BAC PRO SEN TR
module « actifs Ethernet »

TP : Configurer les VLAN (niveau 1)

Nom : _____ **Prénom :** _____ **Classe :** **Date :**	**Appréciation** :	**Note** :
Objectifs : - Être capable d'effectuer le brassage Ethernet (Compétence C4-2) - Être capable de configurer les VLANs par port (Compétence C4-2)		**durée** : 6h

Matériel :

- 4 ordinateurs type "PC"
  - prod-1 : windows xp (machine "fujitsu" dans la salle D041)
  - prod-2 : windows xp (virtuel sur HostVMx dans la salle D042)
  - gestion-1 : windows xp (machine "fujitsu" dans la salle D041)
  - gestion-2 : windows xp (machine "fujitsu" à déplacer dans la salle D042)

- 1 commutateur Ethernet DLINK 3628
- 1 commutateur Ethernet DLINK 1228
- 4 cordons de descente
- 8 cordons de brassage

Travail à réaliser :

Avant de commencer le tp (page 4), vous devez au préalable **configurer vos 4 pc** avec les paramètres IP indiqués sur le schéma de la page 2 (attention aux masques !!)

Important : vous ne devez configurer aucune "passerelle par défaut" sur ces 4 postes

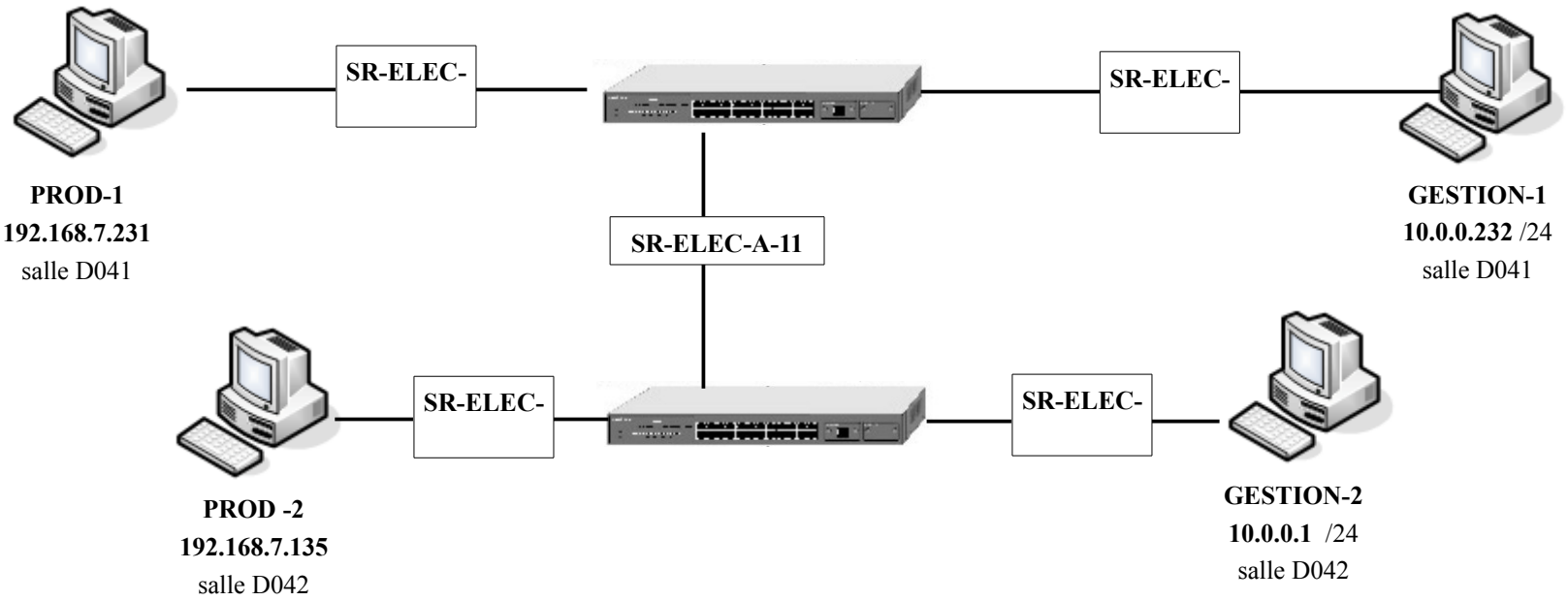
Vous aller ensuite tester la segmentation d'un réseau avec deux méthodes :

