

AFPA DE DUNKERQUE

ADAM Julien

DINH Anthony

# COOKBOOK TSRIT

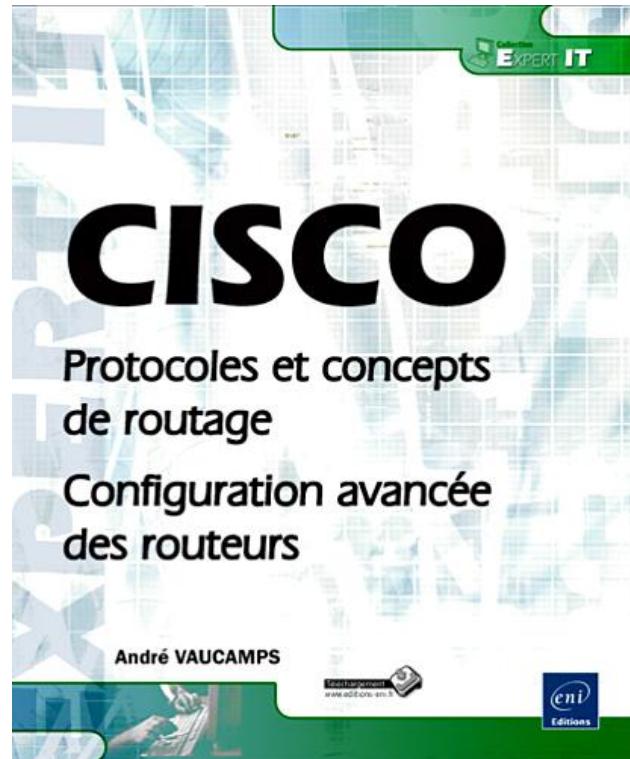
---

TSRIT 2010

16/02/2011

Notre mémoire étant ce qu'elle est, je demande toujours à mes stagiaires de tenir à jour un calepin synthèse de nos travaux et qui doit fournir une information immédiatement utile, une sorte de livre de cuisine (« cookbook ») de l'administrateur réseau. Julien et Anthony sont allés plus loin et en ont fait cette très belle version électronique qui certainement pourra être utile à beaucoup. Qu'ils soient remerciés. André VAUCAMPS.

Pour plus d'informations ou compléter vos connaissances, voici de quoi satisfaire votre curiosité:



(cliquez sur la couverture pour accéder au site)

Le symbole utilisé en page 53 et 54 est l'œuvre de M. Vaucamps André, merci de sa contribution.

« Protocole VTP » provient du PDF de l'Université de Reims Champagne-Ardenne, écrit par F. Nolot.

Le chapitre sur « Domain Name Server » est la création de M. VANLERBERGHE Nicolas.

## QUELQUES COMMANDES DE BASE

---

### CONFIGURATION IP

<b>ipconfig</b>	Résumé.
<b>ipconfig /all</b>	
<b>ipconfig /release</b>	Relâcher l'adresse IP fournie par DHCP.
<b>ipconfig /renew</b>	Renouveler le bail DHCP.
<b>ipconfig /displayDNS</b>	Afficher les correspondances.
<b>ipconfig /flushDNS</b>	Effacer les correspondances.

### CADRE ARP

<b>ARP -a</b>	Afficher les correspondances.
<b>ARP -d</b>	Effacer les correspondances.

### PING

<b>ping @IP -t</b>	Ping étendu. Arrêt via la commande CTRL+C.
--------------------	--------------------------------------------

### NSLOOKUP

<pre>&gt; nslookup www.wikipedia.org Serveur : dns1.proxad.net Address: 212.27.40.240  Réponse ne faisant pas autorité : Nom : rr.esams.wikimedia.org Address: 91.198.174.2 Aliases: www.wikimedia.org rr.wikimedia.org</pre>	<i>nslookup</i> permet donc d'interroger les serveurs DNS pour obtenir les informations définies pour un domaine déterminé. Par défaut <i>nslookup</i> indique les enregistrements A et CNAME du domaine fourni en argument connus du serveur DNS configuré.
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## VMWARE

---

### Ajouter une carte réseau :

Faites un clic droit sur l'onglet de votre machine, puis sélectionner '*Settings*'. Cliquez sur '*Network Adapter*'.

### Changer le type de carte réseau :

Faites un clic droit sur l'onglet de votre machine, puis sélectionner '*Settings*'.

Dans la partie de gauche, cliquez sur '*Network*', cliquez sur '*Network Adapter*', puis dans la partie de droite, faites '*Custom : Specific Virtual Network*', et choisissez une carte réseau du type '*VMNet8*'.

### Partager un dossier entre une machine physique et une machine virtuelle :

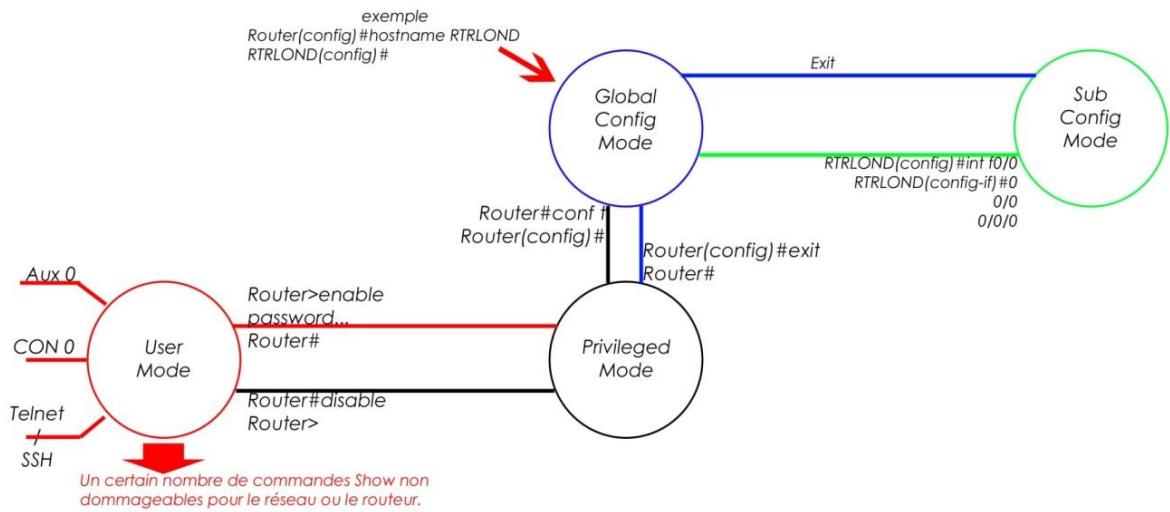
Dans VMware, sélectionner une machine.

Dans l'onglet de gauche '*Commands*', cliquez sur '*Edit Virtual Machine Settings*'. Dans l'onglet '*Options*', sélectionnez '*Shared Folders*', cliquez sur '*Add*' puis sélectionnez le répertoire que vous voulez partager (ex : le dossier VMShare dans c:\). Sélectionnez les options suivantes :

- Always enabled.
- Map as a network drive in Windows Guest.

## LES DIFFERENTS MODES D'UN ROUTEUR

---



## MEMO DES COMMANDES LINUX

---

<b>Aide sur les commandes</b>	
<b>man ls</b>	appel de l'aide pour la commande ls
<b>xman &amp;</b>	appel de l'aide en mode graphique
<b>option -h ou --help</b>	demande d'aide pour une commande
<b>ls - -help</b>	demande d'aide pour la commande ls
<b>Manipulation des fichiers</b>	
<b>ls</b>	liste des fichiers du répertoire
<b>ls -l</b>	liste détaillée des fichiers du répertoire
<b>cd</b>	déplacement dans l'arborescence des fichiers
<b>cd /etc</b>	positionnement sur le répertoire etc
<b>pwd</b>	nom du répertoire courant
<b>cd ..</b>	positionnement dans le répertoire précédent
<b>mkdir prog</b>	création du répertoire prog
<b>cd prog</b>	positionnement dans le répertoire prog
<b>rmdir prog</b>	effacement du répertoire prog
<b>cp prog1.c prog2.c</b>	copie du fichier prog1.c dans prog 2.c
<b>rm prog1.c</b>	effacement du fichier prog1.c
<b>mv prog1.c prog2.c</b>	renommage ou déplacement du fichier prog1.c en prog2.c
<b>file prog.c</b>	type du fichier prog.c
<b>wc prog.c</b>	nombre de lignes, de mots, de caractères, du fichier prog.c
<b>cat prog.c</b>	liste du contenu du fichier prog.c
<b>cat a.txt &gt;&gt;b.txt</b>	copie du fichier a.txt au bout du fichier b.txt
<b>more prog.c</b>	liste du contenu du fichier prog.c, arrêt en bas d'écran
<b>less prog.c</b>	liste du contenu du fichier prog.c, amélioration de more
<b>grep "main" prog.c</b>	affiche toutes les lignes du fichier prog.c contenant main
<b>vi prog.c</b>	édition du fichier prog.c
<b>emacs prog.c</b>	édition du fichier prog.c
<b>chmod a+r fich.html</b>	permission de lecture pour tous du fichier fich.html
<b>sort fich.html</b>	tri du fichier fich.html
<b>cmp a.txt b.txt</b>	compare deux fichiers
<b>diff a.txt b.txt</b>	affiche les différences entre les deux fichiers
<b>touch fich.txt</b>	crée un fichier vide de ce nom s'il n'existe pas, sinon change la date de dernière modification du fichier.
<b>Compression et archivage</b>	
<b>tar czf prog.tar.gz prog</b>	création (c) d'un fichier archive (f) prog.tar.gz comprimé (z), à partir de tous les fichiers de l'arborescence prog
<b>tar tzvf prog.tar.gz prog</b>	liste (v) de la table (t) des fichiers de l'archive prog.tar.gz
<b>tar xzf prog.tar.gz prog</b>	extraction (x) des fichiers de l'archive prog.tar.gz
<b>gzip fich.txt</b>	compression du fichier fich.txt en fich.txt.gz
<b>gunzip fich.txt.gz</b>	décompression du fichier fich.txt.gz en fich.txt
<b>gzip -d fich.txt.gz</b>	idem
<b>Combinaison de commandes</b>	
<b>echo « bonjour » &gt; fich.txt</b>	écriture de « bonjour » dans le fichier fich.txt
<b>ls &gt; liste.txt</b>	envoi de la liste des fichiers du répertoire dans liste.txt
<b>ls &gt;&gt; liste.txt</b>	idem mais c'est copié au bout de liste.txt
<b> </b>	envoi de la sortie d'une commande dans l'entrée de la suivante
<b>ls wc -l</b>	nombre de fichiers du répertoire en cours (wc -l compte les lignes)

