Multisites S.A.
module « actifs »

TP N°7 : Configurer les VLAN (niveau 1)

Nom : **Prénom :** **Classe :** **Date :**	**Appréciation** :	**Note** :
Objectifs : - Être capable d'effectuer le brassage Ethernet - Être capable de configurer les VLANs par port		**durée** : 12h

Matériel (réseau "fondcombes"):

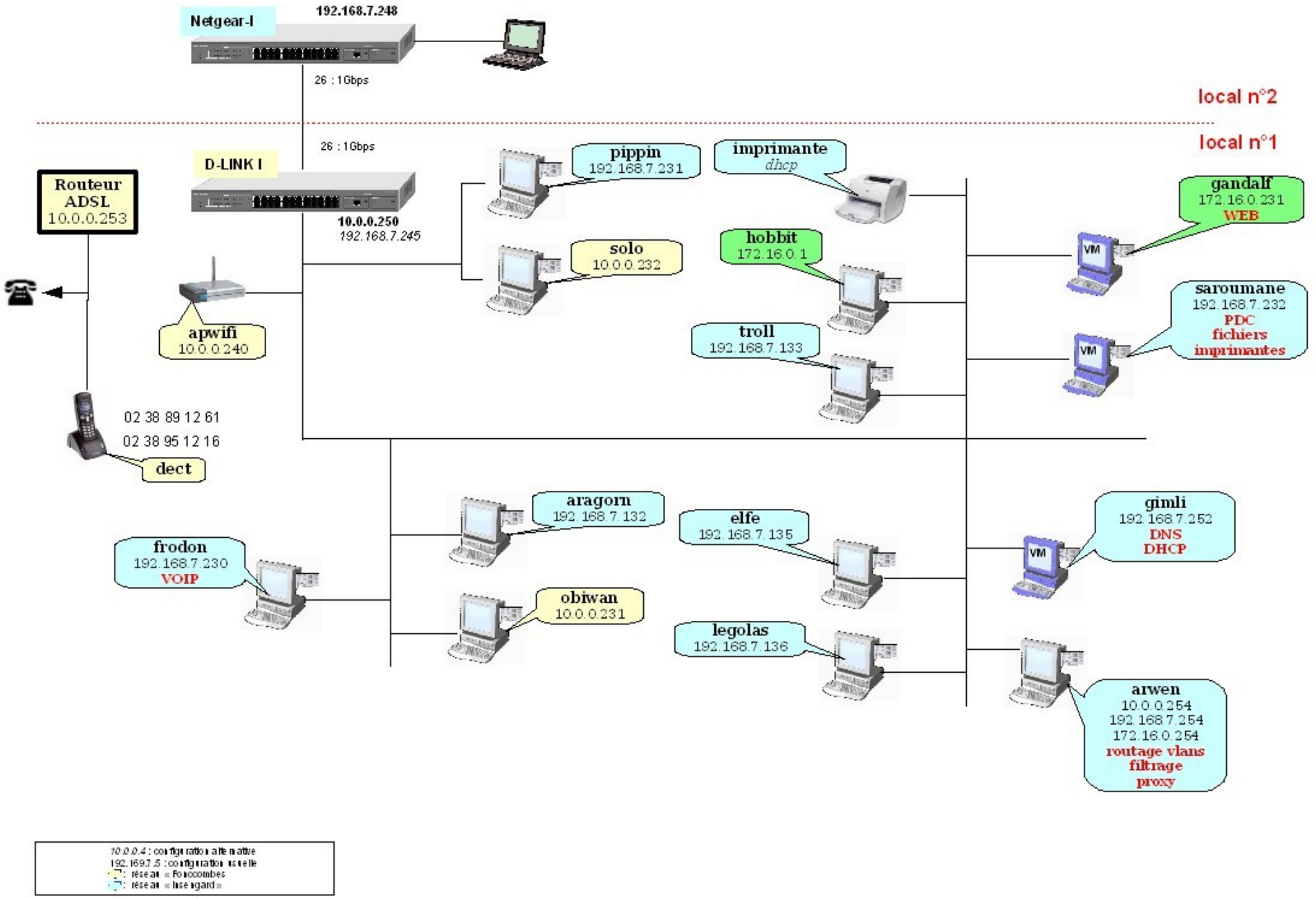
- 1 ordinateur PC
- 1 commutateur Ethernet

Travail à réaliser :

Compléter le schéma de réseau en page 3, en entourant la partie « actifs » du réseau, dont vous avez la responsabilité.