- 1ere situation : le réseau est simplement segmenté par des **sous-réseaux** IP
- 2ème situation : le réseau est segmenté par des **vlans** définis sur les commutateurs

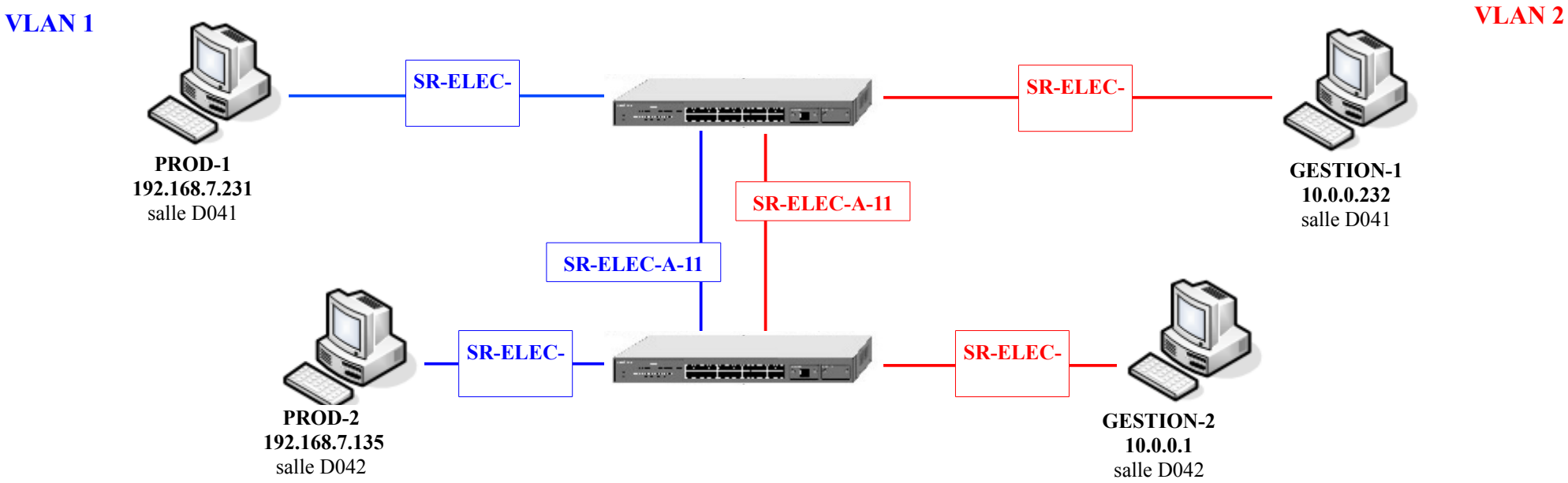
Dans les deux cas, vous testerez l'efficacité de cette segmentation

Le TP comporte aussi des phases théoriques pour vous apporter les savoirs obligatoires sur le sujet

1ERE SITUATION : 2 SOUS-RESEAUX IP



2EME SITUATION : 2 SOUS-RESEAUX VLAN



1ère situation : Segmentation en sous-réseaux IP

Mettre deux ordinateurs d'un réseau dans 2 sous réseaux différents a pour but de les empêcher de communiquer. On peut avoir plusieurs raisons à cela :

- ✔ Diminuer la taille des domaines de diffusion
- ✔ La sécurité des données (les machines appartiennent à des services ou propriétaires différents)