	affichées par ls)
<b>Gestion de la session</b>	
<b>passwd</b>	changement de mot de passe
<b>who</b>	utilisateurs connectés
<b>w</b>	utilisateurs connectés et action en cours
<b>whoami</b>	userid de la session en cours
<b>id</b>	uid et gid (numéro d'utilisateur et de groupe)
<b>h</b>	historique des commandes
<b>↑</b>	commande précédente
<b>echo « bonjour »</b>	affichage d'une chaîne de caractères
<b>echo \$PATH</b>	affichage du chemin d'accès aux commandes
<b>printenv</b>	affichage des variables d'environnement
<b>alias</b>	liste des alias
<b>tty</b>	nom du terminal
<b>xterm -fn 10x20 &amp;</b>	nouvelle fenêtre en mode graphique fonte fixe 10x20
<b>export LANG=fr_FR</b>	diagnostic en français
<b>export LANG=c</b>	diagnostic en anglais
<b>locale</b>	affiche les options locales de langue
<b>exit</b>	quitte le shell (ou la session)
<b>logout</b>	idem
<b>ctrl-d</b>	idem (ctrl = touche contrôle)
<b>Communication réseaux</b>	
<b>ping auger.c-strasbourg.fr</b>	Test de l'accessibilité de la machine auger.c-strasbourg.fr
<b>host auger.c-strasbourg.fr</b>	Demande au serveur DNS l'adresse IP de auger.c-strasbourg.fr
<b>mail -s bonjour dupond@truc.fr</b>	Envoi d'un mail à dupond@truc.fr ayant pour sujet « bonjour ». terminer le message « . » en début de ligne
<b>mail</b>	Lecture de sa boîte aux lettres par la commande mail BSD
<b>pine</b>	Gestion de boîte aux lettres par pine
<b>mutt</b>	Gestion de boîte aux lettres par mutt
<b>nestcape url</b>	Navigateur Web (url optionnel)
<b>mozilla url</b>	Navigateur Web (url optionnel)
<b>lynx url</b>	Navigateur Web non graphique
<b>wget -r url</b>	Déchargement récursif de pages Web à partir d'url
<b>slogin auger.c-strasbourg.fr</b>	Connexion sécurisée sur la machine Unix auger.c-strasbourg.fr
<b>scp prog.c auger:/tmp</b>	Copie du fichier prog.c dans /tmp sur la machine auger
<b>scp -r auger :prog</b>	Copie récursive des fichiers du répertoire prog de la machine auger dans le répertoire courant de la machine locale
<b>ftp ftp.u-strasbg.fr</b>	Déchargement de fichier par ftp, userid <i>anonymous</i> , password <i>votre mail</i> , commandes cd, get
<b>ncftp ftp.u-strasbg.fr</b>	ftp amélioré (login automatique sur serveur ftp anonymous)
<b>Réseaux</b>	
<b>sudo nano /etc/network/interfaces</b>	Accéder aux interfaces réseaux
<b>sudo /etc/init.d/networking restart</b>	Redémarrer des cartes réseaux
<b>ifconfig -a</b>	Voir l'interface réseau montée

## COMMANDES GENERIQUE SUR L'IOS

---

Touches magiques : **?** et **tabulation**.

Toute commande entrée est :

- à effet immédiat ;
- dans le fichier de config courant ;

Pour supprimer une commande, ressaisir la commande dans son intégralité en ajoutant **no** devant.

### EFFACER LE RÉGLAGE D'UN SWITCH

---

```
Switch#erase startup-config
Switch#delete vlan.dat
Switch#reload
```

### EFFACER LE REGLAGE D'UN ROUTEUR

---

#### METHODE 1

```
Router#wr er
Router#reload
```

#### METHODE 2

```
Router#erase startup-config
Router#reload
```

### NOMMER UN ROUTEUR

---

```
Router(config)#hostname Tokyo
Tokyo(config)#
```

### DEFINIR UN MOT DE PASSE SUR LA LIGNE CONSOLE

---

```
Router(config)#line con 0
Router(config-line)#password password <password>
Router(config-line)#login
Router(config-line)#logging synchronous
Router(config-line)#exec-t 0 0 <la session n'expire jamais>
Router(config-line)# CTRL+Z
Router#
```

### PASSAGE AU MODE PRIVILEGIE

---

Version 1 – ancienne version le mot de passe apparaît en clair

```
Router(config)# enable password cisco456      <mot de passe cisco456>
Router(config)# CTRL+Z
Router#sh run le mot de passe apparaît en clair
Router(config)#service password-encryption
```

Router#sh run le mot de passe apparaît chiffré mais est déchiffrable grâce à des outils sur le net.

Version 2 – version actuelle le mot de passe apparaît chiffré

```
Router(config)# enable secret cisco456      <mot de passe cisco456>
```

```
Router(config)# CTRL+Z
```

Router#sh run le mot de passe apparaît chiffré selon l'algorithme de hachage md5.

## DEFINIR DES MOTS DE PASSE POUR LE MODE PRIVILEGIE

---

```
Router(config)#enable password <password>
```

```
Router(config)#enable secret <password>
```

Pour encrypter les mots de passe :

```
Router(config)#service password-encryption
```

## TELNET

---

(vty signifie tty car on est en virtuel):

```
Router(config)#line vty 0 4 (permet 5 administrateurs de se connecter en simultané)
```

```
Router(config-line)#password <password>
```

```
Router(config-line)#exec-t 0 <la session n'expire jamais>
```

```
Router(config-line)#logging synchronous
```

```
Router(config-line)# CTRL+Z
```

```
Router#terminal monitor (pour recevoir les messages console)
```

## COMMANDES SHOW

---

### Show interfaces:

Affiche les statistiques relatives à toutes les interfaces du routeur.

Pour afficher les statistiques d'une interface spécifique, entrez la commande show interfaces, suivie par le numéro spécifique de l'interface et du port.

Exemple:

```
Router#show interfaces serial 0/1
```

### show controllers serial:

Affiche les caractéristiques de l'interface.

Cette commande doit indiquer le port ou l'emplacement et le numéro de port (slot / port number) de l'interface série.

Par exemple:

```
Router#show controllers serial 0/1
```

### show IP interface br :

Affiche l'état de la connectique

```
Router#show IP interface br
```

## CONFIGURER UNE INTERFACE

---

```
Router(config)#interface serial 0/0
```

```
Router(config)#description ce que j'ai envie de dire
```

```
Router(config-if)#ip address 172.16.41.1 255.255.255.0
```

```
Router(config-if)#no shutdown
```

`Router(config-if)#bandwidth 2000` signifie 2mb/s, la valeur est en kbps sinon par défaut c'est une T1 soit 1,5 mb/s  
`Router(config-if)#clock rate 2000 000` signifie 2mb/s, la valeur est en bps, attention c'est un cas d'école, la commande clockrate est uniquement utilisée par le DCE, la commande `sh controllers` permet de savoir si on est en DCE ou en DTE.  
Exemple:  
`Router(config)#interface serial 0/0`  
`Router(config-if)#clock rate 56000`  
`Router(config-if)#no shutdown`

## SAUVEGARDE DE LA CONFIG SUR SERVEUR TFTP

---

`Router#copy running-config tftp.`  
Étape 1 :  
Tapez l'adresse IP de l'hôte dans lequel vous désirez stocker le fichier de configuration.  
Étape 2 :  
Tapez le nom que vous désirez attribuer au fichier de configuration.  
Étape 3 :  
Confirmez votre choix en répondant yes chaque fois.

## AJOUTER UNE ROUTE STATIQUE

---

`GAD(config)#ip route 192.168.16.0 255.255.255.0 192.168.15.2`  
`BHM(config)#ip route 192.168.14.0 255.255.255.0 192.168.15.1`

## UNE ROUTE STATIQUE PAR DEFAUT

---

`BHM(config)#ip route 0.0.0.0 0.0.0.0 192.168.15.2`

## CONFIGURATION DE RIP

---

Sélectionné le protocole RIP comme protocole de routage  
`Router(config)#router rip`  
Spécifié un réseau directement connecté.  
`Router(config-router)#network 10.0.0.0`  
Spécifié un réseau directement connecté.  
`Router(config-router)#network 192.168.13.0`

## ENREGISTRER LA CONFIGURATION

---

Préconisation Cisco pour sauvegarder les réglages:  
`Router#Copy run start`  
Ou `Router#Copy running-config startup-config`  
Préconisation André Vaucamps pour sauvegarder les réglages:  
`Router#wr`

## PROTOCOLES DE ROUTAGE

---

### RIP V1 (RFC 1058)

---

Protocole de routage **par classe**, à vecteur de distance.  
 Métrique = **nombre de sauts** M>15 → route inaccessible  
 Mises à jour = **Broadcasts toutes les 30 secondes.**

Messages RIP encapsulé dans UDP, port 520

- 2 types : **Requête** ou **Réponse**.
- Jusqu'à **25** routes dans un message.

### CONFIG

---

```
router rip
network X
```

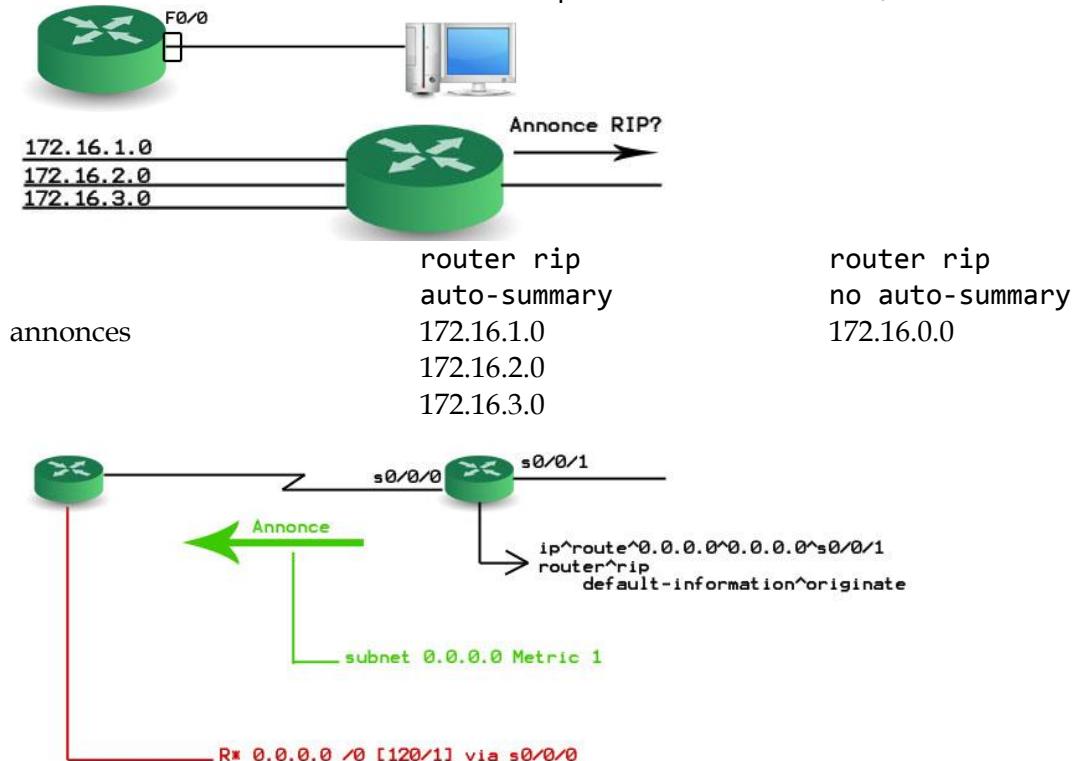
**Active RIP sur toutes les interfaces appartenant au réseau**  
**+ Annonce X sur toutes interfaces RIP actives n'appartenant pas au réseau X.**

### DÉPANNAGE

---

```
sh ip interfaces
sh ip protocols
sh ip route
undebbug all
debug ip rip
```

Le Pc n'exploite pas les mises à jour RIP  
**passive-interface F0/0**



---

## TEMPORISATIONS

---

MAJ : **30s**

Route invalide : **180s**

Hold down :

Effacement (flush): **240s**

### Prévention des boucles de routage :

- Split Horizon.
- Poison reverse.
- Hold down.