Partie A :

Partie B :



Compléter le schéma de réseau , en entourant la partie « actifs » du réseau, dont vous avez la responsabilité

PARTIE B VLANs

Segmentation par sous-réseaux IP

➔ Quelle est la **plage d'adresse** réservée aux machines du groupe **Gestion** : _____

➔ Quelle est la plage d'adresse réservée aux machines du groupe **Production** : _____

➔ Relever l'adresse IP de **frodon** : _____ *(normalement : 192.168.7.231)*

➔ Relever l'adresse IP de **Solo** : _____ *(normalement : 10.0.0.232)*

➔ Relever l'adresse IP de **dhcp** : _____ *(normalement : 192.168.7.135)*

➔ Faire un ping de **frodon** vers **Solo**; Quel est le résultat ? : _____ *(non)*

➔ Faire un ping de **frodon** vers **dhcp**; Quel est le résultat ? : _____ *(ok)*

➔ Remplir le tableau suivant en vérifiant les adresses IP réelles des machines :

➔ Continuer de remplir le tableau suivant en mettant une croix quand le ping fonctionne :

Destination du ping

	Solo
voip ____ .____ .____ .____	
frodon ____ .____ .____ .____	
Elfe ____ .____ .____ .____	
Obiwan ____ .____ .____ .____	
Adsl ____ .____ .____ .____	

Source du ping

➔ Expliquez ces résultats :_____

_____

Information : notion de réseau et sous-réseau IP

On peut segmenter un réseau IP en plusieurs sous-réseaux en donnant à chacun d'eux une adresse de réseau différente; car seules deux machines sur le même réseau peuvent communiquer.

On rappelle que l'adresse réseau est déterminée par le masque de réseau :

Adresse de la machine : 192.168.	7.1		10 .0 .0 .1	: Adresse de la machine
masque de réseau :	255.255.255.0	(ET logique)	255.255.255.0	: masque de réseau
Adresse de réseau : 192.168.	7.0		10 .0 .0 .0	: Adresse de réseau

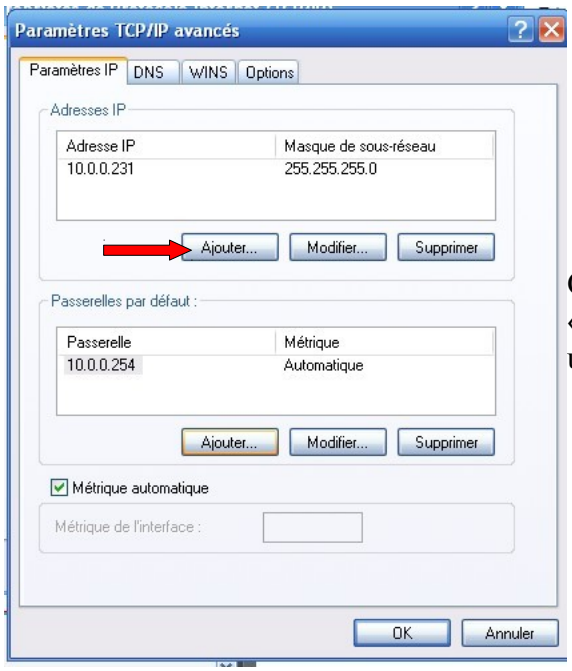
Cette méthode de segmentation est-elle fiable et sûre ? Non, car il est facile de changer l'adresse IP ou le masque de réseau d'un poste pour se connecter à une machine de l'autre groupe; de plus cela n'empêche pas les trames de broadcast de polluer les deux parties du réseau

➔ La machine **Solo** appartient au groupe « **gestion** ». Elle appartient donc au réseau IP : ____ .____ .____ .0

➔ Vous allez ajouter une seconde adresse IP à la machine **Solo** pour lui donner accès au groupe « **Production** ». Cette adresse doit être dans le réseau : IP : ____ .____ .____ .0

- Ouvrir les propriétés TCP/IP de la carte Ethernet

- Cliquez sur « Avancé... » comme ci-dessous :



Cliquez sur « Ajouter » une adresse IP

- Faisons à nouveau des ping vers différentes machines :

Destination du ping

	Solo
voip ____ .____ .____ .____	
frodon ____ .____ .____ .____	
Elfe ____ .____ .____ .____	
Obiwan ____ .____ .____ .____	
Adsl ____ .____ .____ .____	

Source du ping

➔ Comparer avec le tableau de la page 2; expliquez ces résultats : _____

_____

Information : limitation de cette méthode
Vous avez constaté que les deux sous-réseaux créés ne sont pas très « étanches »; il suffit de donner une adresse IP de l'autre réseau pour y avoir accès; par exemple : un virus pourrait cette méthode pour se propager d'un sous-réseau à l'autre. Nous allons maintenant voir une méthode beaucoup plus puissante pour segmenter le réseau : les vlans

Utilité des VLANS

➔ Qu'est-ce qu'un VLAN ? _____

_____

➔ Citez les trois types de VLAN possibles (en fonction du critère de segmentation)

_____

➔ Qu'est-ce qu'une trame de broadcast (diffusion) ? _____

➔ Les trames de broadcast peuvent-elles traverser les vlans ? _____

➔ Citez des protocoles qui utilisent des trames de broadcast et qui donc ne fonctionneront pas entre vlan

_____

➔ Quelle fonction est nécessaire pour permettre à deux machines situés sur deux vlan différents de communiquer ?

_____

Information : trames de broadcast

Les trames de broadcast (en français : « diffusion ») sont des trames envoyée par une machine, destinée à toutes les autres machines du réseau.