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

➔ 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

Source du ping

		gestion-1
prod-1	____ .____ .____ .____	
prod-2	____ .____ .____ .____	
gestion-1	____ .____ .____ .____	
gestion-2	____ .____ .____ .____	

➔ Expliquez ces résultats :_____

_____

➔ La machine **gestion-1** a pour adresse ip : 10.0.0.232 et le masque : 255.255.255.0

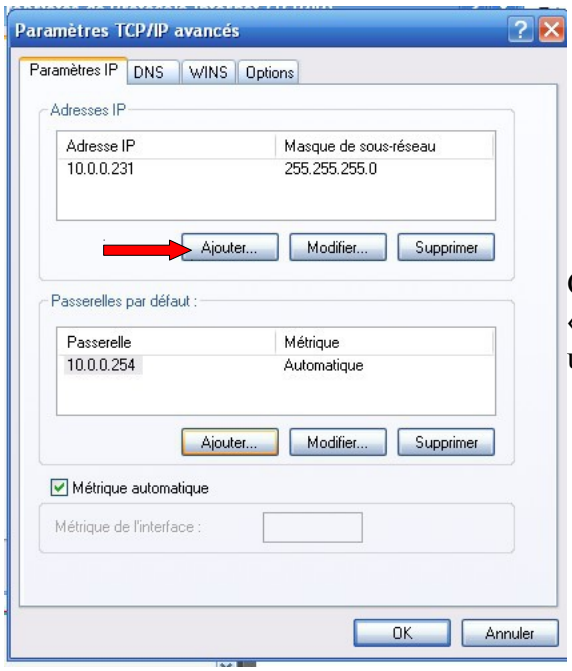
Elle appartient donc au réseau IP : _____ ._____ ._____ .0

➔ La machine prod**-1** a pour adresse ip 192.168.7.231 et le masque : 255.255.255.0

Elle appartient donc au réseau IP : _____ ._____ ._____ .0

➔ Vous allez ajouter une seconde adresse IP à la machine **Gestion-1** pour lui donner accès au réseau **"prod"**

- Ouvrir les propriétés TCP/IP de la carte Ethernet
- Cliquez sur « Avancé... » comme ci-dessous :



Cliquez sur « Ajouter » une adresse IP

- La machine **Gestion-1** a maintenant 2 adresses IP : 10.0.0.232 et 192.168.7.232. Faisons à nouveau des ping entre les différentes machines et remplissez le tableau :

Destination du ping

	gestion-1
prod-1 ____ .____ .____ .____	
prod-2 ____ .____ .____ .____	
gestion-1 ____ .____ .____ .____ ____ .____ .____ .____	
gestion-2 ____ .____ .____ .____	

Source du ping

➔ Conclusion : la méthode de segmentation par sous-réseaux IP vous parait-elle totalement fiable ?

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

2ème situation : Segmentation en VLANs - théorie

➔ 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.

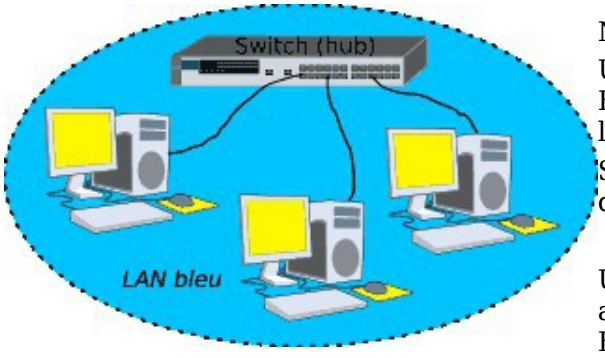
L'inconvénient de ces trames est qu'elle ont tendance à polluer le réseau, comme la publicité dans les boites aux lettres car elles sont envoyées même à ceux qui ne sont pas concernés. De même que la publicité peut saturer votre boite aux lettres, les trames de broadcast peuvent finir par saturer un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