---

## DIVERS

---

Partage de charge à coût égal : jusque 6 chemins (4 par défaut).

---

### RIP V2 (RFC 2453)

---



---

### POURQUOI RIP V2 ?

---

Car il supporte l'abandon des classes, la solution consiste à annoncer l'adresse IP et le masque.

Exemple :

RIP v1 annonce : 10.0.11.0/ ?.

RIP v2 annonce : 10.0.11.0/24.

---

### LES NOUVELLES FONCTIONNALITES DE RIP V2

---

- Une adresse de prochain saut.
- Un marqueur destiné à distinguer une route transportée par RIP mais non issue de RIP (une route externe).
- Multidiffusion (une adresse de groupe, qui appartient à la classe D (224...), affectation sur le site de l'IANA (RIP : 224.0.0.9). R1 fait une annonce RIP v2, l'adresse destination = 224.0.0.9. De la trame : l'IEFT disposait de 00 :00 :5E 23 bits pour l'adresse groupe, la 1<sup>ère</sup> adresse de groupe : 01 :00 :5E:00 :00 :00 l'adresse MAC est 01 :00 :5E:00 :00 :09).
- Authentification des messages, optionnel.

---

## COMPATIBILITE

---

La RFC 2453 prévoit :

- Emission des annonces RIP :
  - RIP v1 → seuls les messages RIP v1 sont envoyés.
  - RIP v1 compatible → les messages RIP v2 sont diffusés.
  - RIP v2 natif.
  - None (passive-interface) :
    - En configuration d'interface : `ip rip send version [1] [2]`
- Un commutateur côté réceptionne des annonces :

- RIP v1 seulement.
- RIP v2 seulement.
- Les deux.
- Aucun
  - En configuration d'interface : `ip rip receive version [1] [2]`  
(vérification avec un `show ip protocols`)

## CONFIGURATION D'UN ROUTEUR :

```
A(config)#router rip
A(config-router)#version 2
A(config-router)#network 172.16.0.0
A(config-router)#^Z (CTRL+Z)
Recette : show ip route summary (comptabilise les subnets).
```

## CONFIGURATION AVANCEE:

Par défaut l'agrégation automatique aux frontières de réseaux majeurs (/8, /16, /24).

Problème : un paquet destiné à 172.16.x.x et reçu par A a une chance sur 3 d'être remis à son destinataire.

Solution : désactiver l'agrégation automatique : ex : C(config-router)#no auto-summary.  
Ce faisant ont constraint C à annoncer à l'ensemble des subnets qu'il connaît de 172.16.x.x.  
Sur les 3 routeurs frontières on entre la commande no auto-summary.

La commande `ip classless` est active (c'est le cas depuis l'IOS 11.3) :

- L'algorithme de routage utilise la plus longue correspondance de préfixe (Longest Match Based Forwarding Algorithm).

Grâce à cette algorithme, il est inutile de désactiver l'agrégation automatique sur le routeur A.

## ACTIVATION DE L'AUTHENTIFICATION :

(Vaut pour RIP et EIGRP)

**Objectif** : authentification par mot de passe en clair « inabottle »

Etape 1 :

Créer un ensemble de clés

- Router(config)#key chain **turing** (`name-of-key-chain`)

Etape 2 :

- Router(config-keychain)#key-string **inabottle** (`le mot de passe`)

Etape 3 :

Appliquer l'authentification à une interface

- Router(config-keychain)#int s0/0
- Router(config-if)# ip rip authentication key-chain **turing**
- Router(config-if)#ip rip authentication mode **text|md5**

Recette :

```
show key chain
  Key-chain turing
    Key 1 inabottle
```

Annonces entrantes **Accept lifetime (always valid)-(always valid) [valid now]**

Annonces sortantes **Send lifetime (always valid)-(always valid) [valid now]**

**Debug ip rip**

RIP : received packet with text authentication inabottle.

## OSPF

---

Pour une zone, la LSD porte la topologie du réseau.

Mise à jour de la LSD par échange de LSA

show ip ospf database.

What is the maximum hop count for link state protocols?

There is no hop count limit.

What is a stub network?

A network that has only one entry and exit.

## OSPF 2

---

Election Dr, BDR

```
show ip ospf interface → state
show ip ospf neighbor
```

Router(config)#router ospf n°\_process (1 à 65535)

Router(config-router)#network @IP@masque\_gen area x

## EIGRP

---

### CARACTERISTIQUES:

---

- Classless : VLSM peut être utilisé sans retenue.
- Supporte l'authentification des messages.
- Multi-protocole : mais sans intérêt aujourd'hui (IP, IPX, Appletalk).
- Les routeurs EIGRP découvrent leurs voisins à l'aide de messages Hello émis de façon périodique.
- La métrique est composite c'est-à-dire qu'elle fait intervenir la bande passante, le délai, la fiabilité, la charge. Les deux dernières étant optionnelles.
- MAJ d'EIGRP sont : périodiques, partielles, ciblées et fiables.

### METRIQUE D'EIGRP

---

Metrique<sub>EIGRP</sub> = Metrique<sub>IGRP</sub> \* 256.

$$\frac{\text{Métrique}_{EIGRP}}{256} = \left\{ k_1 * \frac{10^7}{BW_{min}(kbps)} + \frac{k_2 * \frac{10^7}{BW_{min}(kbps)}}{256 - charge} + k_3 * \sum_{chemin} dly(10\mu s) \right\} * \left\{ \begin{array}{l} \frac{k_5 (\neq 0)}{Fiabilite + k_4} \\ | 1 \text{ quand } k_5 = 0 \end{array} \right\}$$

Avec les coefficients par défaut :

$$\frac{\text{Métrique}_{EIGRP}}{256} = \frac{10^7}{BW_{min}} + \sum_{chemin} dly(10\mu s)$$

---

### QUELQUES COMMANDES:

---

```
show ip eigrp topology
show ip eigrp neighbor
ip load sharing per-packet
```

#### LE CRITERE DE FAISABILITE → DISTANCE ANNONCEE < DISTANCE FAISABLE EN COURS

Dans EIGRP, un voisin peut avoir trois états :

1. Voisin simple: `show ip eigrp neighbor`.
2. Successeur potentiel: `show ip eigrp topology [all-links]`.  
*Pour voir tous les routeurs qui proposent une alternative y compris ce qui ne respectent pas RD<FD.*
3. Successeur : `show ip eigrp topology + show ip route`.

---

### PARTAGE DE CHARGE:

---

Mode CEF = Cisco Express Forwarding (à partir de l'IOS 11.1).

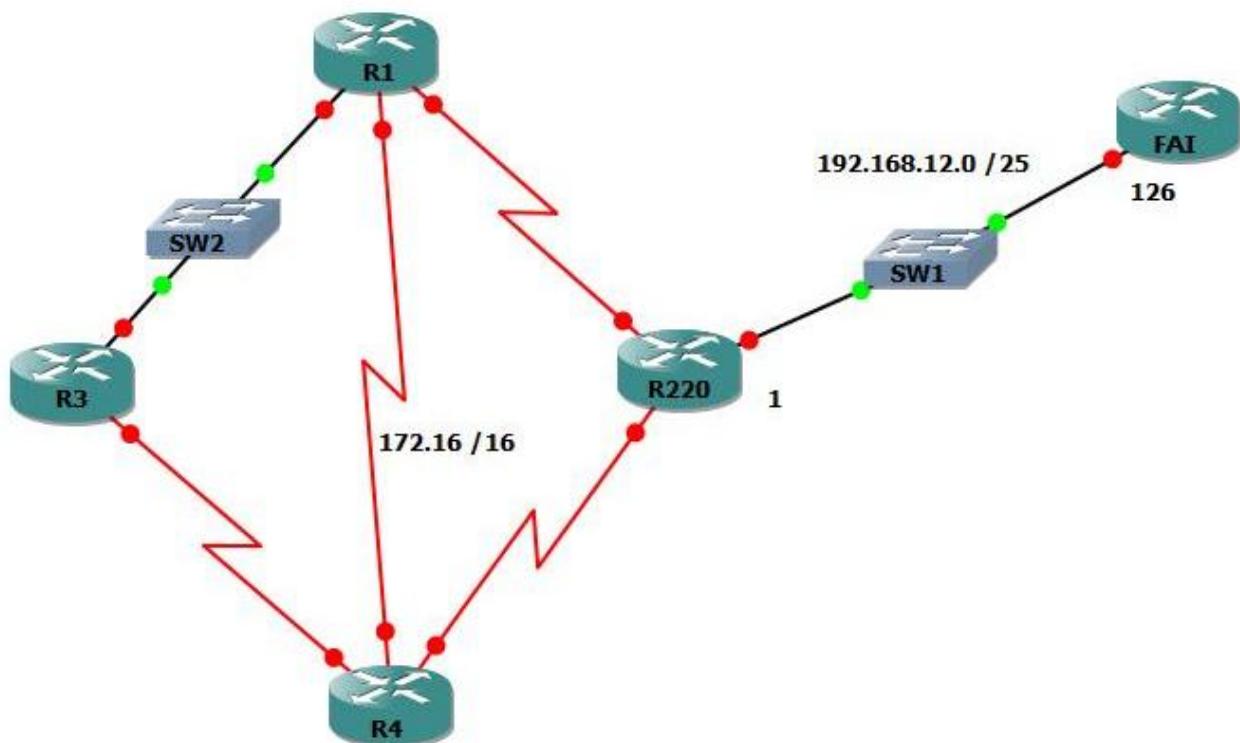
Activé via la commande : `ip cef` (en mode de configuration globale). CEF crée une table de commutation, dites table FIB (Forwarding Information Base).

```
show ip cef 10.1.102. ? internal
```

---

### PROPAGATION DE LA ROUTE PAR DEFAUT :

---



**Etape 1 :** sur chaque routeur (sauf FAI)

```
no router rip
router eigrp 64501
network 172.16.0.0
```

**Etape 2:** sur R220, ôter la route par défaut vers 192.168.12.0  
no ip default-network 192.168.12.0

**Etape 3:** sur R220, ajouter une route statique vers FAI  
ip route 0.0.0.0 0.0.0.0 192.168.12.126

**OBJECTIF : LES AUTRES ROUTEURS DOIVENT APPRENDRE CETTE ROUTE PAR EIGRP.**

**Etape 4:** sur R220, activer la redistribution de route statique par EIGRP.  
router eigrp 64501  
redistribute static

**Recette:** sur R220  
show ip route  
Gateway of last resort is 172.16.34.12 network 0.0.0.0  
D\* EX 0.0.0.0 [170/40514560] via 172.16.32.42

## RESUME DES COMMANDES DES PROTOCOLES DE ROUTAGE

---

RIP v1	RIP v2	EIGRP	OSPF
Déclaration d'un protocole sur un routeur ( <i>commande à rentrer en mode de configuration globale</i> )	router rip network 192.168.1.0	router eigrp ? <1 – 65535> Autonomous system number router eigrp 1 network 192.168.1.0	router ospf 1 network 192.168.1.0 0.0.0.255 area 0
Commandes show	show ip route show ip protocols	show ip protocols show ip route debug ip rip undebug all	Configuration de la bande passante interface F0/0 bandwidth 1024 (en kbps) ip ospf cost 1562 Modifier le coût de la liaison
Commandes spécifiques au protocole	Désactiver les mises à jour sur une interface passive-interface F0/0	show ip eigrp neighbors show ip eigrp topology show ip protocols show ip route show ip route	Désactivation du résumé automatique no auto-summary

## DEBITS LIENS WAN

---

### Europe

E0 : 64 Kbps.  
E1 : 32 lignes E0 → 2Mbps  
E2 : 128 lignes E0 → 8Mbps  
E3 : 16 lignes E1 → 34 Mbps  
E4 : 64 lignes E1 → 140 Mbps

### US

T1 : 1,544 Mbps  
T2 : 4T1 → 6,312 Mbps ≈ 6Mbps  
T3 : 28T1 → 44,736 Mbps ≈ 45 Mbps  
T4 : 168T1 → 275 Mbps

### Satellite

>72000km → latence 700ms.

