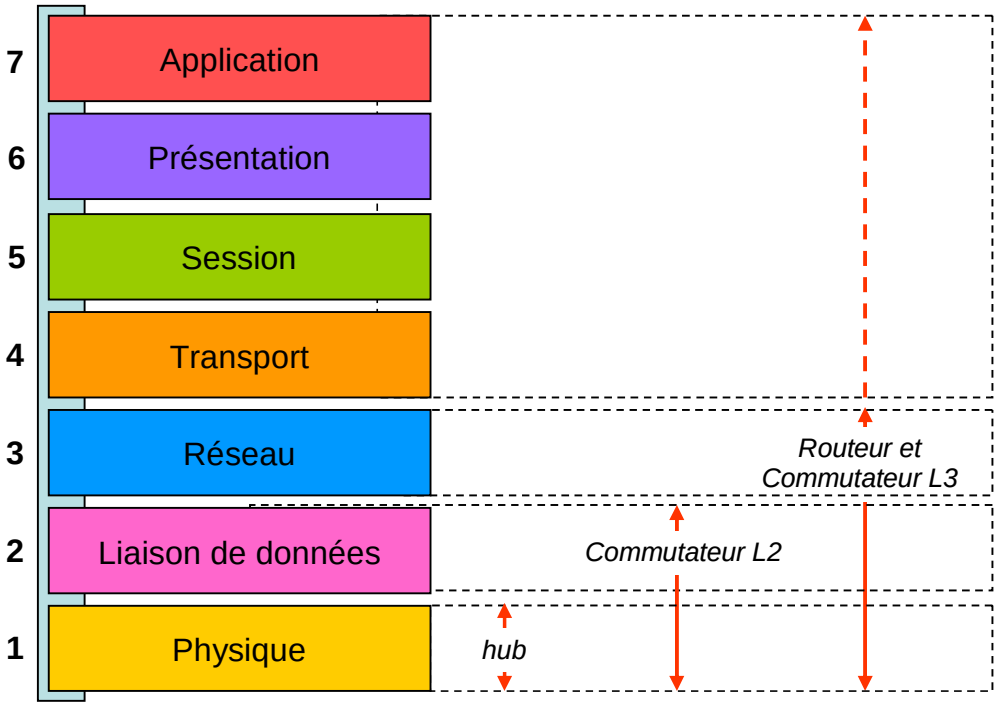
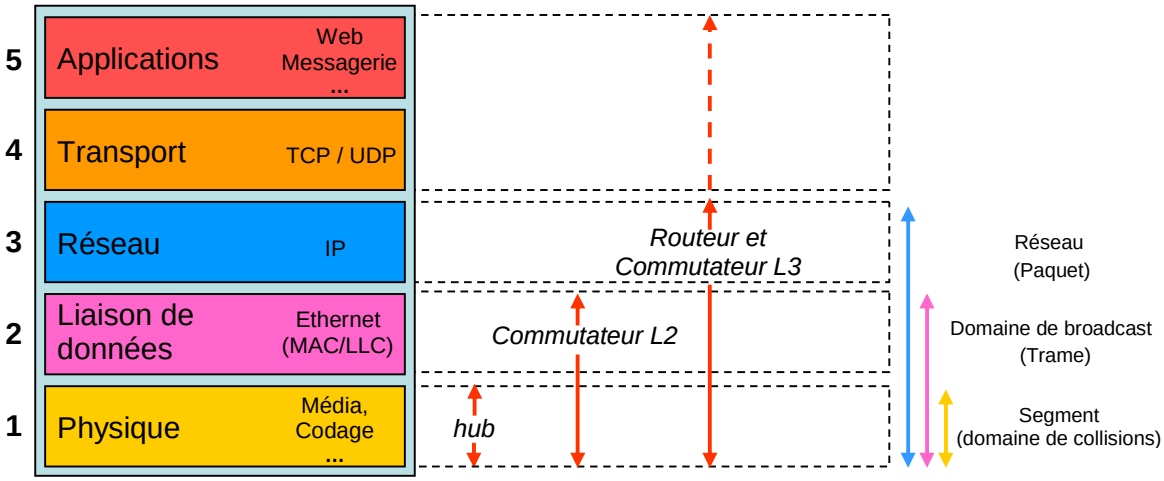
Activation

Rappels :

Modèle OSI



Modèle TCP/IP



- Le protocole réseau le plus utilisé est, de très loin, IP (Internet Protocol). c'est alors le schéma ci dessus qui modélise l'architecture en place.
- Les autres protocoles réseaux parfois rencontrés sont : IPX, Appletalk, DECnet

Hubs, Switch, Switch manageables niv2, 3, 4

1. Management de Switchs :

Connexion par port console avec un cordon Null-modem et l'utilisation d' **Hyper Terminal** afin d'affecter une adresse IP au Switch :

Lorsque le commutateur est en configuration usine seul une connexion par le port console est possible. C'est donc ce moyen qui doit être utilisé pour attribuer les paramètres IP au module d'administration.