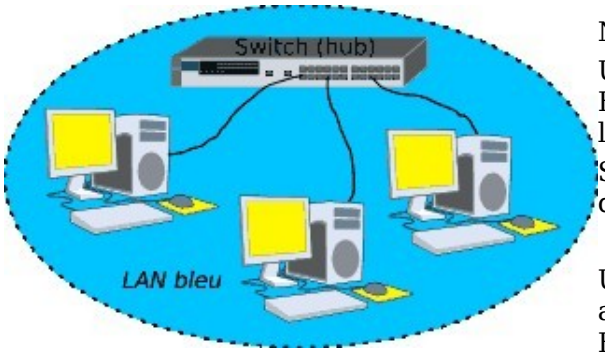
L'inconvénient de ces trames est qu'elle ont tendance à polluer le réseau, comme la publicité dans les boites aux lettres car elles sont envoyées même à ceux qui ne sont pas concernés. De même que la publicité peut saturer votre boite aux lettres, les trames de broadcast peuvent finir par saturer un réseau, ou au moins à le ralentir.

Les machines sous MS-Windows intègrent des protocoles qui génèrent beaucoup de broadcast, comme le protocole Netbios.

VLANs : principes

(source : Christian Caleca - http://stielec.ac-aix-marseille.fr)

Première situation : Un LAN non-segmenté



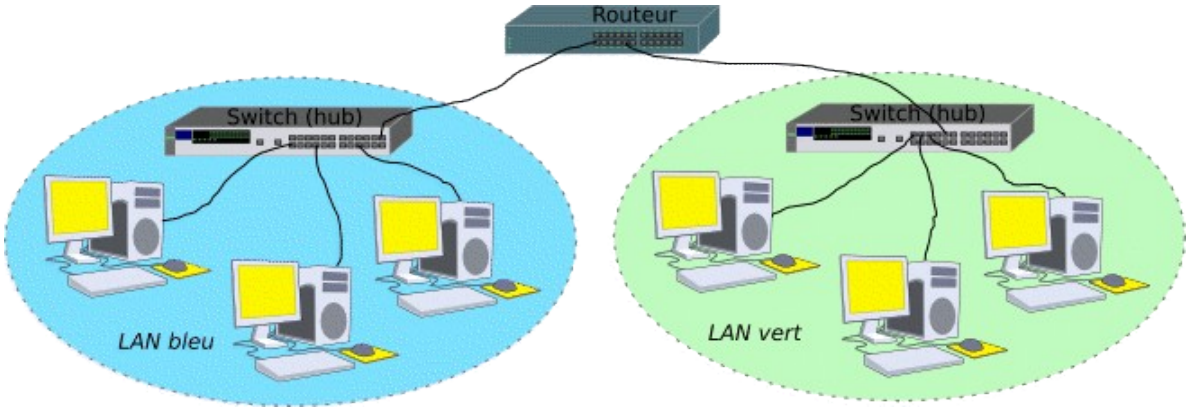
Nous sommes ici sur un réseau Ethernet.

Un LAN est un réseau local dans lequel toutes les trames Ethernet sont visibles depuis tous les noeuds (=machines) si le LAN est construit avec un HUB.

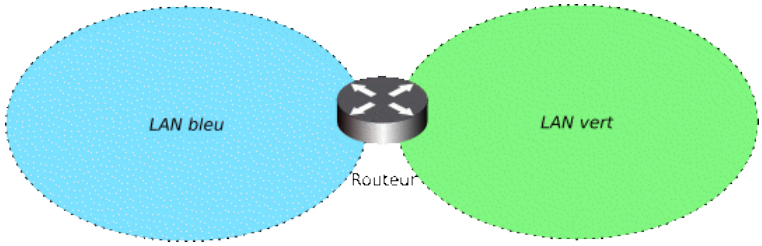
Si nous avons affaire à un SWITCH, seules les trames de diffusions (broadcast) seront visibles depuis tous les noeuds,

Un SWITCH est capable d'apprendre et de retenir la ou les adresses MAC qui se présentent sur chacun de ses ports. Hormis les trames de diffusion qui seront systématiquement répercutées sur tous les ports, le SWITCH ne laissera communiquer entre eux que les ports concernés par un dialogue entre deux noeuds. C'est sa fonction principale de pont Ethernet.

Deuxième situation : deux ou plusieurs LAN connectés

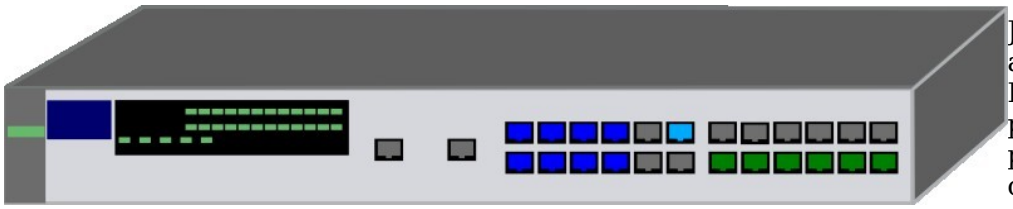


Lorsque nous avons deux LANs et que nous souhaitons les inter-connecter, tout en conservant dans chaque LAN les mêmes propriétés au niveau Ethernet, nous devons faire appel à la couche 3 (IP) pour assurer l'interconnexion : il nous faut donc **un routeur**.