Upload de 128K à 1024K.

Download de 512k à 2Mbps.

Attention à la confusion possible avec le schéma de référence du RNIS :

T0 = accès de base (2 canaux B + 1 canal D)

T2 = accès primaire (jusque 30 canaux B)

Canal B = 64 kbps

## COMMANDES SHOW

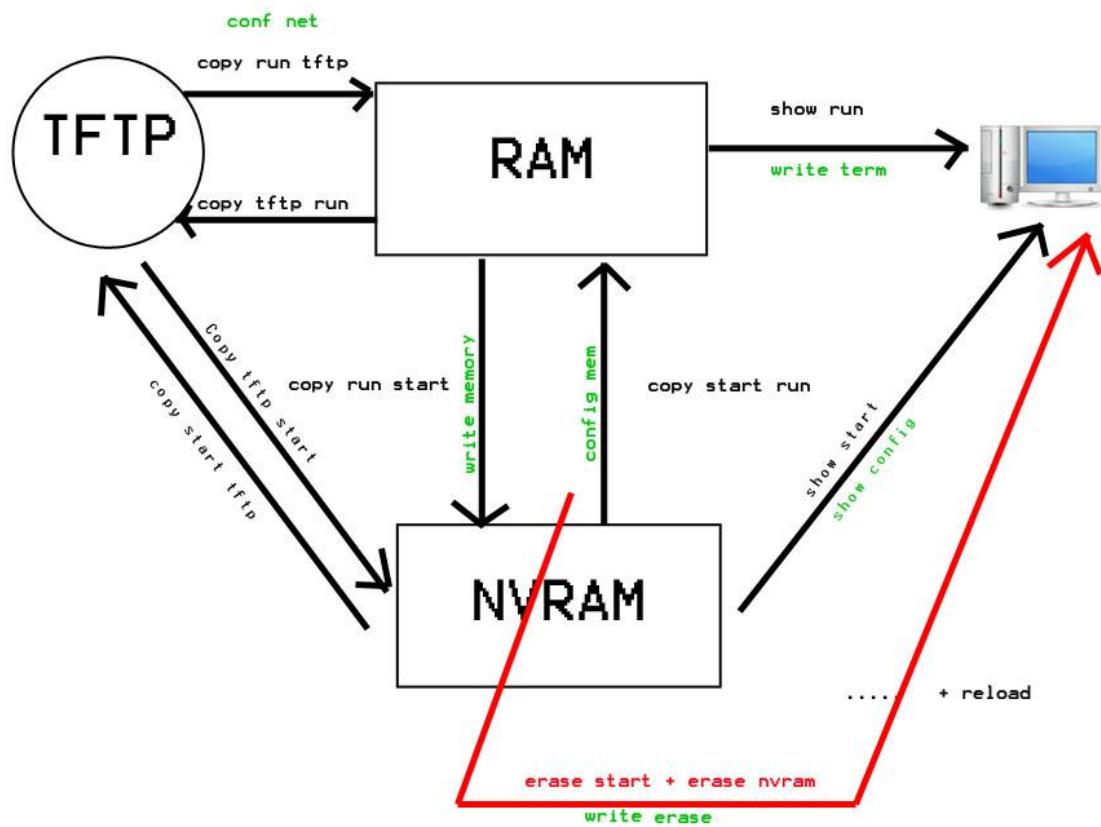
---

<b>Commandes</b>	<b>Fréquence d'utilisation</b>	<b>Descriptif de la commande</b>
<b>show ip route</b>	5	Contenu de la table de routage
<b>show running-config</b>  begin maker  include  exclude	5	
<b>show ip int [type numéro] br</b>	5	Informations IP
<b>show run</b>	5	Affiche la configuration du routeur.
<b>show interfaces status</b>	5	
<b>show interfaces F0/1 status</b>	5	
<b>show startup-config</b>	4	
<b>show protocols</b>	3	Nom et l'état de tout protocoles de couche 3 sur routeur
<b>show controllers [type numéro]</b>	3	Informations couche 1 – une interface serial est-elle dte ou dce ?
<b>show ip protocols</b>	3	Informations sur la configuration des protocoles de routage
<b>show processus cpu</b>	2	Consommation des ressources machines
<b>show version</b>	2	La config matérielle, la version d'IOS, le nom et la source de l'image IOS, la valeur du registre de configuration
<b>show flash</b>	2	Contenu de la partition Flash
<b>show arp</b>	2	
<b>show hosts</b>	2	
<b>show interface[type numéro]</b>	2	Informations couche 2&3 statistiques de trafic
<b>show sessions</b>	2	Liste des sessions Telnet en cours.
<b>show users</b>	2	Liste des utilisateurs connectés
<b>show history</b>	2	
<b>show clock</b>	1	
<b>show ip interface</b>		Permet de vérifier si liste d'accès est mise en œuvre
<b>show access-list</b>		Contenu de toutes les listes d'accès
<b>show ip access-list</b>		Contenu de toutes les listes + comptage
<b>show access-list {numéro nom}</b>		
<b>show ip nat translations</b>		Look the nat translation on the gateway router
<b>show ip nat statistics</b>		

NB : la fréquence d'utilisation est notée de 1 à 5, 1 étant une commande peu utilisée et 5 une commande couramment utilisée.

## GESTION DES FICHIERS DE CONFIGURATION

Run ≡ running-config  
 Start ≡ startup-config



`copy {tftp|run|start} {tftp|run|start}`

\*ancien jeu de commandes.

Si NVRAM vide au démarrage → le routeur propose le mode setup.

## ENCAPSULATION

---

Encapsulation	Dénomination CISCO
hdlc on serial	hdlc
802.2	sap
802.3	novell-ether
ethernet V2	arpa * (champ type)
ethernet SNAP	snap
ipx fddi-raw	novell-fddi

## DEBUG

---

```
undebbug all
debug ip arp
debug ip packet
debug ip rip:annonces émises / recues RIP
```

## DISTANCE ADMINISTRATIVE

---

**Notion de métrique :** C'est le coût d'une route. Permet le choix lorsque plusieurs alternatives existent. A chaque protocole de routage correspond une méthode de calcul du coût.

Facteurs pouvant intervenir sur le calcul du coût :

- Trafic
- Bande passante
- Fiabilité

A chaque route on associe :

- Sa métrique (son coût)
- Un indice de confiance (distance administrative)

Le routeur prend en compte d'abord la distance administrative la plus basse et prendra à distance administrative égale le coût métrique le plus bas.

La distance administrative codée sur 8 bits, de 0 à 255

	DA
<b>Route directement connectée</b>	0
<b>Route statique</b>	1
<b>Route EIGRP</b>	90
<b>Route IGRP</b>	100
<b>Route OSPF</b>	110
<b>Route RIP</b>	120
<b>Route EIGRP EX</b>	170
<b>DA = 255</b>	Aucune confiance

## ACL

---

ACL : Access Control List.

Permet de contrôler le trafic, par exemple :

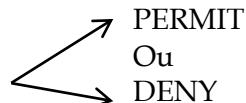
- Autorisé ou non l'établissement d'une session Telnet sur un routeur.
- Autorisé ou non l'établissement d'une session http sur un routeur.
- Réduire la portée d'une commande, `debug ip packet`.
- Identifier les paquets qui justifient l'ouverture d'une session DDR (Dial on Demand Routing = liaison commutée).
- Authentifier les utilisateurs à l'origine d'un trafic.
- Identifier les paquets devant faire l'objet d'un chiffrement.

## FONCTIONNEMENT

---

Liste : suite d'items lus en séquence.

1 item SI condition\_à\_vérifier ALORS action



## LISTE D'ACCES STANDARD

---

```
Router(config)#access-list ACL_# {permit|deny} {@IPsource [masque
générique]|any} [log 1-99] [masque] [utilisateur]
          Ou
          1300-1399
```

Un ensemble d'adresse

<b>1-99</b>	Standard
<b>100-199</b>	IP étendue
<b>600-699</b>	Apple Talk
<b>800-899</b>	IPX
<b>900-999</b>	IPX avancé
<b>1000-1099</b>	SAD IPX

## MASQUE GENERIQUE

---

Un bit "0" signifie vérifier la valeur du bit correspondant dans l'adresse IP.  
Un bit « 1 » signifie ignorer la valeur du bit correspondant dans l'adresse IP.

ACL standard : au plus près de la destination.  
ACL étendue : au plus près de la source.

What does -1 mean in an extended IPX access-list?  
Any host or any network.

Any  $\equiv 0.0.0.0^255.255.255.255$   
host $\wedge 172.30.16.29 \equiv 172.30.16.29^0.0.0.0$

## COMMANDES

---

### REGLE DES 3P :

Une liste par :

- Interface.
- Protocole.
- Sens de flux.

### CREATION D'UNE LISTE SUR R100 :

```
R100(config)#access-list 1 permit 10.0.8.0 0.0.0.127
```

### APPLIQUER LA LISTE SUR L'INTERFACE E1/0 ET EN SORTIE:

```
R100(config)#interface e1/0
R100(config-if)#ip access group 1 out
```

### APPLICATION D'UNE LISTE A UNE LIGNE :

```
R100(config)#line vty 0 4
R100(config-if)#access-class ACL_# {in|out}
```

### COMMENT TRAQUER LES PAQUETS REFUSES ?

```
R100(config)#interface e1/0
R100(config-if)#ip accounting access-violations
...
R100#show ip accounting access-violations
Remise à zero: R100#clear ip accounting
```



A délayer quand on en a pu besoin car risque d'oblitérer certains modes de commutations.

```
show ip access-list
clear ip access-list counter
```

## LISTE D'ACCES ETENDUE

---

### OBJECTIF

Installer une liste de contrôle d'accès étendue qui permette le trafic SMTP du MTA interne au MTA externe à l'exclusion de tous les autres trafics.