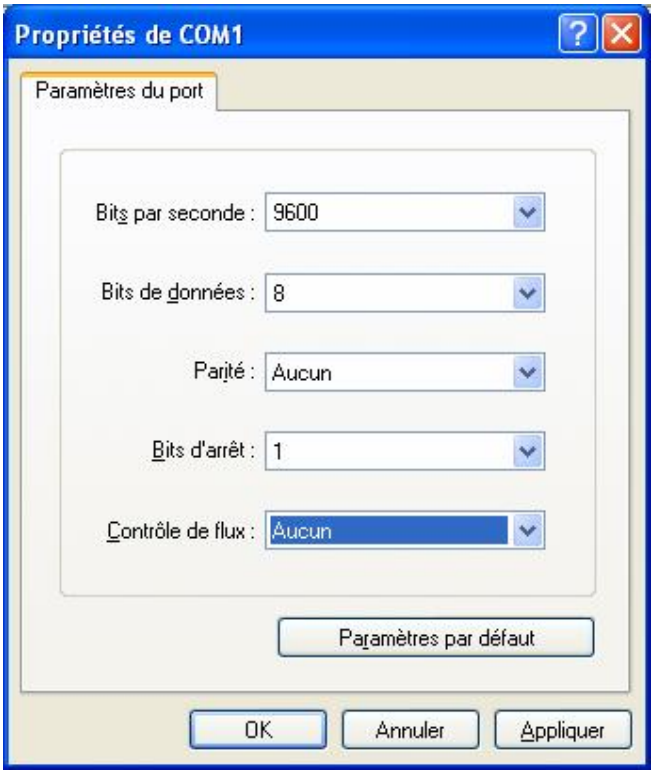
Utiliser le câble console fourni en le connectant d'un port au port RS232 (DB9) et d'autre part au port COM d'un PC. A l'aide d'un utilitaire d'émulation de terminal tel que HyperTerminal (livré avec Windows), créer une nouvelle connexion ayant les caractéristiques suivantes:

Paramètre	***Valeur***
Vitesse	De 1200 à 115200 bps (défaut 9600)
Bit de données	8
Parité	Aucune
Bit de top	1
Contrôle de flux	Aucun
Type d'émulation	VT100

a - Donner un nom à la connexion et choisir une icône

b- Sélectionner le port Com à utiliser

c- Entrer les paramètres de la connexion



d- Modifier le mode d'émulation

Une fois cette connexion créée et activée, appuyer sur la touche « Entrée » deux fois pour faire apparaître l'écran suivant :

```
Connected to serial port at 9600 bps baud rate

Local User Access Verification:

Login:
```

Entrer alors les informations de login et mot de passe. Lors de la première connexion sur un commutateur en sortie d'usine, utiliser les paramètres suivants :

- login : **manager**
- mot de passe : **friend**

Il vous sera possible par la suite de changer ce mot de passe. Pour des raisons de sécurité, ceci est fortement recommandé.

1.1. Interface de commande et de configuration

Le menu principal (***Main Menu***) du commutateur est présenté ci-dessous. C'est la version 3.20 (ATS-39 3.2.0) du système d'exploitation sur un AT-8024M qui est présentée. Toutefois, tous les commutateurs de la série AT-8000 utilisent la même image de système et, par conséquent, présentent la même interface de configuration. Le passage d'un modèle à un autre ne modifie pas l'ergonomie et les fonctionnalités proposées.

```
                Allied Telesyn Ethernet Switch AT-8024M - AT-S39 v3.2.0
                                <No System Name>
Login Privilege: Manager
                                    Main Menu

1 - Port Menu
2 - VLAN Menu
3 - Spanning Tree Menu
4 - Administration Menu
5 - System Config Menu
6 - MAC Address Tables
7 - Ethernet Statistics
8 - Diagnostics
9 - Enhanced Stacking
C - Command Line Interface

Q - Quit

Enter your selection?
```