Le routeur agit au niveau 3 (IP). Ce qu'il est absolument fondamental de comprendre, c'est qu'au niveau Ethernet, le LAN bleu ignore complètement l'existence du LAN vert, et réciproquement. Les trames Ethernet, qu'elles soient de la diffusion ou non, n'iront jamais dans l'autre LAN. Il y a isolation complète des deux LANs au niveau Ethernet. Concrètement, **quand une trame est routée d'un LAN vers l'autre, l'adresse MAC source n'est plus celle du poste qui envoie le message, mais celle du routeur**.

Où intervient le « virtuel » de « VLAN »

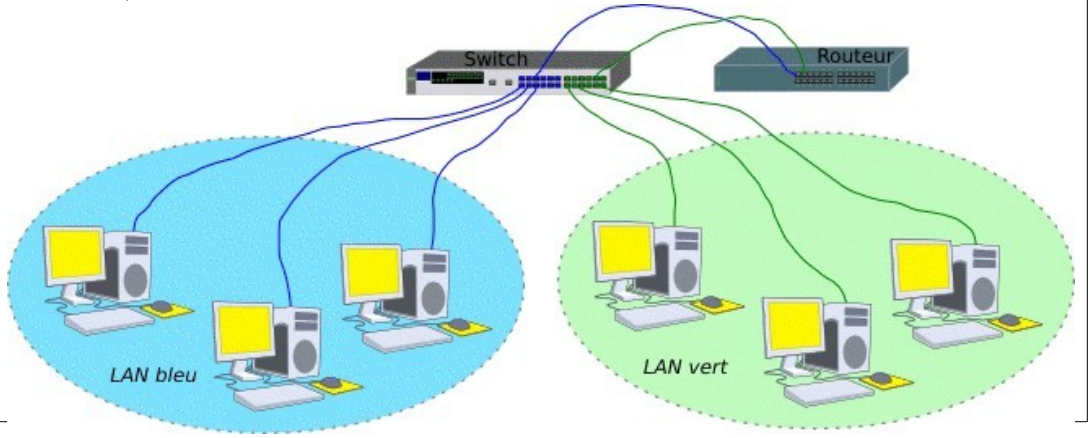


Jusqu'ici, un SWITCH appartenait à un et un seul LAN. L'idée de base est de pouvoir assigner certains ports du SWITCH à un LAN, certains autres ports à un autre LAN etc :

Sur un même SWITCH physique, nous allons pouvoir créer plusieurs LANS et **assigner certains de ses ports aux divers LANs créés**. Ici, nous avons un LAN bleu et un LAN vert.

Tout va (presque) se passer comme si l'on avait découpé notre SWITCH en deux parties virtuelles. Notre maquette deviendrait ceci :

(notez que le routeur a une "patte" dans chacun des vlan)



➔ Quelle est l'utilité des VLAN ?