### SYNTAXE D'UNE LISTE D'ACCES ETENDUE TCP

```
Router(config)#access-list ACL_# [dynamic dynamic_name [timeout minutes]]
{permit|deny} tcp {@IP_source [masque_générique]|any} [operator [port]]
```

```
{@IP_dest [masque_générique] | any} [operator [port]]
[established][precedence precedence] [tos tos] [dsep dsep] [time-range
plage-de-temps] [fragment] [log [cookie]|log-input [cookie]]
```

## OPERATOR

lt : less than ; gt : greater than; eq: equal; neq: not equal; range

- 1 – flux entrant sur F0/0 de R120.
- 2 – liste étendue.
- 3 – adresse source non retenue pour accepter des courriers en provenance de tout domaine.
- 4 – port source = 25.
- 5 – adresse de destination : 10.0.8.3.
- 6 – port de destination non retenu.
- 7 – les seuls paquets non autorisés sont ceux qui transitent sur un circuit virtuel TCP ouvert (ACK positionné).

```
Router(config)#access-list 125 permit tcp any eq smtp (ou 25) host 10.0.8.3
established
Router(config)#access-list 125 deny ip any any ← Facultatif pour comptage
Router(config)#int F0/0
Router(config-if)#ip access-group 125 in
Router(config-if)#CTRL+Z
```

## POUR PERMETTRE LA RECEPTION DE MAIL PROVENANT DU RESTE DU MONDE

```
R120(config)#access-list 125 permit tcp any eq smtp (ou 25) host 10.0.8.3
R120(config)#access-list 125 permit tcp any host 10.0.8.3 eq smtp
R120(config)#inf F0/0
R120(config-if)#ip access-group 125 in
```

## ADRESSAGE IP

---

By enabling IP SUBNET ZERO, the number of networks is  $2^N$ , not  $2^N-2$ .

### CLASSES

---

<b>A</b>	0 à 126
<b>B</b>	128 à 191
<b>C</b>	192 à 223
<b>D</b>	224 à ...

### ADRESSES PRIVEES (RFC 1918)

---

<b>A</b>	10.0.0.0 – 255.255.255.255
<b>B</b>	172.16.0.0 – 172.31.255.255
<b>C</b>	192.168.0.0 – 192.168.255.255

Dans IP, champ protocole

<b>6</b>	TCP
<b>17</b>	UDP
<b>89</b>	OSPF

### ATTRIBUTION D'ADRESSE IP

---

Statique

Dynamique :

- RARP
- BOOTP/DHCP (sur UDP)

### NUMÉROS DE PORT (RFC 1700)

---

<b>&lt;255</b>	Applications publiques.
<b>De 255 à 1023</b>	Attribuées aux entreprises pour des applications commercialisables.
<b>&gt;1023</b>	Attribution dynamique.

## LES PORTS TCP / UDP

---

TCP	UDP
<b>20</b>	Données FTP
<b>21</b>	Contrôle FTP
<b>22</b>	SSH
<b>23</b>	Telnet
<b>25</b>	SMTP
<b>53</b>	Transfert de zone DNS
<b>80</b>	http
<b>110</b>	POP3
<b>139</b>	Session Netbios
<b>179</b>	BGP
<b>53</b>	Requête DNS
<b>67</b>	Serveur BOOTP
<b>68</b>	Client BOOTP
<b>69</b>	TFTP
<b>123</b>	NTP (Network Time Prot)
<b>137</b>	Service de noms Netbios
<b>138</b>	Datagrammes Netbios
<b>161</b>	SNMP
<b>162</b>	Trap SNMP
<b>520</b>	RIP

+ netstat -an ou netstat -ano

## IDENTIFICATION

---

```
hostname
prompt
banner motd#
    accounting dep....#
Description d'interface
    router(config-if)#description ...
```

## AIDE

---

? ≡ Touche entrée bis

Commande ? → liste des commandes commençant par commande.

Commande ? → Tous les 1ers paramètres de la commande.

## TAMPON DES COMMANDES

---

10 commandes par défaut, modifiable

<b>terminal history size x</b>	X appartenant à [0,256]
<b>show history</b>	Enable or stop the advanced editing feature.
<b>terminal editing</b>	
<b>terminal no editing</b>	
↑ ou CTRL-P	Previous
↓ ou CTRL-N	Next
← ou CTRL-B	Backward
→ ou CTRL-F	Forward
CTRL-R	réaffiche l'invite système + ligne de commande courante ou logging^synchronous.
CTRL-A	1 <sup>er</sup> caractère commande affiché
CTRL-E	dernier caractère commande affiché
ESC+B	1 mot en avant / en arrière
ESC+F	

## CORDON DROIT OU CROISE

---

Equipement	Chez CISCO	CROISE ou pas ?
Hub	Concentrateur	Croisé <b>nX</b>
Switch	Commutateur	Croisé <b>nX</b>
Routeur	Router	Ne croise pas
Carte réseau	Adaptateur réseau	Ne croise pas
Ou		
NIC		

Si croisé **vers** ne croise pas → utiliser un cordon droit

Dans tous les autres cas → **utiliser un cordon croisé**

Exception :

- Norme qui vient du Giga qui assure un croisement automatique.
- 

Utiliser un cordon droit.
- Certains équipements disposent d'un port MDI/MDI-X décroisable.

## GESTION DES IMAGES IOS

---

<b>Non modifiable par l'admin</b>	1 POST Power On Self Test Objet : découvrir et vérifier le matériel.
<b>Modifiable</b> <b>Par</b> <b>admin</b>	2 Charge et exécute le code d'amorçage à partir de la ROM. 3 Charge l'IOS (localise l'IOS puis le charge). 4 Localise config et charge en RAM.

copy tftp flash  
show flash // si plusieurs images IOS présentes en Flash, le 1<sup>er</sup> listé est celui que le routeur charge au démarrage.  
show version // nom de fichier + version IOS qui a été chargé lors du dernier démarrage.

### LE ROUTEUR PEUT CHARGER 3 OS

---

<b>IOS complet</b>	<b>Mémoire flash le plus souvent. Parfois serveur TFTP</b>
<b>IOS limité</b>	<b>Version IOS complète utilisée en « prod »</b> ROM (RX BOOT)
	<b>Version avec connectivité de base utilisée lorsqu'aucune version IOS valide n'est pas dispo en mémoire Flash.</b>
<b>ROM Monitor</b>	<b>ROM (ROM MON)</b> <b>Débogage de bas niveau (CATC) + récupération des mots de passe</b>

### DEUX Outils POUR INDIQUER L'IMAGE A CHARGER

---

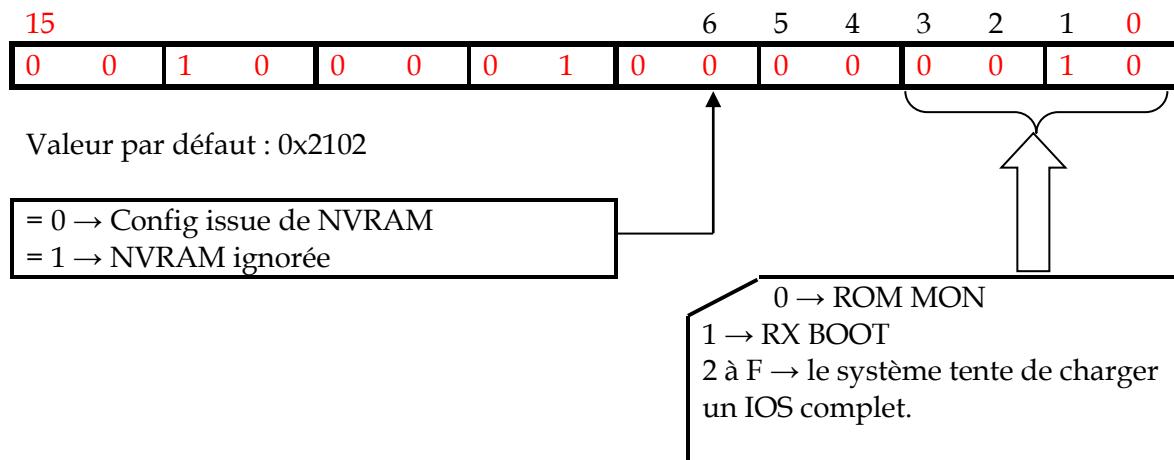
Le registre de configuration sur 16 bits

2500 en ROMMON 0/r {0x2142 | .... | ....}

2600 en ROMMON confreg

Sous l'IOS : #config-register

La commande de configuration : boot system



Champ d'amorçage	Cdes boot^system	Effet
0x0	Ignorées	ROM MON (CTRL-Pause /60s)
0x1	Ignorées	RX BOOT
0x2 à 0xF	Aucune	Le 1 <sup>er</sup> fichier IOS est chargé Si échec → TFTP Si échec → RXBOOT
	boot system rom	RX BOOT
	boot system flash	Le 1 <sup>er</sup> fichier IOS en flash est chargé
	boot system flash nom_fichier	L'IOS "nom_fichier" est chargé
	boot system tftp nom_fichier@IP	Idem
	Plusieurs cdes boot system	Tente chaque cde jusqu'à réussir

Show version pour connaître la valeur du registre.

## MANIPULATIONS SUR L'IOS

### Etape 1: Sauvegarde IOS

- R12#copy flash:c2081-ipphase-mz.124-16a.bin tftp://10.0.12.100/IOS/ [on peut appuyer sur la touche TAB afin de compléter le nom du fichier]  
!!!! N.B : « ! » = 10 paquets de 512 ko, selon CISCO.

### Etape 2 : l'idée c'est de tester l'image

- R12(config)#no boot system ← pour être sûr qu'il n'y a plus de commandes boot system dans le fichier de config.
- R12(config)#boot system tftp://10.0.12.100/IOS/c2801-ipphasek9-mz.124-25c.bin
- R12(config)#CTRL-Z
- R12#wr
- R12#reload
- R12#sh^version

**Etape 3: l'IOS est valide donc on le copie en flash**

- R12#copy tftp://10.0.12.100/IOS/c2801-ipphasek9-mz.124-25c.bin Flash
- R12#verify flash:c2801-ipphasek9-mz.124-25c.bin
- Embedded hash verification successful

**Etape 4:**

- R12(config)# no boot system
- R12(config)#boot system flash:c2801-ipphasek9-mz.124-25c.bin
- R12#reload
- R12#sh version

---

**ET SI PLUS D'IOS ? → ROMMON**

---

2 solutions

1. Chargement par le port console

- xmodem = 3 heures.
- ymodem = <1 heure.

2. TFTPDNLD → F0/0 ou F0/1

➤ Via xmodem

R12#reload

Pendant le chargement CTRL-Pause

ROMMON 1>?

xmodem → x/ymodem image download

ROMMON 2> confreg 3922

ROMMON 3> reset

Régler le terminal à 115200

ROMMON 1> xmodem -c c2801-ipphase...