Intitulés et significations du menu principal

Intitulé	*Signification*
Port Menu	Configuration de ports : - Recopie de port. - Agrégation de lien. - Vision de l'état de l'ensemble de ports. - La sécurisation des ports
VLAN Menu	Configuration des VLAN : - Status du VLAN. - Création, configuration et suppression de VLAN. - Configuration de ports du VLAN et les priorités.
Spanning Tree Menu	Configuration du Spanning Tree.
Administration Menu	Configuration IP de l'agent: - Adresse IP - Masque de sous réseau - Passerelle - Le nom du système, etc
System Config Menu	Configuration système du commutateur : - Temps d'inactivité des adresses MAC. - Le mode du commutateur (Tagged ou Basic). - Le temps d'inactivité en mode console. - Le statut du serveur WEB. - Le statut de l'agent SNMP
MAC Address Tables	Configuration de la table d'adresses MAC : - Montre toutes les adresses MAC. - Ajoute une adresse MAC statique. - Supprime une adresse MAC. - Supprime toutes les adresses MAC. - - Montre toutes les adresses MAC statiques, etc
Ethernet Statistics	Configuration des statistiques Ethernet : - Statistiques par port. - Initialisation de statistiques. - Affichage de statistiques
Diagnostics	Affichage de informations du commutateur.
Enhanced Stacking	Configuration de la supervision de plusieurs commutateurs AT-8000 reliés entre eux via la technologie Enhanced Stacking™
Command Line Interface	Permet de taper des lignes de commandes.

La navigation se fait par des séquences de contrôle suivantes:

- **Numéro** : en renseignant le numéro du menu, on entre dans celui-ci.
- **R** : retour au menu précédent.
- **Q** : ferme la session de supervision.
- **S** : sauvegarde les modifications (à effectuer après chaque phase de configuration lorsque cette option apparait)
- **Entrée** : valide un choix

1.2. Configuration IP

Entrer dans le menu **Administration Menu** pour réaliser le paramétrage IP du commutateur.

```
          Allied Telesyn Ethernet Switch AT-8024M - AT-S39 v3.2.0
                          <No System Name>
Login Privilege: Manager
                       Administration Menu

1 - IP Address ........ 192.168.0.1
2 - Subnet Mask ....... 255.255.255.0
3 - Default Gateway ... 192.168.0.254
4 - System Name .......
5 - Administrator .....
6 - Comments ..........
7 - Set Password ......
8 - BOOTP/DHCP ........ Disabled

9 - Reset Switch
A - Server-based Authentication
D - Downloads & Uploads
P - Ping a remote system

R - Return to Previous Menu

Enter your selection?
```

Saisir la configuration IP du commutateur, comme par exemple ci-dessous :

IP Address :	[**192.168.0.1**]
Subnet Mask :	[**255.255.255.0**]
Default Gateway :	[**192.168.0.254**]

De manière optionnelle, il est également possible via cet écran de modifier les paramètres System Name, Administrator et Comments afin de renseigner le nom et l'emplacement du commutateur, la personne physique chargée de son administration, etc…

Une fois que les paramètres souhaités sont entrés, appuyer sur la touche S pour sauvegarder la configuration. Quitter le menu **Administration Menu** en appuyant sur R pour revenir au menu **Main Menu** puis appuyer sur Q pour clôturer la session d'administration.

Important : dans le but d'éviter les conflits d'administration, seule une session peut être ouverte à la fois. Il est donc nécessaire de fermer proprement une session tel qu'indiqué ci-dessous sous peine de ne pouvoir se connecter par un autre moyen pendant quelques minutes (par défaut 5 mn).

L'ensemble de la configuration du commutateur peut être effectuée à travers ces menus. Toutefois, pour des raisons d'ergonomie, la méthode de configuration décrite dans ce document s'appuie sur l'interface Web qui est décrite par la suite.

Port trunking

Configuration des ports : Port Trunking

Le port trunking ou agrégation de liens permet de constituer un lien logique à partir plusieurs liens physiques qui interconnectent des commutateurs. Ceci impose que les deux commutateurs utilisent le même protocole et de configurer ces deux commutateurs avant de les connecter physiquement.

