



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

- Copyright © 2022 Olivier Glück; all rights reserved
- Ce support de cours est soumis aux droits d'auteur et n'est donc pas dans le domaine public. Sa reproduction est cependant autorisée à condition de respecter les conditions suivantes :
 - Si ce document est reproduit pour les besoins personnels du reproducteur, toute forme de reproduction (totale ou partielle) est autorisée à la condition de citer l'auteur.
 - Si ce document est reproduit dans le but d'être distribué à des tierces personnes, il devra être reproduit dans son intégralité sans aucune modification. Cette notice de copyright devra donc être présente. De plus, il ne devra pas être vendu.
 - Cependant, dans le seul cas d'un enseignement gratuit, une participation aux frais de reproduction pourra être demandée, mais elle ne pourra être supérieure au prix du papier et de l'encre composant le document.
 - Toute reproduction sortant du cadre précisé ci-dessus est interdite sans accord préalable écrit de l'auteur.

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

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 Academy
- Des figures sont issues des livres cités en bibliographie

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

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

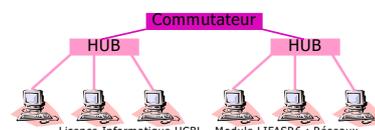
Réseaux Locaux Virtuels (VLAN)

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



Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

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)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

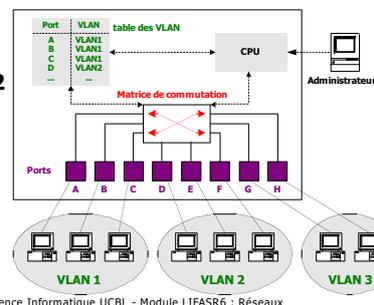
7

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



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

8

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**

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

9

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

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

10

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

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

11

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)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

12

12

Appartenance à un VLAN (3)

Pas de filtrage des broadcasts sur un même segment

VLAN V

RV

VLAN de niveau 1 (par port ou segment)

VLAN R

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

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 13

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

RV

VLAN de niveau 2 ou 3

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 14

14

Appartenance à un VLAN (5)

VLAN 2

VLAN 1

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

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 15

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

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 16

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

@MAC dest	@MAC src	0x8100	TCI	Lg/Type	Données utiles	Bourrage	FCS
6 octets	6 octets	2 octets	2 octets	2 octets	min 46 octets - max 1500 octets		4 octets

VID (12 bits)

Priorité (3 bits)

CFI (1 bit)

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 17

17

Administration des VLANs (1)

VLAN Setup

VLANs Available:

VLAN Operation:

Available Ports: Unit 1 Port 1, Unit 1 Port 2, Unit 1 Port 3, Unit 1 Port 4, Unit 1 Port 5, Unit 1 Port 6, Unit 1 Port 7, Unit 1 Port 8, Unit 1 Port 9, Unit 1 Port 10

Add to VLAN using 802.1Q tagging

Remove from VLAN (802.1Q tagged ports only)

VLAN Members: Unit 1 Port 1, Unit 1 Port 2, Unit 1 Port 3, Unit 1 Port 4, Unit 1 Port 5, Unit 1 Port 6, Unit 1 Port 7, Unit 1 Port 8, Unit 1 Port 9, Unit 1 Port 10

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

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 18

18

Administration des VLANs (2)

Create VLAN

Enter the details for the new VLAN:

VLAN Name:

802.1Q VLAN ID:

Local ID:

- Paramétrage d'un VLAN

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 19

19

Administration des VLANs (3)

Port 7 Setup

Port: 7	Media Type: 10 BASE-T/100 BASE-TX
Link State: Disabled	Port Speed: 10Mbps FD
Auto-negotiation: Enabled	Port State: Enabled
Speed/Duplex: Auto	Security: Disabled
FD Flow Control: Auto	PACE: Stack Default
HD Flow Control: Enabled	VLT Tagging: Disabled
802.1p Multicast Learning: Stack Default	802.1Q VLAN Learning: Stack Default
Untagged VLAN: 2 VLAN 2	
Fwd Unknown VLAN Tags: Auto	

- Configuration d'un port

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 20

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 ?

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 21

21

Exemples de matériels (1)

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 22

22

Exemples de matériels (2)

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 23

23