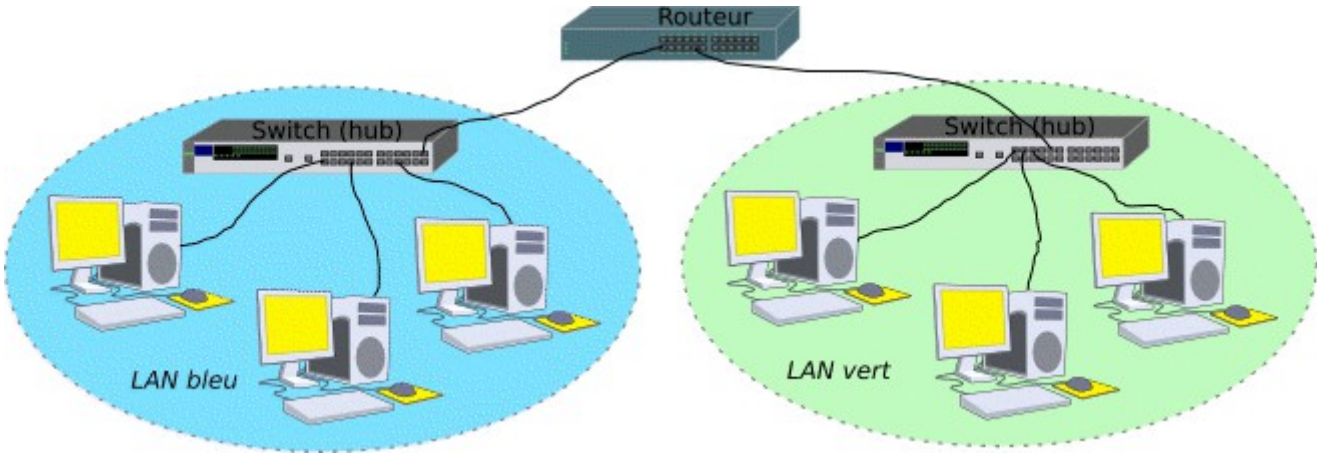
Nous sommes ici sur un réseau Ethernet.

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.

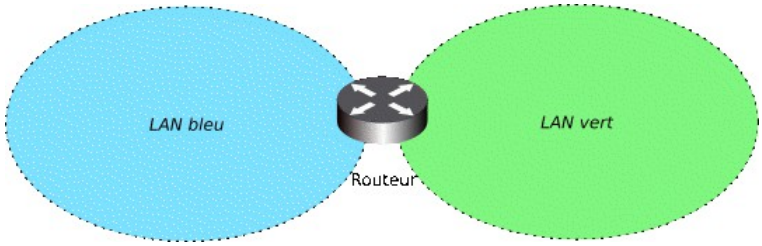
Si nous avons affaire à un SWITCH, seules les trames de diffusions (broadcast) seront visibles depuis tous les noeuds,

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

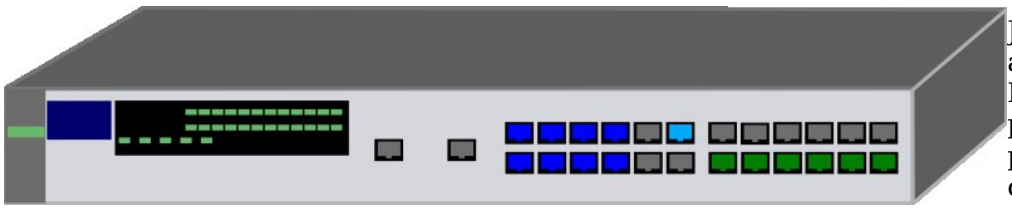


Lorsque nous avons deux LANs et que nous souhaitons les inter-connecter, tout en conservant dans chaque LAN les mêmes propriétés au niveau Ethernet, nous devons faire appel à la couche 3 (IP) pour assurer l'interconnexion : il nous faut donc **un routeur**.