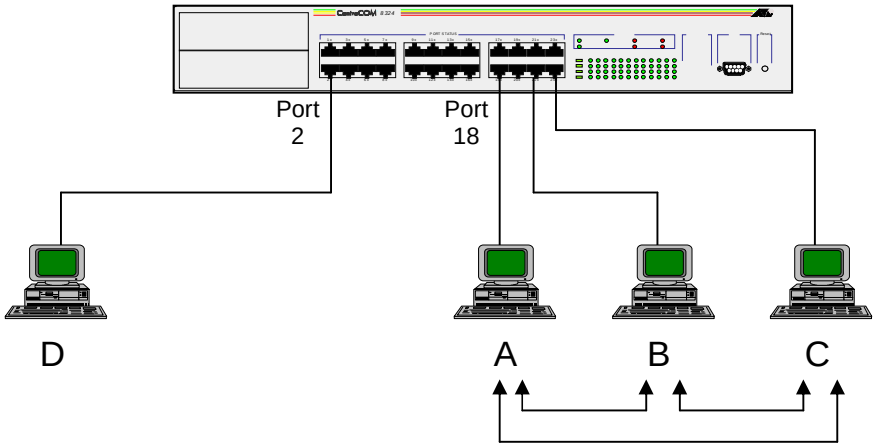
-> augmentation de la bande passante (débit)
-> redondance de lien
-> répartition de charge

Trunk sur 2 ports 100 Mbs FD ce qui donne une bande passante de 200 Mbs FD entre les deux commutateurs.
La configuration doit être symétrique sur les deux commutateurs
Le raccordement ne doit être fait qu'après la configuration.

Le nombre de trunk possible ainsi que le nombre de port pouvant être agrégé dans un trunk varie en fonction de l'équipement. Les N° de port qui peuvent être associés sont également soumis à des contraintes qui dépendent de l'équipement.

Configuration des ports : Port Mirroring

- Au contraire de ce qui se passe sur un concentrateur, le trafic transitant entre deux ports d'un commutateur n'est pas répercuté sur les autres.
- Le Port Mirroring permet de répercuter le trafic transitant par un port sur un autre port.



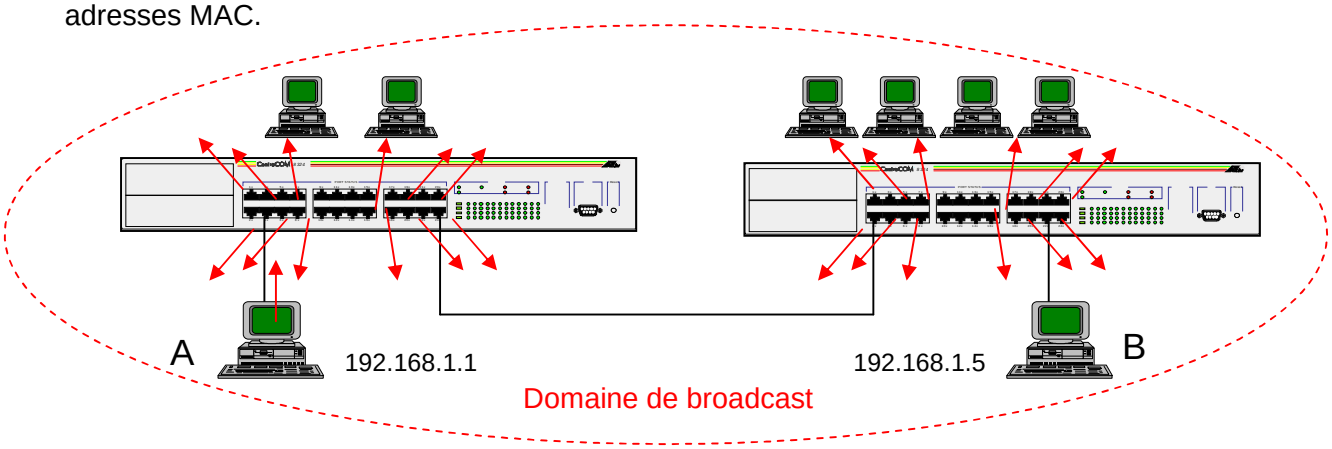
Le port 18 est « mirroré » sur le 2

Equipée d 'un analyseur de protocole (sniffer), la station D peut visualiser les échanges entre A et B, A et C mais pas ceux entre B et C

(Virtual Local Area Network)

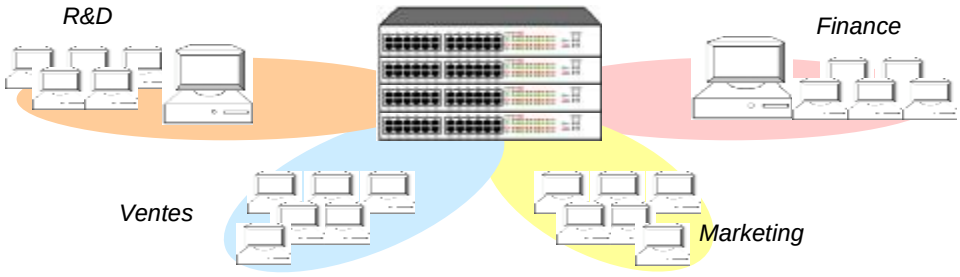
Les échanges broadcast

- Broadcast = trame envoyée par un équipement à l'ensemble des équipements interconnectés au niveau 2.
- Le broadcast est un mécanisme indispensable pour effectuer une correspondance entre l'adresse de niveau 3 (adresse IP) et l'adresse de niveau 2 (adresse MAC).
- Sur un réseau Ethernet, deux stations qui communiquent doivent mutuellement connaître leurs adresses MAC.