-c fait passer le CRC sur 16 bits au lieu de 8 bits par défaut.

Le routeur se place en attente.

Dans HyperTerminal : provoquer l'envoi de l'image via xmodem

(xmodem très long = avorter)

➤ ROMMON 2>xmodem -c -y c2801...

➤ TFTPDNLD

ROMMON 1>tftpdnld -h

ROMMON 2>IP\_ADDRESS=10.0.12.1

ROMMON 3>IP\_SUBNET\_MASK=255.255.255.0

ROMMON 4>DEFAULT\_GATEWAY=10.0.12.254

ROMMON 5>TFTP\_SERVER=10.0.12.100

ROMMON 6>TFTP\_FILE=IOS/c2801-ipphasek9-mz.124-25c.bin

ROMMON 7>set

ROMMON 8>tftpdnld [même effet que x/ymodem c'est à dire effacement de la flash]

## RECUPERATION D'UN PASSWORD

---

1. Eteindre puis allumer le routeur.
2. **CTRL+PAUSE** pendant les 60ères secondes.
3. Positionner le bit **6** du registre de configuration à 1.  
2500 → commande ROMMON **0/r 0x2162**  
2600 → commande ROMMON **confreg** et  
Répondre Yes à « ignore system config info »  
Laisser les autres réponses par défaut.
4. Redémarrer  
2500 → **initialize**  
2600 → **reload**
5. Répondre **no** pour éviter le mode setup.
6. **enable**  
**copy run start**  
**show run**
7. changer (ou prendre connaissance) le password.  
Exemple : **enable secret toto**
8. Rétablir conf register **#config-register 0x2102**.
9. Sauvegarder **copy run start**
10. Redémarrer.

## PROCEDURE DE GHOST DEPUIS UN DISQUE DUR BOOTABLE

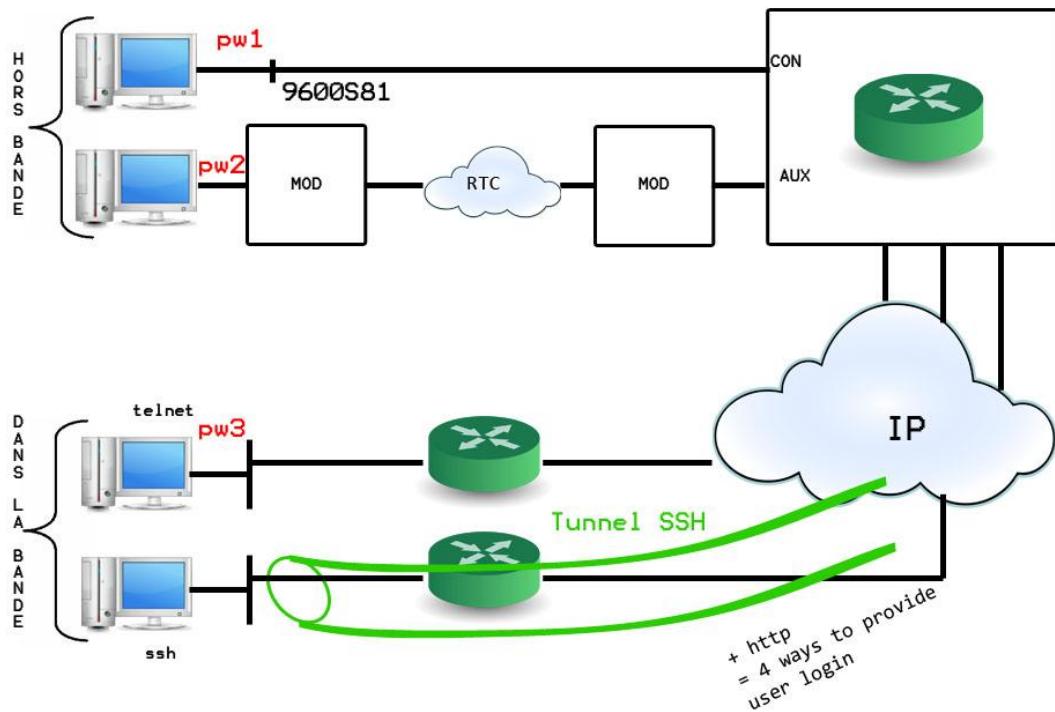
---

1. Pendant le démarrage, F8 pour choisir le support de boot.
2. WinPE démarre puis lance Ghost32.
3. Menu Local | Disk | From Image.
4. Chercher l'image convenable.
5. Sélectionner le disque cible, confirmer.  
**Une fois le déploiement achevé.**
6. Quitter Ghost32.
7. Revenir à la racine de X\.
8. Lancer Ghostwalker par appui sur A pour modifier SID.
9. Une fois le SID modifié, rebooter.
10. Sous Windows, bouton droit sur Poste De Travail | Propriétés pour modifier le nom de machine ainsi que le WG.

## ACCES A L'INTERFACE CLI

---

5 PW à connaître pour le CCNA



## PROTECTION DE L'ACCES

---

Aucun mot de passe par défaut MAIS seul accès possible au sortir du carton → via le port console.

```
line con 0
password pw1
login
```

```
line aux 0
password pw2
login
```

```
line vty 0 4
password pw3
login
```

## PROTECTION DU PASSAGE AU MODE PRIVILEGIE

---

En configuration globale

```
enable password pw4
```

ou

```
enable secret pw5
```

Pw5 apparaîtra crypté (MD5) dans un fichier de conf.

## LISIBILITE DES MOTS DE PASSE

---

En configuration globale

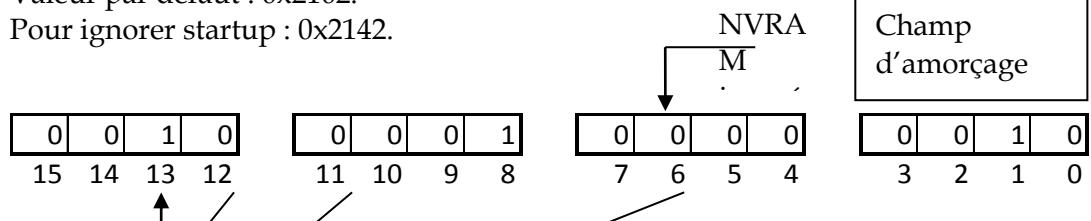
```
service-password encryption
```

Crypte en mode 7 tout password présents, protège des « regards par-dessus l'épaule de l'administrateur ».

## REGISTRE DE CONFIGURATION

Valeur par défaut : 0x2102.

Pour ignorer startup : 0x2142.



	Champ d'amorçage	Cdes des bootstem	Effet
0 0 0	9 6 0 0	0x0	ignorées ROMMON
0 0 1	1 9 2 0	0x1	ignorées Rx BOOT
0 1 0	4 8 0 0		
0 1 1	3 8 4 0		Le 1er IOS en flash
1 0 0	1 2 0 0	0x2	sinon TFTP sinon Rx
1 0 1	5 7 6 0		Boot
1 1 0	2 4 0 0		
1 1 1	1 1 5 2 0 0	0x2	tente chaque
			une à plusieurs commandes jusqu'au succès

Pour modifier la valeur

ROMMON1> confreg^2102

En ILC → Router (config)#config-register 0x2102

## AIDE-MÉMOIRE SUR POWERSHELL

Prise en charge native pour différents systèmes de types		\$a[5]	6 <sup>ème</sup> élément d'un tableau	Opérateurs d'extension de commande	
Windows PowerShell adapte les objets WMI, XML, ASDI, ADO et COM afin de proposer une syntaxe commune pour accéder à leurs propriétés et méthodes.  <b>Exemple</b> \$g = Get-WmiObject Win32_Process \$g[0].Name # au lieu de \$g[0].Properties["Name"]	\$a[2][3]	Quatrième élément ou troisième	\$()	Retourne la valeur Null.	
	\$a[2..20]	Retourner les éléments 3 à 21	\$(1,2,3)	Retourne un tableau contenant 1,2,3.	
	Opérateurs d'affectation		\$(Get-Alias a*)	Retourne l'évaluation de l'expression.	
=, +=, -=, *=, /=, %=			@(Get-Alias;Get-Process)	Exécute les deux commandes et retourne les résultats sous forme de tableau.	
Opérateurs binaires arithmétiques		Tableaux associatifs (tables de hachage)			Commentaires
+	Addition, concaténation	\$hash = @{} \$hash += "foo=1;bar=2"	Créer une table de hachage vide	# Ceci est un commentaire parce que # est le premier caractère d'un jeton \$a = "#Ceci n'est pas un commentaire..." \$a = "something" # ...mais cela en est un. Write-Host Hello#world	
-	soustraction	\$hash -= "bar"	Créer et initialiser une table de hachage	\$a = \$hash["bar"]	
*	Multiplication, répétition de chaîne	\$hash.key1 = 1	Affecter 1 à la clé « key1 »	Opérateurs de comparaison	
/	Division	\$hash.key1 / 2	Retourne la valeur de key1	-eq	égal
%	Module	\$hash["key1"] % 2	Retourne la valeur de key1	-ne	Different de
Opérations sur les tableaux		Valeurs et opérateurs booléens			-gt ; -ge
Ce tableau contient-il un 3		True	False	Supérieur à, supérieur ou égal à	
1,2,3,5,3,2 -contains 3		\$True	\$False	-lt ; -le	
Retourner tous les éléments égaux à 3 : 1,2,3,5,3,2 -eq 3		Toute chaîne de longueur > 0 sauf le mot « false »	Chaîne vide ou la chaîne « false »	« i » ou « c » peut être ajouté avant l'opérateur pour obtenir des opérations qui ne respectent pas la casse ou qui la respectent (par exemple, -ceq)	
Tout nombre !=0		Tout nombre =0	Tout nombre !=0	Inférieur à, inférieur ou égal à	
Retourner tous les éléments inférieurs à 3 : 1,2,3,5,3,2 -lt 3		Tableau de longueur > 1	Tableau de longueur 0	Continue (Script)	
Tableau de longueur 1 dont l'élément est TRUE		Tableau de longueur 1 dont l'élément est FALSE	Tableau de longueur 1 dont l'élément est FALSE	L'instruction <b>continue</b> continue l'itération suivante d'une boucle sans en sortir. Exemple :	
Tester si 2 figure dans la collection : if (1, 3, 5 -contains 2) ... Autres opérateurs : -gt, -le, -ge, -ne		Référence à un objet	Null	while (1) {     \$a = something if (\$a -eq 1) (continue) # Cette ligne n'est atteinte que si \$a == 1 } # Cette ligne n'est jamais atteinte.	
Tableaux		Les commandes <b>break</b> permettent de sortir d'une boucle. Elles peuvent accepter un LIBELLÉ facultatif auquel s'arrêter.			Point et espace avant
“a”, “b”, “c”	Tableau de chaînes				
1,2,3	Tableau d'entiers				
@()	Tableau vide	Exemple : while (1) {     \$a = something if (\$a -eq 1) break;			L'ajout d'un point et d'un espace avant un nom de fonction, un bloc de script ou un script autorise leur exécution dans la portée actuelle plutôt que dans une portée locale (local). Exemple :
@(2)	Tableau à 1 élément				
1,(2,3),4	Tableau dans un tableau				
,”hi”	Tableau à 1 élément				

Et n'oubliez pas : dans 99% des cas, le problème se situe entre le clavier et le dossier de la chaise !

