de la commutation mais de façon logique (indépendamment du câblage physique)

7

Principe des VLANs (1)

- Créer des réseaux logiques indépendants les uns des autres

Une diffusion provenant d'une station du VLAN2 ne sera répercutée que sur les ports D, E, F



8

Principe des VLANs (2)

- L'administrateur configure statiquement la table des VLAN
- Les communications inter-VLAN ne sont possibles qu'à travers un routeur
- L'appartenance à un VLAN est indépendante de la localisation géographique - un VLAN peut s'étendre sur plusieurs commutateurs
- Un segment Ethernet est un domaine de collision
- Un VLAN est **un domaine de diffusion**

9

Intérêts des VLAN

- Confidentialité et sécurité
  - le trafic entre les réseaux virtuels est isolé
  - permet de limiter l'accès à certains équipements ou services (VLAN des machines en libre service, VLAN des accès à Internet, ...)
- Performance
  - limite la portée des *broadcast* (ARP)
  - répartition de la charge du réseau
- Facilité de mise en œuvre et souplesse
  - logiciel d'administration du commutateur
  - on peut retirer ou donner l'accès à un VLAN sans modifier le câblage dans les armoires de brassage, voire sans déplacer la station
  - une station peut appartenir à plusieurs VLANs

10

Appartenance à un VLAN (1)

- définie par le port physique du commutateur
  - chaque port est associé à 1 ou plusieurs VLAN
  - configuration statique fixée par l'administrateur
  - inconvénient : le déplacement d'une machine nécessite la reconfiguration du port du commutateur
  - sécurisé : un utilisateur ne peut pas changer de VLAN
- définie par l'adresse MAC
  - plus souple : permet la mobilité des machines sans reconfigurer les VLAN
  - l'administrateur doit connaître les @ MAC...
  - deux stations du même segment Ethernet peuvent appartenir à des VLAN distincts
  - moins sécurisé : un utilisateur peut changer son @ MAC

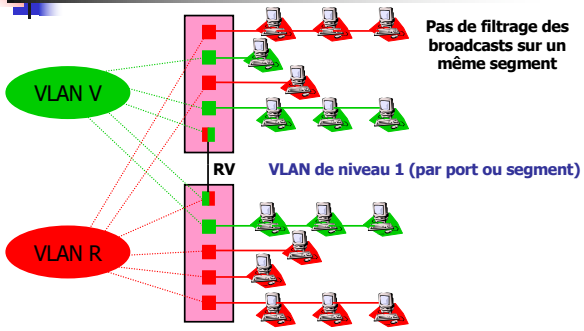
11

Appartenance à un VLAN (2)

- définie par les adresses de niveau 3 (IP)
  - très souple : association d'un préfixe IP (@ de sous-réseau ou plages d'@) et d'un numéro de VLAN
  - un routeur permet de passer d'un VLAN à l'autre
  - perte de performance : il faut analyser les trames au niveau 3 pour déterminer l'appartenance à un VLAN
  - ne respecte pas l'indépendance des couches...
  - non sécurisé : l'utilisateur peut facilement changer son @ IP
- définie par protocoles de niveau 3 (permet d'isoler le trafic de chaque protocole)
- définie par numéro de port TCP (permet d'isoler le trafic de chaque type d'applications)

12

Appartenance à un VLAN (3)

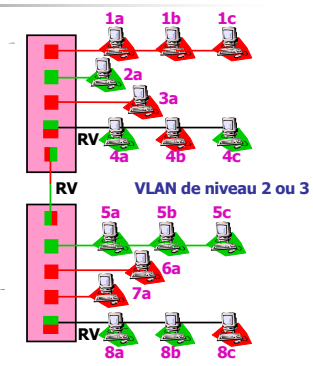


Pas d'analyse de la trame pour déterminer l'appartenance à un VLAN

13

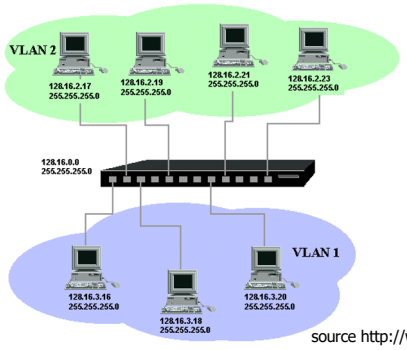
Appartenance à un VLAN (4)

- Une adresse MAC ne peut appartenir qu'à un seul VLAN
- Plusieurs VLAN par port autorisés
- Nécessite une analyse de chaque trame
- Echange des tables de correspondances @MAC/VLAN entre les commutateurs ou étiquetage des trames nécessaires



14

Appartenance à un VLAN (5)



source http://www.univ.edu.dj/cours

15

VLAN sur plusieurs commutateurs (1)