VLAN par port

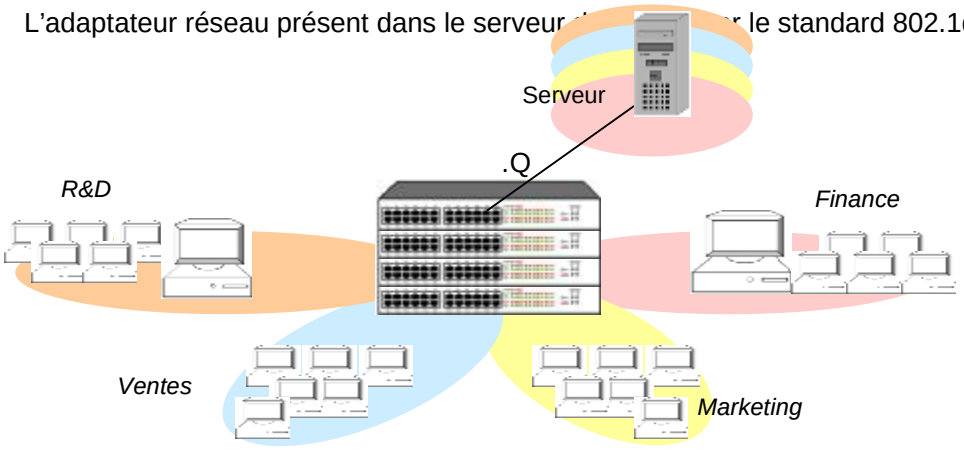
- Constituer des VLAN par port permet de créer des groupes logiques de stations.
- **<u>Un VLAN définit un domaine de broadcast</u>**
- La communication entre membres de VLANs différents n'est pas possible sans utiliser un équipement de niveau 3.
- Objectif :
  - Sécurité par cloisonnement du trafic.
  - Mutualisation des ressources (actif/passif).
  - Performance, grâce au contrôle des broadcasts.



- Les ports sont groupés de manière logique pour former les VLANs

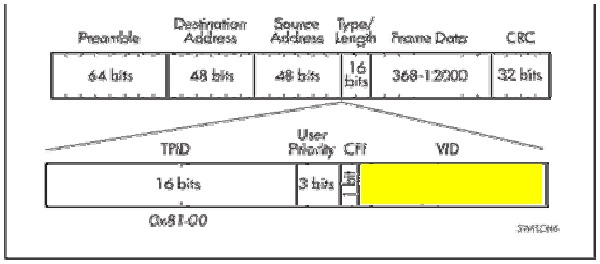
VLAN Tagging

- Un VLAN est caractérisé par un identifiant numérique (VID).
- Le partage d'une ressource telle qu'un serveur entre des VLANs peut être fait grâce au VLAN tagging (IEEE 802.1q).
- Dans ce cas, le port auquel est attaché cette ressource est ajouté dans tous les VLAN qui doivent y accéder en indiquant que ce port doit marquer les trames émises avec l'identifiant du VLAN d'où a été initiée la connexion.
- L'adaptateur réseau présent dans le serveur [illegible] le standard 802.1q