_____

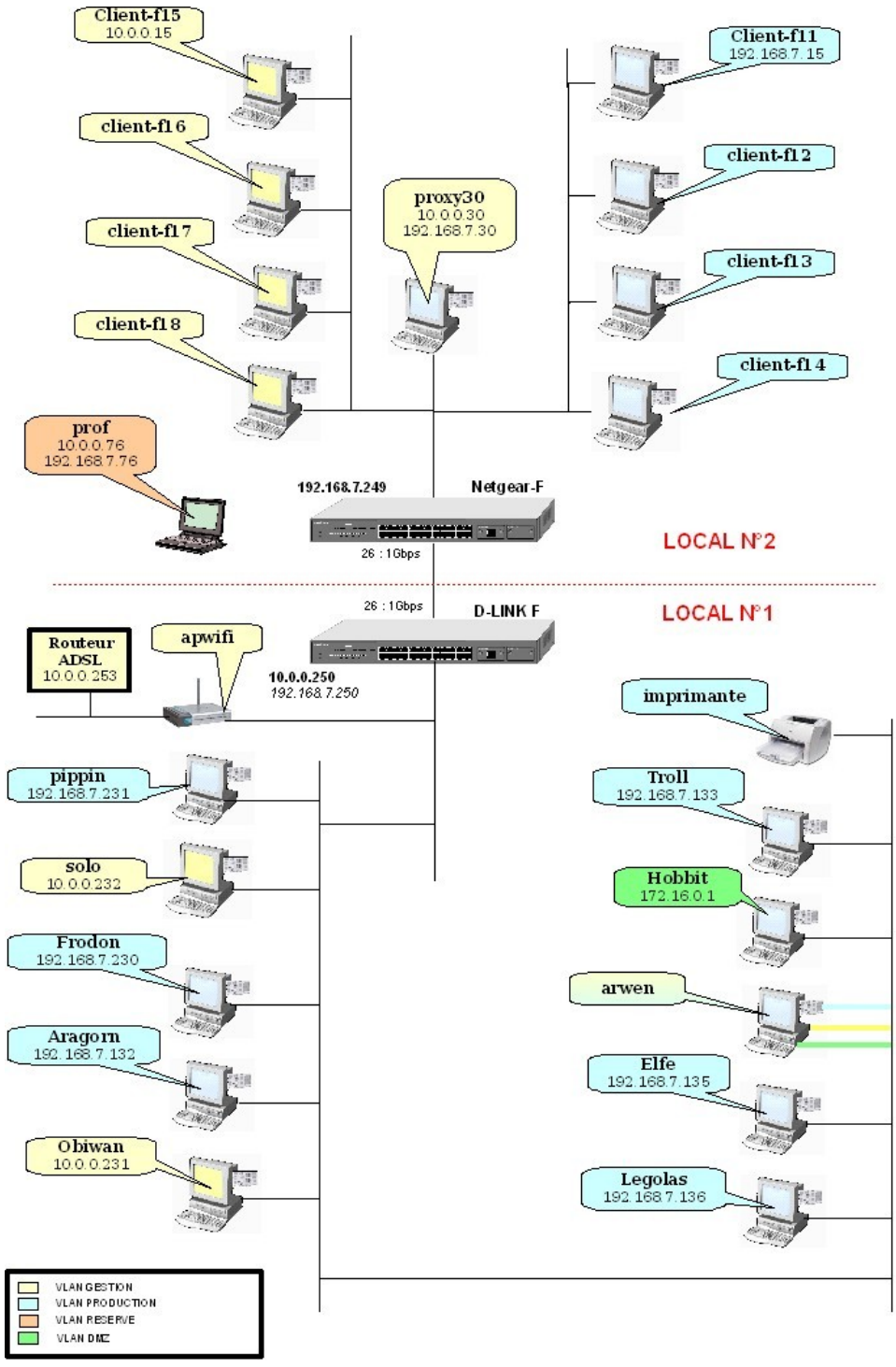
_____

_____

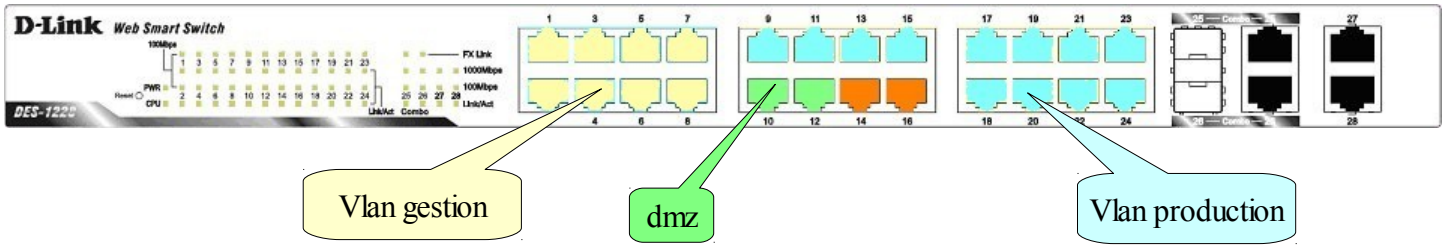
Information : utilité des VLAN
Les VLAN sont une option des configuration disponible dans les commutateurs dit « manageable ». Cela permet de **segmenter le réseau** en plusieurs parties, comme si ces machines étaient reliées à des commutateurs indépendants. Les avantages sont : • optimisation du matériel. En effet,nous n'avons plus besoin que d'un seul SWITCH, là où il nous en fallait deux au départ, les différents LANs restant malgré tout bien isolés les uns des autres (sécurité plus facile à gérer) • passer un poste de travail d'un LAN à l'autre devrait pouvoir se faire de façon "soft". Plutôt que de débrancher puis de re-brancher ailleurs le lien du poste, nous pourrons le faire par l'outil de configuration du SWITCH. • Les trames de broadcast d'un VLAN ne vont pas « polluer » un autre VLAN. On dit qu'on a **segmenté le domaine de broadcast**.

Information : les différents types de VLAN
Il y a trois types de VLAN en fonction du critère du segmentation : • Segmentation par port : chaque port du switch est affecté à un vlan • Segmentation par adresse MAC : chaque adresse MAC est affectée à un vlan. Cela suppose de relever les adresses MAC de tous les ordinateurs et imprimantes du réseau. • Segmentation par adresse IP : chaque plage d'adresse IP est affectée à un vlan. les ordinateurs et imprimantes sont donc affectés à un vlan en fonction de leur adresse IP

Schéma du réseau segmenté *(voir annexes 2 et 3)*



- Réaliser le brassage sur le commutateur (salle D041 uniquement) de façon à faire apparaître les vlans :
  (Voir les instructions de brassage en Annexe 2 !!!)