<b>. MyFunction</b>		function test ([string]\$label="default label",[int]\$start=0) { BEGIN {\$x=\$start} PROCESS {"\$label: \$_";\$x++} END{"\$x total"} }	\$_	Objet de pipeline actif
Si MyFunction définit une variable, celle-ci est définie dans la portée actuelle, et non dans la portée locale de la fonction.  \$a = [Get-Process   Select -First 2] . \$a #Évalue le bloc de script dans la portée actuelle		\$Args	Arguments passés à un script ou à une fonction	
<b>Séquences d'échappement</b>		<b>Filter (script)</b>	\$Error	Tableau d'erreurs de commandes précédentes
Le caractère d'échappement Windows PowerShell est l'accent grave (`). Pour rendre un caractère littéral, faites-le précéder de `. Pour spécifier un `, utilisez `.		Un filtre (filter) est un moyen raccourci d'écrire une fonction avec un bloc de script PROCESS. filter MyFilter { \$_.name }	\$Foreach	Référence à l'énumérateur d'une boucle foreach
<b>Séquences d'échappement spéciales</b>		<b>If/elseif/else (script)</b>	\$Home	Répertoire de base de l'utilisateur ; généralement défini sur %HOMEPATH%\%HOMEPATH%
`0	(valeur Null)	if (condition) {...} elseif (condition) {...} else {...}	\$Host	Référence à l'application qui héberge le langage POWERSHELL
`a	(alerte)	Sur la ligne de commande, l'accolade fermante doit figurer sur la même ligne que elseif et else. Cette restriction ne s'applique pas aux scripts.	\$Input	Énumérateur des objets dirigés vers un script
`b	(retour arrière)		\$LastExitCode	Code de sortie du dernier programme ou script
`f	(saut de page)			
`n	(nouvelle ligne)	<b>Opérateur d'appel</b>		
`r	(retour chariot)	L'opérateur & peut être utilisé pour appeler un bloc de script ou le nom d'une commande ou fonction.		
`t	(tabulation)	<b>Exemple :</b> \$a = "Get-Process" &\$a		
`v	(tabulation verticale)	\$a = { Get-Process   Select -First 2 } &\$a		
<b>Ordre d'exécution</b>		<b>Opérateurs logiques</b>	\$Matches	Table de hachage des correspondances trouvées avec l'opérateur de correspondance
Windows PowerShell essaie de résoudre les commandes dans l'ordre suivant : alias, fonctions, applets de commande, scripts, fichiers exécutables et fichiers normaux.		!, -not, -and, -or	\$PSHome	Emplacement d'installation de Windows PowerShell
<b>For (script)</b>		<b>Appels de méthodes</b>	\$profile	Profil standard (peut ne pas être présent)
[:label] for ([initialiseur]; [condition]; [itérateur]) {}		Les méthodes peuvent être appelées sur des objets. Exemples : \$a = "Ceci est une chaîne" \$a.ToUpper() \$a.SubString(0,3) \$a.SubString(0,(\$a.length/2)) \$a.Substring((\$a.length/2), (\$a.length/3))		
<b>Exemple :</b> for (\$i = 0; \$i -lt 5; \$i++) {Write-Object \$i}		Les méthodes statiques peuvent être appelées au moyen de l'opérateur « :: ». [DateTime]::IsLeapYear(2005)		
<b>Foreach (script)</b>		<b>Variables automatiques Windows PowerShell (liste non exhaustive)</b>	\$StackTrace	Dernière exception interceptée par Windows PowerShell
[:label] foreach (identificateur dans la collection) {} Expression   foreach {} Expression   foreach {BEGIN{} PROCESS{} END{}}		\$ Dernier jeton de la ligne de commande précédente	\$Switch	Énumérateur d'une instruction switch
<b>Exemples :</b> \$i = 1,2,3 foreach (\$z in \$i) {Write-Object \$z} Get-Process   foreach {BEGIN{\$x=1} PROCESS{\$X++} END{"\$X Processées"}}		\$ ? État booleen de la dernière commande		<b>Propriétés d'objets</b>
<b>Function (script)</b>		\$^ Premier jeton de la ligne de commande précédente		Les propriétés d'un objet peuvent être référencées directement avec l'opérateur « .. ». \$a = Get-Date \$a.Date
function MyFunction { write-object \$args[0] }				

\$a.TimeOfDay.Hours Les propriétés statiques peuvent être référencées avec l'opérateur « :: ». [DateTime]::Now  Précédence des opérateurs Dans Windows PowerShell, les opérateurs sont évalués selon la précédence suivante : () {}, @ \$, !, [ ], ., &, ++ --, + -, * / % unaires, + - binaires, opérateurs de comparaison, -and -or,  , > >>, =	Blocs de script		<b>Exemple :</b> \$var = "word1","word2","word3" switch -regex (\$var) { "word1" {"Multi-match Exact " + \$_} "word2" {"Multi-match Exact " + \$_} "w.*2" {"Pattern match Exact " + \$_} default {"Multi-match Default " + \$_} }  <b>Résultat :</b> Multi-match Exact word1 Multi-match Exact word2 Pattern match Exact word2 Multi-match Default word3  <b>Throw</b>
Scripts			
Les commandes Windows PowerShell peuvent être stockées dans et exécutées à partir de fichiers de script. L'extension de fichier des scripts Windows PowerShell est « .ps1 ». Des paramètres peuvent être passés à un script et un script peut retourner une valeur. <b>Exemple :</b> \$sum = MyAdder.ps1 1 2 3			
Chaines			
Constantes de chaîne : "ceci est une chaîne, cette \$variable est étendue comme \$(2+2)" 'ceci est une chaîne, cette \$variable n'est pas étendue' @" Ceci est une "chaîne ici" qui peut contenir n'importe quoi y compris des retours chariot et des guillemets. Les expressions \$(2+2) sont évaluées "@ @' La "chaîne ici" avec guillemets simples n'évalue pas d'expressions. '@			
Opérateurs de chaîne			
+      Concaténer deux chaînes			
*      Répéter une chaîne un certain nombre de fois			
-f      Mettre en forme une chaîne (spécificateurs de format .NET)			
-replace      Opérateur de remplacement "abcd" -replace "bc", "TEST" aTESTd			
-match      Correspondance d'expression régulière			
-like      Concordance par caractères génériques			
Switch (script)			
La variable \$_ est disponible dans le script. \$_ représente la valeur actuelle évaluée. Si un tableau est utilisé dans switch, chaque élément du tableau est testé.		<b>Variables</b> <b>Format :</b> [\$scope:]name or \${anyname} or \${any path}  <b>Exemples :</b> \$a = 1 \${!@#\$%^&*()}=3 \$global:a = 1 # visible partout \$local:a = 1 # définie dans cette portée et visible pour les enfants \$private:a = 1 # identique à local, mais invisible pour les portées enfants	

\$script:a=1 # visible pour tout dans ce script \$env:path = "d:\windows" \${C:\TEMP\testfile.txt}="Ceci écrit dans un fichier" Get-Variable -scope 1 a #Obtient une valeur de la portée parente Get-Variable -scope 2 a # grand-parent	2+2	Le mode Expression démarre avec un nombre.
	"text"	Le mode Expression démarre avec un guillemet.
	text	Le mode Commande démarre avec une lettre.
	& "text"	Le mode Commande démarre avec une esperluette.
	. "file.ps1"	Le mode Commande démarre avec un point suivi d'un espace.
	.125	Le mode Expression démarre avec un point suivi d'un nombre, et non d'un espace ou d'une lettre.
	.text	Le mode Commande démarre avec un point qui fait partie du nom de commande « .text ».
<b>While (script)</b> [:label] while (condition) { ... }  do { ... } while (condition)		Combiner des expressions et des commandes est très utile. Vous pouvez pour ce faire utiliser des parenthèses. Dans les parenthèses, le processus de découverte du mode recommence. Write-Host (2+2) 2+2 est traité comme une expression à évaluer et passé à la commande <b>Write-Host</b> . (Get-Date).day + 2 <b>Get-Date</b> est traité comme une commande et le résultat de son exécution devient la valeur de gauche dans l'expression. Vous pouvez imbriquer des commandes et expressions sans restrictions. Write-Host ((Get-Date).day + 2) <b>Get-Date</b> est une commande. ((Get-Date).day+2) est une expression et Write-Host ((Get-Date).day + 2) est de nouveau une commande. Write-Host ((Get-Date) - (Get-Date).date) La commande <b>Get-Date</b> est utilisée deux fois pour calculer le temps écoulé depuis minuit (condition).
<b>Analyse</b> Windows PowerShell propose deux modes d'analyse : Commande et Expression. En mode Expression, Windows PowerShell analyse comme le font la plupart des langages de haut niveau : les nombres sont des nombres ; les chaînes doivent figurer entre guillemets, etc. Les expressions sont des éléments tels que : 2+2 4 "Hello" + " world" Hello world \$a = "hi" \$a.length * 13 26 Lors de l'analyse en mode Commande, les chaînes n'ont pas besoin de figurer entre guillemets et tout est traité comme une chaîne à l'exception des variables et des éléments entre parenthèses. Par exemple : copy users.txt accounts.txt users.txt et accounts.txt sont traités comme des chaînes write-host 2+2 2+2 est traité comme une chaîne et non comme une expression à évaluer copy \$src \$dest \$src et \$dest sont des variables. Le fait de ne pas avoir à utiliser de guillemets lors du travail dans un environnement de commande peut être très avantageux sur le long terme, car cela réduit considérablement le volume de saisie nécessaire. Le mode d'analyse est déterminé par le premier jeton rencontré. Si le jeton est un nombre, une variable ou une chaîne entre guillemets, l'environnement utilise le mode Expression. Si la ligne commence par une lettre, une esperluette (&) ou un point(.) suivie d'un espace ou d'une lettre, l'analyse est effectuée en mode Commande.		

## WINDOWS SERVER

### ACTIVE DIRECTORY

Active Directory (AD) est la mise en œuvre de Microsoft des services d'**annuaire** pour une utilisation principalement destinée aux environnements Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un **réseau** administré tels que les comptes d'utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées. Si les administrateurs ont renseigné les attributs convenables, il sera possible d'interroger l'annuaire pour obtenir par exemple : « toutes les imprimantes couleurs à cet étage du bâtiment ».

Le service d'annuaire Active Directory peut être mis en œuvre sur [Windows 2000 Server](#), [Windows Server 2003](#) et [Windows Server 2008](#), il résulte de l'évolution de la base de compte plane SAM. Un serveur informatique hébergeant l'annuaire Active Directory est appelé **contrôleur de domaine**.

Active Directory stocke ses informations et paramètres dans une base de données centralisée. La taille d'une base Active Directory peut varier de quelques centaines d'objets pour de petites installations à plusieurs millions d'objets pour des configurations volumineuses.