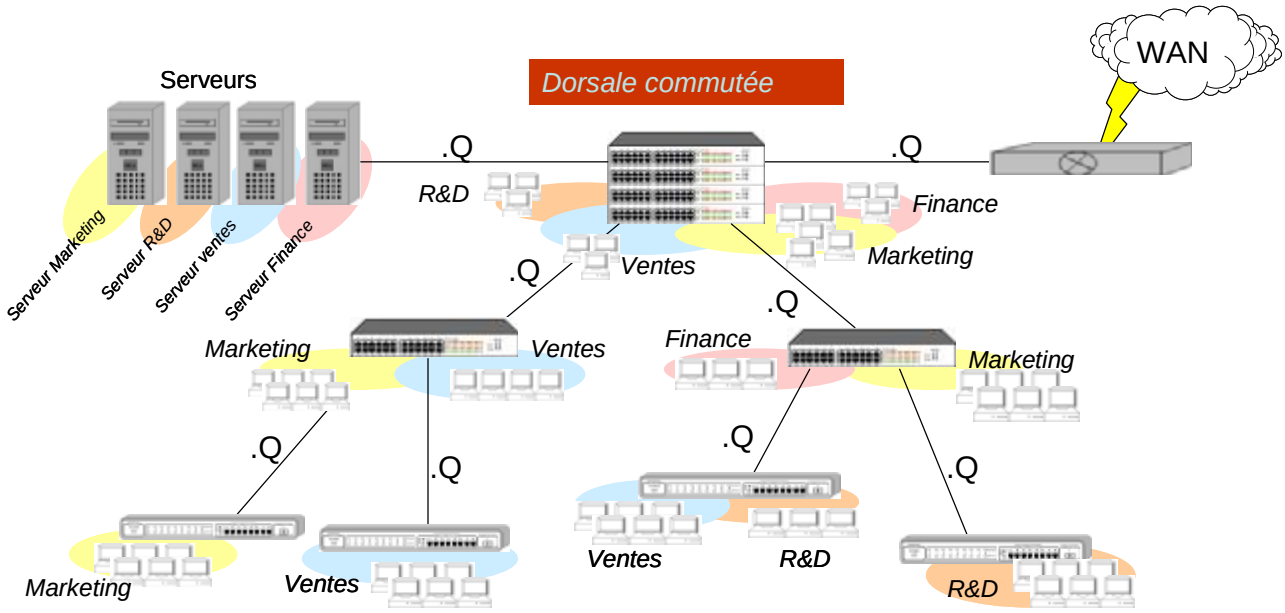


VLAN Tagging (802.1q)

- Le VLAN tagging permet de véhiculer l'identifiant du VLAN d'où a été initiée la communication.
- Lors du marquage, 4 octets sont ajoutés à l'entête Ethernet entre l'adresse source et le champs type :
  - 2 octets pour indiquer que c'est une trame taggée (0x81-00)
  - 2 octets que l'on peut découper du poids fort au faible en :
    - 3 bits User tag priority field (priorité 802.1p)
    - 1 bit CFI
    - 12 bits pour l'identifiant de VLAN (VID) soit 4096 ID possibles.
- Cela implique que la taille maximale d'une trame Ethernet taggée passe de 1518 octets à 1522 octets, la taille mini ne change pas.

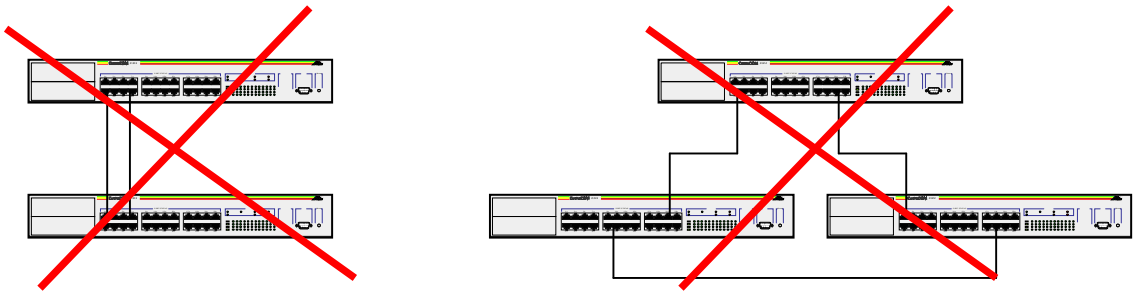


VLAN Tagging



Spanning Tree

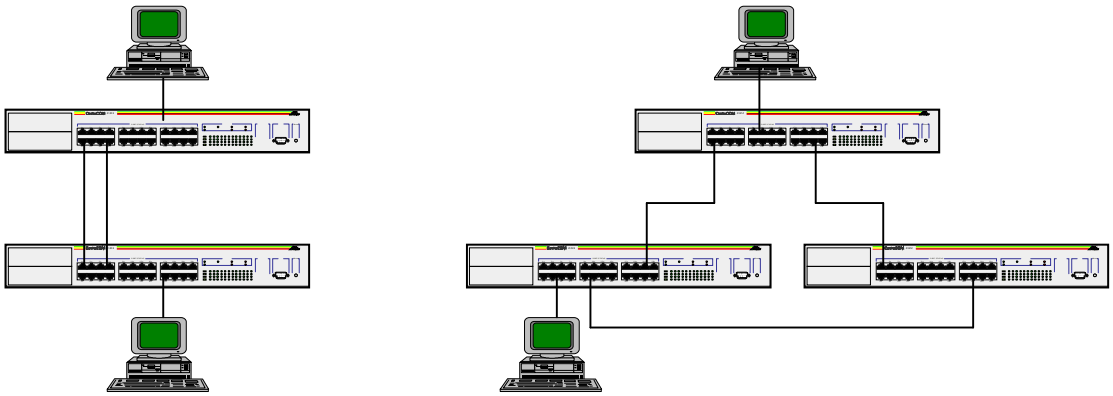
- Ethernet ne permet pas la mise en place de boucles. Entre deux équipements il ne doit exister qu'un seul chemin possible.