Configuration du commutateur D-LINK 1228

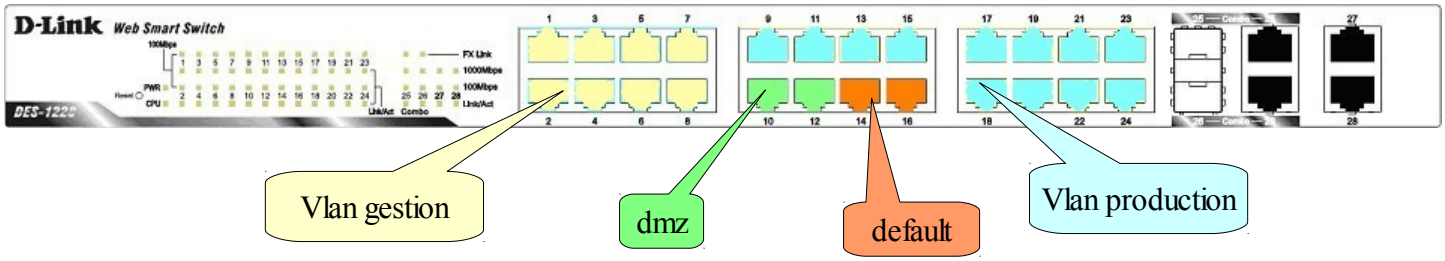
***note** : vous trouverez la documentation à l'adresse http://www.cvardon.fr/restricted/doctech.html*

Information : la connexion série ou RS232C et Hyperterminal
Les commutateurs administrables possèdent (presque) tous un mode dit « console » qui permet d'accéder à l' interface d'admin, même si on ne connaît pas sa configuration IP

Information importante : mots de passe!!
Les commutateurs administrables possèdent un ou plusieurs mots de passe pour accéder à l'interface d'administration. En cas de perte du mot de passe, il est nécessaire de renvoyer l'appareil en réparation chez le fabricant, ce qui a évidemment un coût très élevé!! **VOUS NE DEVEZ DONC JAMAIS CHANGER LES MOTS DE PASSE DES MATERIELS QUI VOUS SONT CONFIES, FAUTE DE QUOI LES FRAIS DE REPARATION VOUS SERAIENT IMPUTES.**

- **Ouvrir l'interface d'administration du commutateur DLINK** à l'adresse IP : _____

➔ A l'aide de la documentation, indiquez la procédure à suivre pour définir un vlan « untagged » (**non-taggué)** :



- Configurer la commutateur de façon à réaliser la segmentation en trois vlans comme indiqué ci-dessus, avec les précisions suivantes :

Nom du vlan	gestion	dmz	production
VID	01	02	03

- Afin de **vérifier** le fonctionnement des vlans, remplir le tableau suivant, en effectuant les « ping » :

Note : la machine *Solo* possède toujours deux adresses ip : une dans *gestion* et une dans *production* (voir p.7)

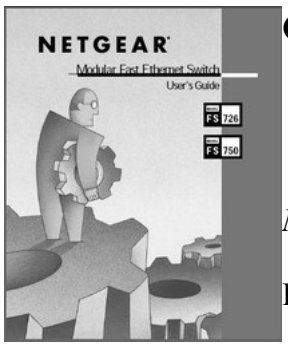
Destination du ping ↓

	Solo	frodon	← ***Source du ping***
voip			
frodon			
Aragorn			
pdc			
dhcp			
Obiwan			
Solo			
adsl			

Qu'en concluez-vous ? A quelle condition deux machines peuvent-elle communiquer entre elles ? : _____

_____

Est-il possible de « pirater » en prenant une adresse IP dans l'autre groupe de machine ? :_____

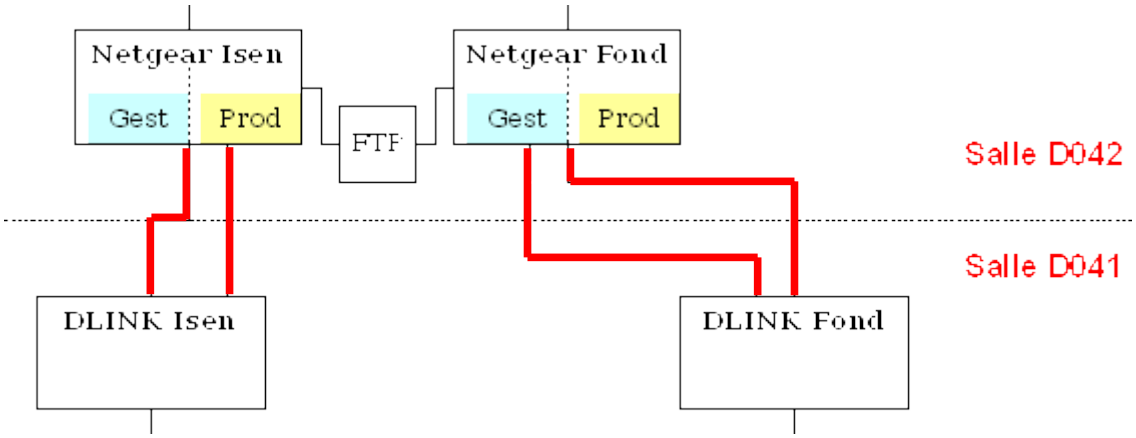


Configuration du commutateur NetGear FS726T

Nous allons maintenant configurer les même vlans dans la salle D042;