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 »

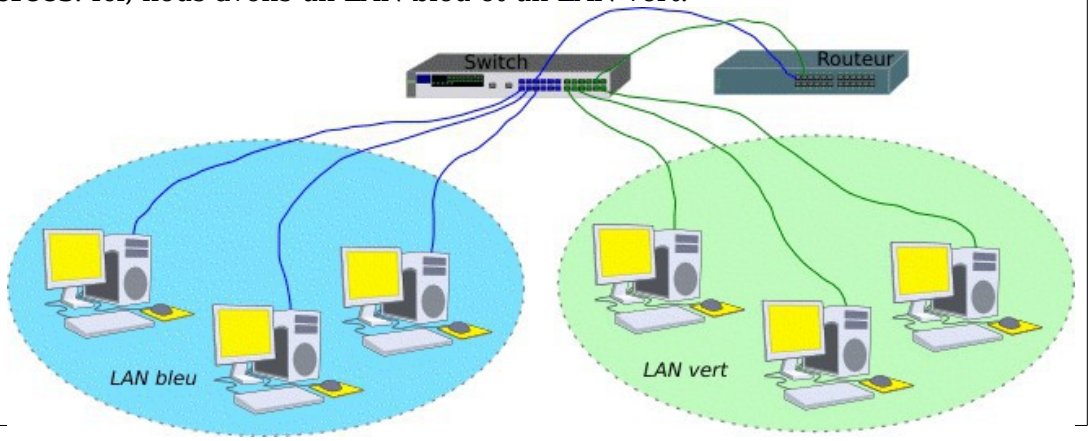


Jusqu'ici, un SWITCH appartenait à un et un seul LAN. L'idée de base est de pouvoir assigner certains ports du SWITCH à un LAN, certains autres ports à un autre LAN etc :

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 (voir les encadrés pages 6-8) ?

_____

_____

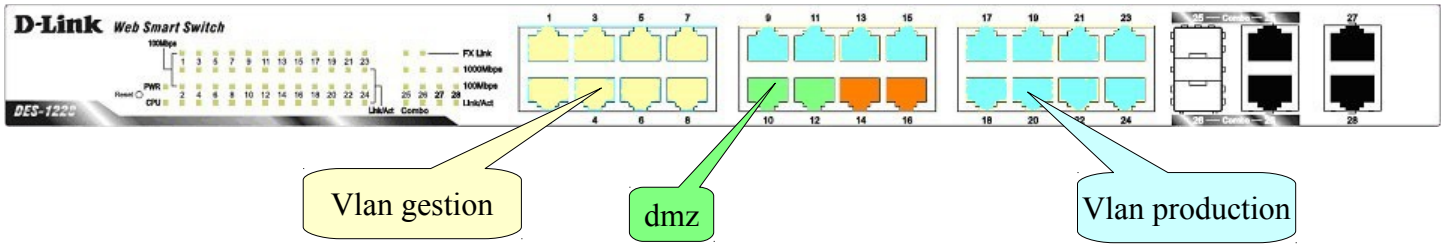
_____

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

2ème situation : SEGMENTATION EN VLANS - MISE EN PRATIQUE

- Le document ci-dessous représente l'affectation des ports des switches au différents VLAN (les 2 swtiches seront configurés de la même facon)