(Sauf s'il sagit d'un trunk)

Spanning Tree (IEEE 802.1D)

- Le protocole Spanning Tree permet de mettre en place une topologie à liens redondant.



- Il est donc possible de mettre en place une redondance de lien qui permet de faire face à une défaillance de lien ou de matériel
- seul un chemin est actif à la fois.

Spanning Tree (802.1d)

Configuration des paramètres de spanning tree du commutateur

Bridge Priority : **32768**

Ce paramètre peut être compris entre 0 et 65535. 0 est la priorité la plus forte. 32768 est la valeur que l'on retrouve par défaut. C'est le commutateur qui possède la priorité la plus élevée qui est élu « root bridge ». En cas de priorité égale c'est le commutateur possédant l'adresse MAC la plus faible qui est élu.

*** Bridge Maximum Age :** **20 Sec.**

C'est la durée de vie d'un message de configuration dans un commutateur. Passé le délai fixé, le commutateur efface le message de configuration. La valeur peut être fixée de 6 à 40 sec. La valeur par défaut est de 20 sec.

*** Bridge Hello Time :** **2 Sec.**

C'est l'intervalle de temps qui sépare l'émission des message de configuration (BPDU : Bridge Protocol Data Unit). Sa valeur peut être comprise entre 1 et 10 sec. La valeur par défaut est 2 sec.

*** Bridge Forward Delay :** **15 Sec.**

Cela indique le temps d'attente avant que le commutateur ne change d'état. Par exemple pour qu'il devienne le nouveau root bridge après un changement de topologie. La valeur par défaut est de 15 sec.

* Les valeurs par défauts sont généralement bien adaptées. Des modifications ne doivent être faites qu'avec la plus grande prudence.

Spanning Tree (802.1d)

Configuration des paramètres de spanning tree pour les ports

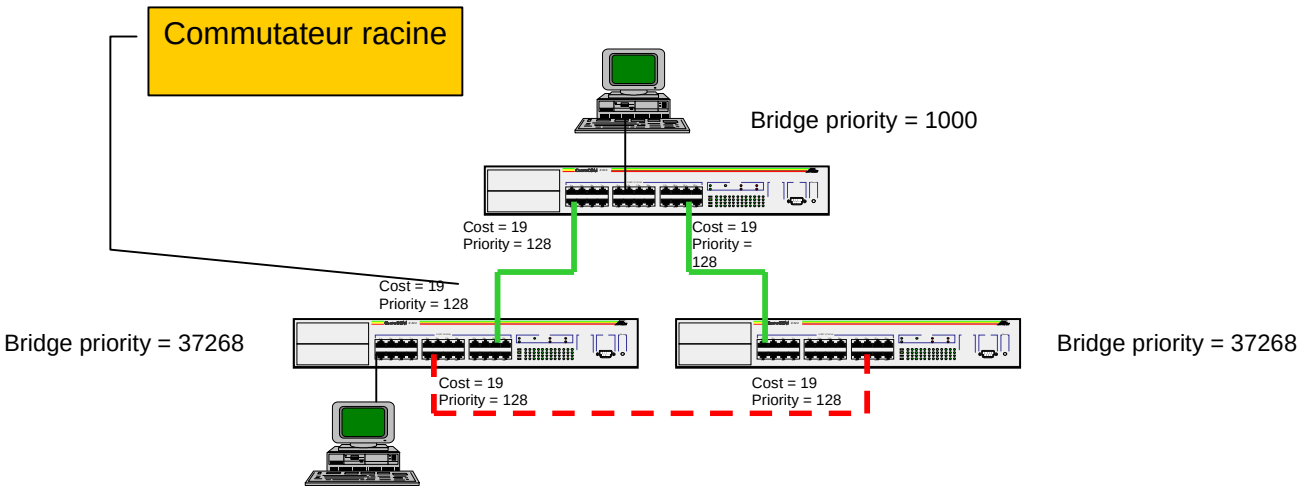
Cost

Permet de fixer un coût au port. Le spanning tree utilise ce paramètre pour déterminer le coût global du trajet si ce port conduit directement ou au travers d'autres commutateurs vers le root bridge. Si plusieurs ports conduisent au root bridge sur un même commutateur, c'est celui qui propose le coût le moins élevé qui est activé. Le ou les autres sont bloqués. Par défaut tous les ports d 'un même commutateur ont la même valeur. Le coût peut aller de 1 à 65535.