Les machines de cette salle sont reliées par un commutateur *NetGear FS726T*;

- On définira les vlans *gestion* et *production* sur ce commutateur Netgear, comme sur les *D-LINK*, puis on les relie ainsi avec un lien Ethernet *Cat 5E* en *RJ45* pour chaque vlan :



- Intervenir sur les baies de brassage salle D041 et D042 de façon à créer ou à vérifier l'existence des deux liens Ethernet pour les deux vlans : *Gestion* et *Production*

Information
Le commutateur FS726T intègre un (mini-) serveur web qui sert d'interface de configuration.

➔ Quel type de logiciel utilisez-vous pour vous connecter à ce serveur web ? _____

➔ **Renseignez** l'adresse LAN du commutateur pour votre site : http://_____. _____. _____. _____

- Lancez cette interface avec l'utilisateur « admin »
  et le mot de passe _____ *(demander au professeur)*

➔ A l'aide de la documentation, indiquez la procédure à suivre pour définir un vlan (par port) :

_____

_____

_____

_____

_____

_____

_____

(insérer ci-dessous une(des) copie(s) d'écran de la page de configuration)

- Réaliser la segmentation en deux vlans comme indiqué ci-dessus :

(insérer ci-dessous une copie d'écran du résultat - « status page »)

- Configurer les postes client-i1, client-f11, client-i5, client-f15 avec les adresses IP appropriées en fonction du vlan auquel ils appartiennent
- Remplir le tableau suivant en vérifiant les adresses IP réelles des machines
- A l'aide de commandes **ping**, remplir le tableau suivant:

Destination du ping

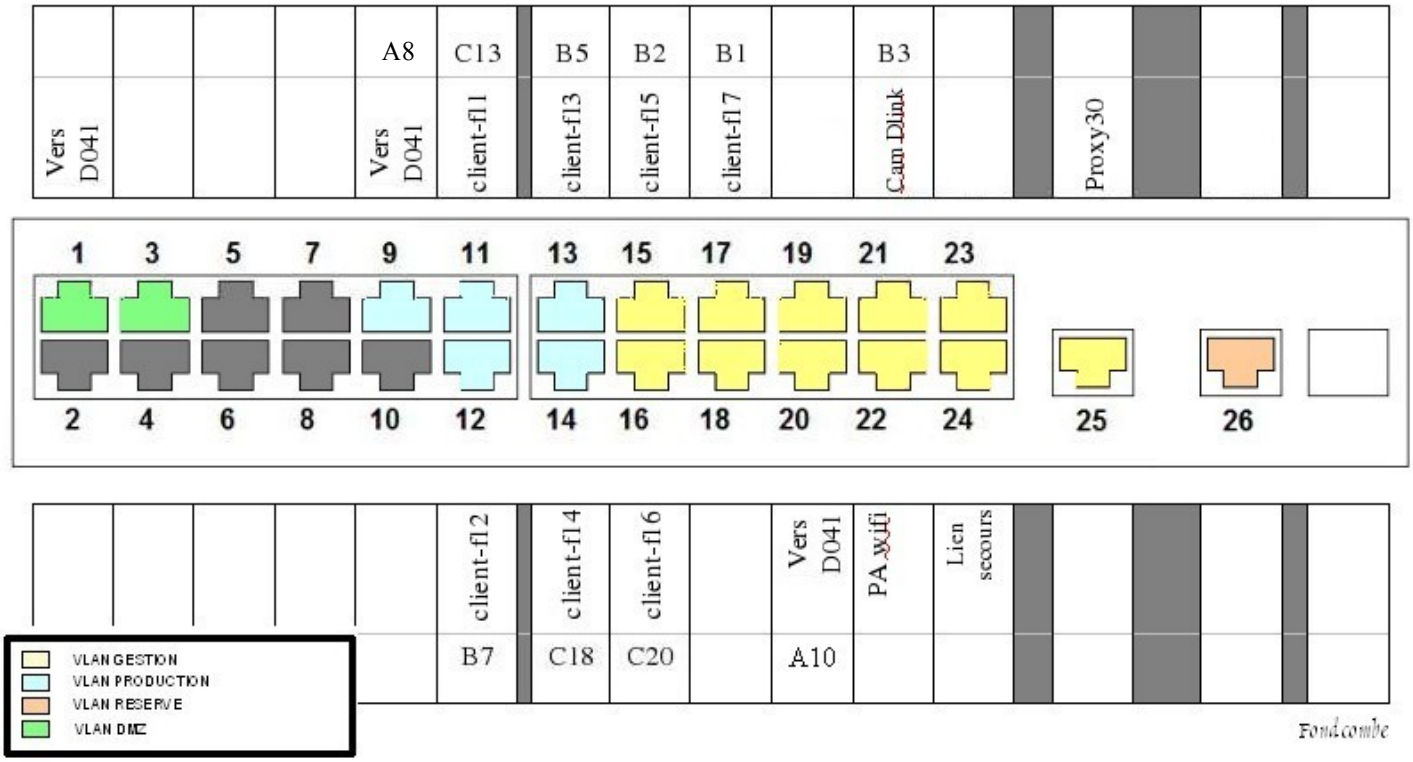
	Solo	frodon	client-i1 client-f11	client-i5 client-f15 ← ***Source du ping***
client-i1 client-f11 ___ .___ .___ .___				
client-i5 client-f15 ___ .___ .___ .___				