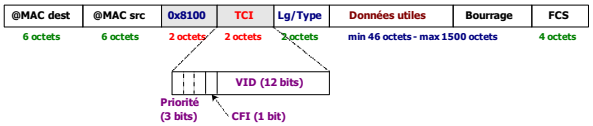
- Il faut transporter l'information d'appartenance à un VLAN (chaque commutateur doit connaître le VLAN associé à la source et au destinataire)
- Deux possibilités
  - chargement des tables de VLAN dans tous les équipements (problème de facteur d'échelle)
  - ajout d'une étiquette aux trames transportées entre les commutateurs uniquement (côté émetteur)
    - l'étiquette identifie le VLAN de la station source
    - norme IEEE 802.1p/Q : format des étiquettes indépendant du constructeur de l'équipement

16

VLAN sur plusieurs commutateurs (2)

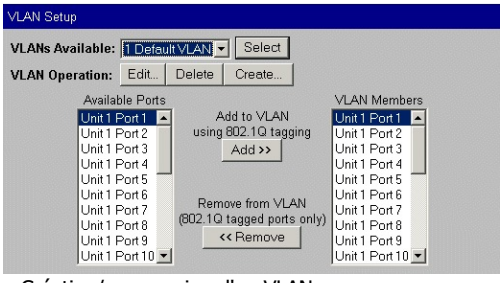
- Modification transparente de l'en-tête MAC (compatibilité avec les anciens équipements)
  - un niveau d'encapsulation 802.1p/Q identifié par 0x8100
  - la trame 802.3 est allongée de 4 octets (nécessite de recalculer le FCS)
  - champ priorité sur 3 bits : files d'attente plus ou moins prioritaires dans les commutateurs (QoS - voix par ex.)
  - bit CFI pour le routage par la source

Trame IEEE 802.1p/Q



17

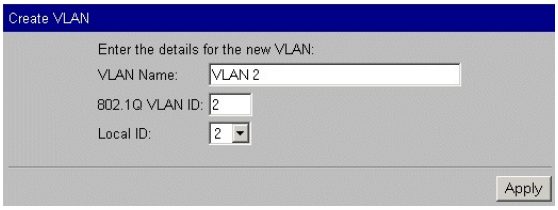
Administration des VLANs (1)



- Création/suppression d'un VLAN
- Ports supportants l'étiquetage 802.1Q des trames

18

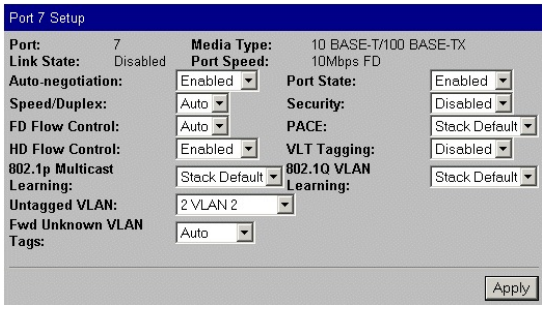
Administration des VLANs (2)



- Paramétrage d'un VLAN

19

Administration des VLANs (3)



- Configuration d'un port

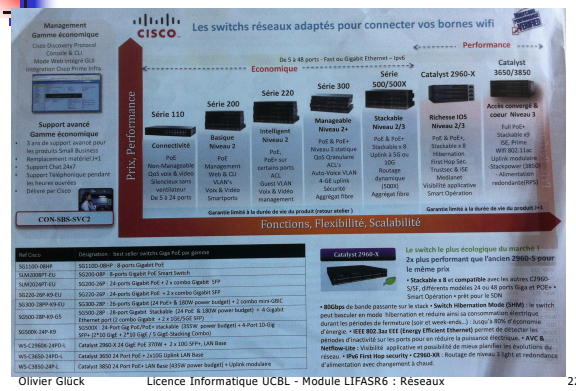
20

Règles de design des VLAN

- Les questions qu'il faut se poser
  - nombre d'utilisateurs du réseau ?
  - plan du campus et plan de câblage ?
  - partitions des utilisateurs partageant des données ou des services ?
  - les utilisateurs qui partagent des données sont-ils géographiquement proches ?
  - la mobilité se fait-elle par département ou par éléments isolés ?
  - répartition du trafic sur le réseau ?
  - ressources centralisées ou distribuées ?

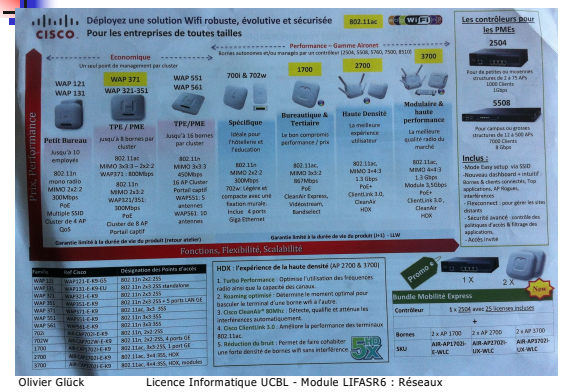
21

Exemples de matériels (1)



22

Exemples de matériels (2)



23