Priority

Ce paramètre permet de départager les ports d 'un commutateur dont le chemin vers le root bridge a un coût égal. Sa valeur peut aller de 0 à 255 et la valeur par défaut est de 128. Si il y a égalité sur cette valeur, c'est le port ayant l'adresse MAC la plus faible qui est élu « root port ».

Spanning Tree (802.1d)



- Pour chaque commutateur c'est le lien qui présente le coût le plus faible vers le commutateur racine qui est activé

- Si pour un même commutateur plusieurs ports présentent un coup identique c'est la valeur de priorité qui les départage puis, si cela ne suffit pas, le plus petit N° de port est choisi.

Routage inter VLAN (niv3)

Gestion de qualité de service (QoS)

Les AT-8500 gèrent les signalisation 802.1p et Diffserv. Ainsi, une trame arrivant marquée au niveau du commutateur est placée dans l'une des quatre files d'attente du port de sortie correspondant à son niveau de priorité. Le mappage par défaut des classes de service (CoS) répond aux préconisations IETF à savoir :

CoS	File d'attente
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

La file d'attente 0 étant la moins prioritaire et la file 3 la plus prioritaire. Le vidage des files d'attente peut être assuré au choix selon les algorithmes :

Priorité stricte (Strict Priotity Queuing): Tant que des trames sont présentes dans la file de plus haute priorité, elles sont émises puis l'on passe à la file de priorité directement inférieure et ainsi de suite. Dès que des trames sont de nouveau présentes dans une file d'attente de niveau supérieur à la file en cours de traitement, le vidage de cette file s'arrête pour laisser la mains à la file de niveau supérieur.

Round Robin Pondéré : Le vidage des files d'attente est alors cyclique. Pour chaque cycle un nombre différent de trames est émis par chaque file. Par exemple la file 3 émettra 12 trames, la file 2 émettre 6 trames, la file 1 émettra 3 trames et la file 0 émettra 1 trame.

Un mécanisme de contrôle de congestion (802.3x Flow Control) peut être activé afin de s'assurer que les files d'attente ne satureront pas.

Outre les capacités décrites ci-dessus, les AT-8500 **peuvent marquer au niveau 802.1p ou Diffserv** un flux classifié via le mécanisme précédemment décrit. Les AT-8500 peuvent ainsi représenter l'entrée du domaine de qualité de service que les trames soient transmises marqués ou non par les équipements terminaux. A noter qu'un niveau de priorité présent au niveau 2 peut être translaté au niveau 3 et vice et versa.

Afin de contrôler au mieux la bande passante disponible sur les liens critiques (liaison montante par exemple), il est possible de définir une limitation de bande passante sur les port en entré jusqu'à une limite basse de 1 Mbs. Il est également possible de définir une limitation de bande passante en sortie jusqu'à une limite basse de 1 Mbs.

Protection contre les attaques dénis de service (DoS)

Les AT-8500 sont les seuls commutateurs de cette catégorie actuellement disponible sur le marché possédant un mécanisme de détection et de protection contre les attaque de type DoS qui seraient dirigé sur leur module d'administration. Ce type d'attaque peut si l'équipement n'est pas protégé conduire à son blocage total. Les attaques de type DoS peuvent avoir pour origine des personnes malveillantes, mais également à l'insu de l'émetteur par le biais de virus ou vers présent sur sa station et qui attaquent au commutateur. Il est à noter que les différents cabinets d'analystes prévoient pour 2004 un accroissement des vers et des virus en comparaison avec les niveaux atteint en 2003 qui était déjà riche en événement de ce type. La protection DoS présente sur les AT-8500 vise à agir de manière complémentaire à tout autre dispositif de sécurité présent sur l'architecture (Firewall, anti virus) sans, bien entendu, les remplacer. Néanmoins, elle apporte une réponse à une source de perte d'exploitation pouvant s'avérer dramatique et qui n'est pas couverte par des moyens traditionnels.

Les six types d'attaque les plus fréquente sont couvertes par la protection DoS intégré aux AT-8500: **SYN-Flood , LAND, IP Options, Teardrop, SMURF, Ping of Death.**