Configuration du commutateur D-LINK 1228

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

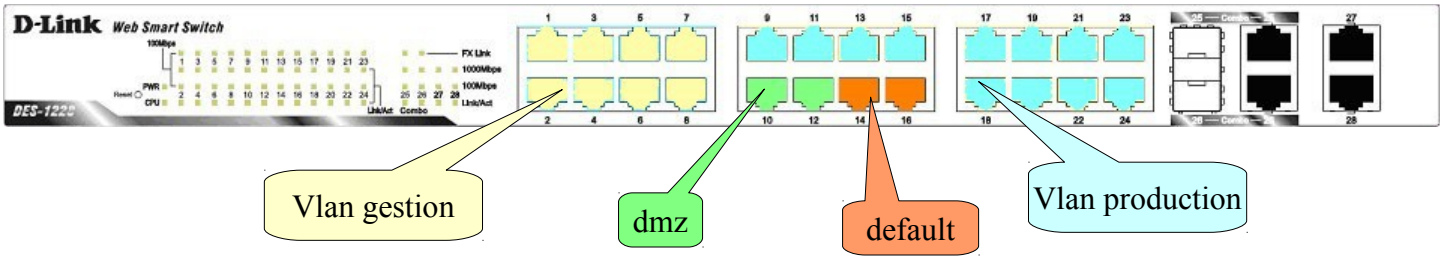
Information : la connexion série ou RS232C et Hyperterminal
Les commutateurs administrables possèdent (presque) tous un mode dit « console » qui permet d'accéder à l' interface d'admin, même si on ne connaît pas sa configuration IP

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)** :

➔ Réalisez maintenant la configuration du switch DLINK 1228 à l'aide de la documentation et du cahier des charges ci-dessous:



- 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

Coller ici la copie d'écran
montrant l'ensemble
des vlans
configurés sur le commutateur

Configuration du commutateur D-LINK 3628

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

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 : _____

➔ Réalisez maintenant la configuration du switch DLINK à l'aide de la documentation et du cahier des charges ci-dessus:

Coller ici la copie d'écran
montrant l'ensemble
des vlans
configurés sur le commutateur

➔ Refaire le brassage des postes de façon à ce que **prod-1** et **prod-2** soient sur le vlan "prod" et de façon à ce que **gestion-1** et **gestion-2** soient sur le vlan "gestion"

>>>>Avant de continuer, appelez le professeur pour valider le brassage<<<<

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

Note : la machine *Gestion-1* possède toujours deux adresses ip : une dans *gestion* et une dans *prod* (voir p.7)

Destination du ping

	Gestion-1	Prod-1
Prod-1		
Prod-2		
Gestion-1		
Gestion-2		

Source du ping

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 ? :_____

Annexe 1 : Fiche d évaluation

Note : cette fiche sert à votre auto-évaluation en phase formative.

Item évalué	page	réponse attendue / critères évalués	
tableau de ping	4	non, non, ok ,ok	
Expliquez ces résultats	4	ne communique qu'avec les machines du même réseau ip	
réseau de gestion-1	4	10.0.0.0	
réseau de prod-1	4	192.168.7.0	
tableau de ping	5	ok,ok,ok,ok	
fiabilité de la méthode ?	5	permet le "piratage" et le broadcast de niveau 2	
savoir : Qu'est-ce qu'un VLAN	6	Virtual Local Area Network Cela permet de segmenter le domaine de broadcast	
savoir : 3 types de VLAN : critère de segmentation	6	VLAN par : - port- adresse MAC- adresse IP	
savoir : qu'est-ce qu'une trame de broadcast ?	6	Une trame de broadcast est destinée à toutes les machines du réseau.	
savoir : broadcast à travers vlans ?	6	Non, ces trames ne peuvent pas traverser les vlans	
savoir : protocoles qui utilisent du broadcast	6	Netbios (réseau Microsoft), requete DHCP	
savoir : pour faire communiquer 2 vlans	6	il faut utiliser un routeur, ou la fonction de routage intégrée sur certains commutateurs de niveau 3	
savoir : utilité de la segmentation en vlan	8		
s'informer : adresse ip du commutateur	9	demandée au professeur	
s'informer : procédure	9	consultation et extraction de la documentation appropriée	
configurer : 3 vlans sur le commutateur	10	respecter le cahier des charges	
s'informer : procédure	11	consultation et extraction de la documentation appropriée	
configurer : 3 vlans sur le commutateur	11	respecter le cahier des charges	
installer les supports	11	réaliser le brassage; postes connectés aux bons vlans (ports), 2 liens entre les deux commutateurs	
tableau de ping	12	ping uniquement à l'intérieur du vlan	
conclusion	12	sous-réseaux parfaitement "étanches"	