Qu'en concluez-vous ? A quelle condition deux machines peuvent-elle communiquer entre elles ? : _____

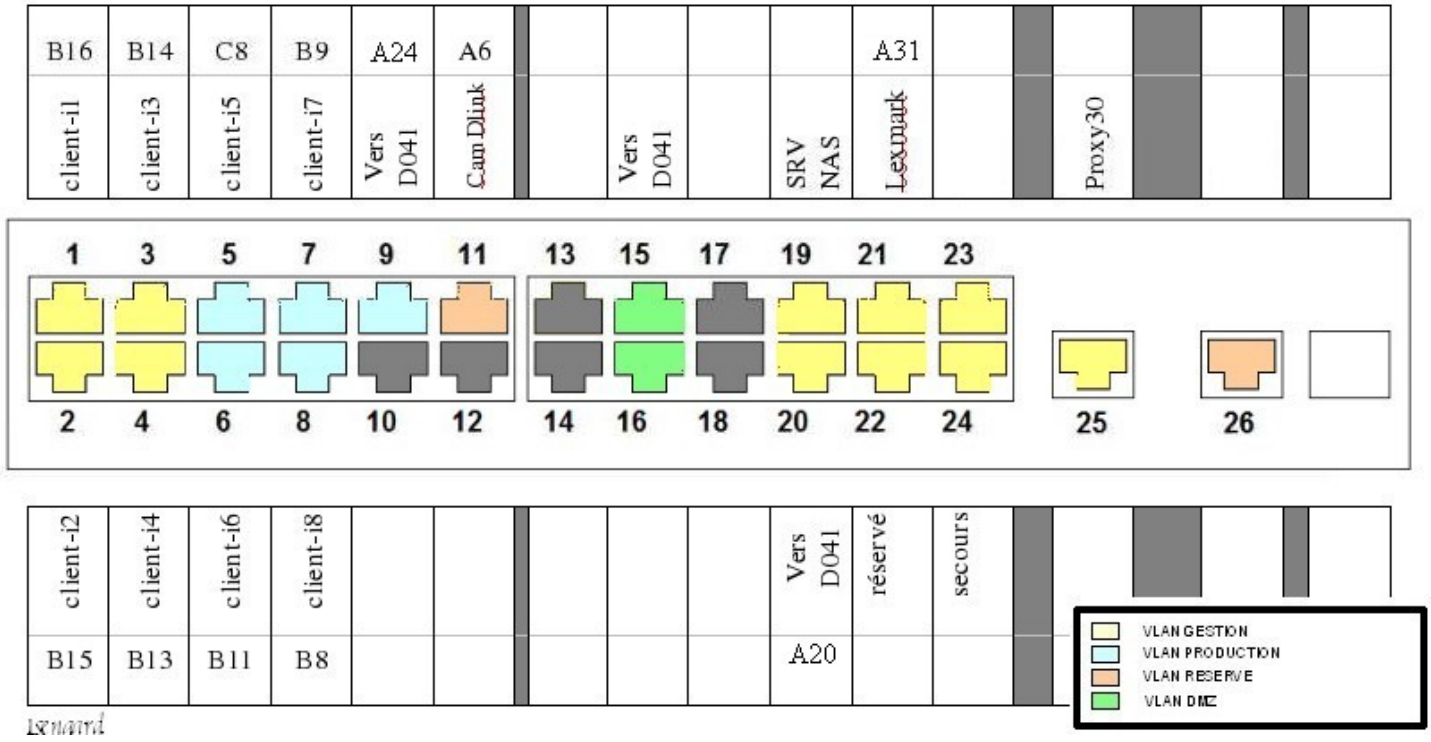
_____

Est-il possible de « pirater » en prenant une adresse IP dans l'autre groupe de machine ? :_____

Annexes 1 : schéma de brassage des NETGEAR FS726



COMMUTATEUR NETGEAR FONDCOMBE (192.168.7.249)



COMMUTATEUR NETGEAR ISENGARD (192.168.7.248)

Annexes 2 : schéma de brassage des D-LINK 1228

COMMUTATEUR D-LINK 1228 (10.0.0.250)

Remarque : le port 2 est relié au panneau de brassage A20 sur Isengard et A10 sur Fondcombe

Remarque : le port 24 est relié au panneau de brassage A24 sur Isengard et A8 sur Fondcombe

Annexes 3 : Attribution des VLAN – site de fondcombes