Dans les premiers documents Microsoft mentionnant son existence, *Active Directory* s'est d'abord appelé **NTDS** (pour **NT Directory Services**, soit « Services d'annuaire de NT » en français). On peut d'ailleurs encore trouver ce nom dans la littérature couvrant le sujet ainsi que dans certains utilitaires AD comme **NTDSUTIL .EXE** par exemple, ou le nom du fichier de base de données **NTDS .DIT**.

### STRUCTURE D'ACTIVE DIRECTORY

#### OBJETS

Active Directory est un service d'**annuaire** utilisé pour stocker des informations relatives aux ressources réseau sur un **domaine**.

Une structure Active Directory (AD) est une organisation hiérarchisée d'objets. Les objets sont classés en trois grandes catégories : les ressources (par exemple les imprimantes), les services (par exemple le courrier électronique) et les utilisateurs (comptes utilisateurs et groupes). L'AD fournit des informations sur les objets, il les organise et contrôle les accès et la sécurité.

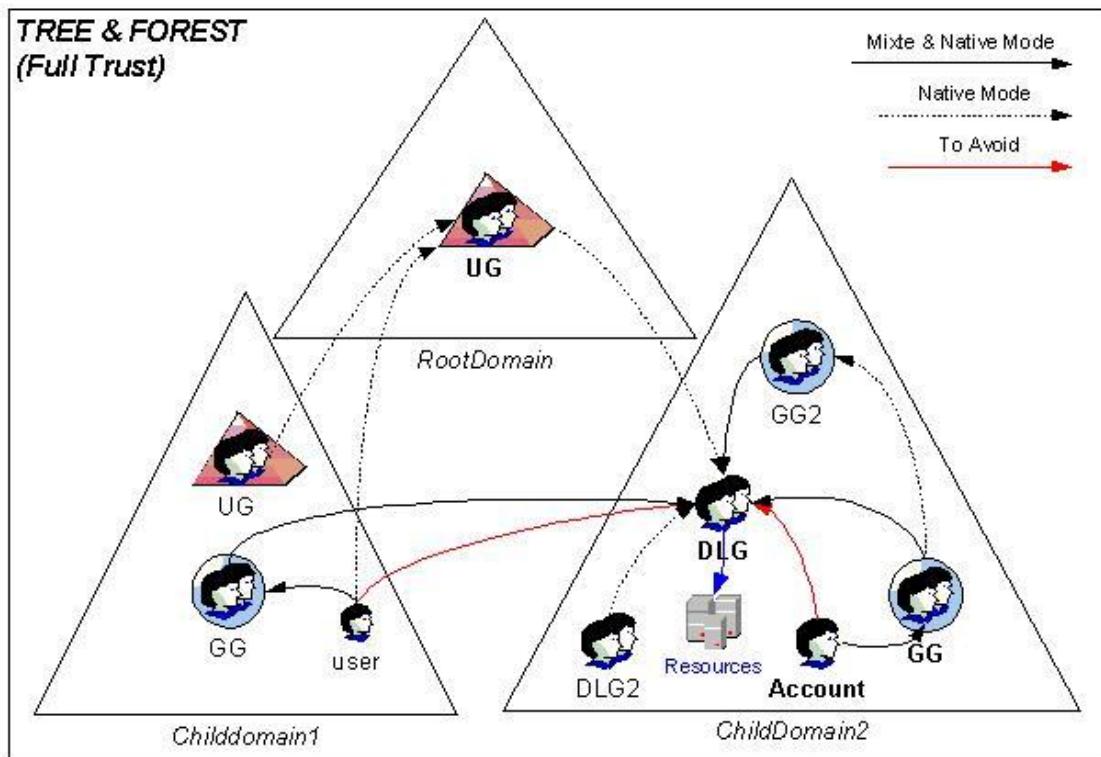
Chaque objet représente une entité unique – utilisateur, ordinateur, imprimante ou groupe – ainsi que ses attributs. Certains objets peuvent également être des conteneurs pour d'autres objets. Un objet est identifié de manière unique dans l'AD par son nom et possède son

propre jeu d'attributs – les caractéristiques et les informations que l'objet peut contenir – défini par un schéma, qui détermine également le type d'objets qui peuvent être stockés dans l'AD.

Chaque objet attribut peut être utilisé dans plusieurs classes d'objets de schéma différents. Ces objets de schéma existent pour permettre au schéma d'être étendu ou modifié si nécessaire. Cependant, comme chaque objet de schéma est intégral à la définition des objets de l'AD, la désactivation ou la modification de ces objets peut avoir de graves conséquences car elle entraîne des modifications fondamentales dans la structure de l'AD. Un objet de schéma, lorsqu'il est modifié, est automatiquement propagé dans Active Directory est une fois créée, il ne peut plus être supprimé (il peut seulement être désactivé). Pour cette raison, une modification du schéma doit être mûrement réfléchie et planifiée.

Le nombre de types d'objets disponibles dans un Active Directory n'est pas limité, en voici quelques exemples :

- OU : l'Unité d'Organisation : Dans l'arborescence, ce sont des conteneurs qui permettent de créer une hiérarchie d'objets au sein d'un domaine. Ces OU sont principalement utilisés pour permettre la délégation de droit et pour l'application [GPO](#). Les OU sont parfois confondues avec les groupes, qui sont des objets et non des conteneurs.
- Ordinateur
- Utilisateur
- Groupe : il est principalement destiné à établir des listes d'utilisateurs pour leur attribuer des droits ou des services. On distingue trois types de groupes :
  - Le groupe local : il ne peut comprendre que des utilisateurs de son propre domaine.
  - Le groupe global : au sein d'un domaine, il est principalement utilisé pour affecter des droits à des ressources dans un domaine. Il peut comprendre des utilisateurs, des groupes globaux ou universels, issus d'autres domaines.
  - Le groupe universel : disponible depuis la version 2000, permet d'inclure des groupes et utilisateurs d'autres domaines.



Active Directory étant un annuaire objet, la notion de schéma définit les contraintes concernant la dérivation et l'héritage des objets, sensiblement de la même manière qu'en programmation objet. Cela introduit également la notion d'extension, permettant d'ouvrir l'annuaire à toutes sortes d'applications souhaitant stocker des objets personnalisés au niveau du ou des domaines constituant la forêt Active Directory.

## UNITE ORGANISATIONNELLE

Une unité organisationnelle (OU ; UO) est un objet conteneur qui permet de hiérarchiser Active Directory. Cette notion était inexistante dans les « versions précédentes » d'AD, telle que la base de données SAM. L'AD permet une hiérarchisation des domaines. A l'intérieur de ces domaines, il existe maintenant des possibilités de structuration et de hiérarchisation des utilisateurs.

Les OU sont le meilleur moyen de créer ces structures hiérarchiques dans Active Directory. Outre la structuration d'informations, qui offre une clarté accrue dans les annuaires complexes notamment, les OU présentent également un avantage important : elles tiennent lieu de frontière pour la délégation d'autorisations administratives. Il est donc possible de personnaliser les droits des différents utilisateurs/groupes de façon ciblée (gestion des mots de passe ; droits d'accès : autorisations concernant les installations...).

## FORETS, ARBORESCENCES ET DOMAINES

Active Directory introduit la notion de hiérarchie, inhérente aux annuaires objets dérivés de X.500, sous la forme d'une arborescence dans laquelle les utilisateurs et les ordinateurs sont organisés en groupes et sous-groupes afin de faciliter l'administration des droits et restrictions utilisateur. C'est aussi Active Directory qui gère l'authentification des utilisateurs de Windows. Active Directory exploite cette notion de hiérarchie intensivement, puisque

l'entité de sécurité appelé « domaine » est également hiérarchisée dans un ensemble partageant un espace de nom commun, appelé « arborescence », enfin, l'entité de plus haut niveau regroupant les arborescences de domaines constitue la forêt Active Directory.

Active Directory permet une réPLICATION multi-maître, c'est-à-dire que chaque contrôleur de domaine peut être le siège de modifications (ajout, modification, suppression) de l'annuaire, sous réserve de permission accordée par **ACL**, qui seront répliquées sur les autres contrôleurs de domaine. SAM ne disposait que d'une seule base en écriture, les autres répliques étant en lecture seule.

Le mécanisme de réPLICATION de ces modifications peut profiter de **RPC** (liaisons **TCP/IP** rapides et disponibles) ou **SMTP** dans les autres cas. La topologie de réPLICATION est générée automatiquement mais elle peut être personnalisée par l'administrateur, tout comme sa planification.

A noter que les ensembles d'espaces de nom correspondant aux arborescences d'Active Directory formant la forêt Active Directory sont superposables à l'espace de nom formé par les zones DNS. DNS est un service indispensable pour le bon fonctionnement de toute l'architecture Active Directory, localisation des contrôleurs de domaine, réPLICATION, etc.

Une arborescence Active Directory est donc composée de :

- La forêt : structure hiérarchique d'un ou plusieurs domaines INDEPENDANTS (ensemble de tous les sous domaines Active Directory).
- L'arbre : domaine et toutes ramifications. Par exemple, dans l'arbre *domaine.tld*, *sous1.domaine.tld*, *sous2.domaine.tld* et *photo.sous1.domaine.tld* sont des sous-domaines de *domaine.tld*.
- Le domaine : constitue les feuilles de l'arborescence. *Photo.sous1.domaine.tld* peut-être un domaine au même titre que *domaine.tld*.

Le modèle de données Active Directory est dérivé du modèle de données de la norme X.500 : l'annuaire contient des objets représentant des éléments de différents types décrits par des attributs. **Les stratégies de groupes** (GPO) sont des paramètres de configuration appliqués aux ordinateurs ou aux utilisateurs lors de leur initialisation, ils sont également gérés dans Active Directory.

Le protocole principal d'accès aux annuaires est **LDAP** qui permet d'ajouter, de modifier et supprimer des données enregistrées dans Active Directory, et qui permet en outre de rechercher et de récupérer ces données. N'importe quelle application cliente conforme à LDAP peut être utilisée pour parcourir et interroger Active Directory ou pour y ajouter, y modifier ou y supprimer des données.

## ROLES UNIQUES

Certaines fonctions, - on parle de rôles - ne peuvent être prises en charge que par un serveur unique, le maître d'opérations (*Operation master* en anglais). Ces rôles, appelés **FSMO** (abréviation de *Flexible Single Master Operations*) peuvent être pris en charge par n'importe quel contrôleur de domaine (mais par un seul à la fois), ils sont au nombre de 5:

Nom du rôle	Position	Description
<b>Maître de schéma (Schéma Master)</b>	1 par forêt	Contrôle les modifications apportées au schéma de données Active Directory.

<b>Maître d'attribution de noms de domaine (Domain Naming Master)</b>	1 par forêt	Contrôle l'ajout et la suppression des noms de domaines dans une forêt afin de garantir leur unicité.
<b>Émulateur de PDC (PDC Emulator)</b>	1 par domaine	Se comporte comme un contrôleur de domaine NT4 pour permettre le support de clients NT4 (par exemple pour gérer les changements de mots de passe), ce contrôleur fournit également l'horloge de référence du domaine.
<b>Maître RID (RID Master)</b>	1 par domaine	Fournit des tranches d'identifiants uniques aux autres contrôleurs de domaine.
<b>Maître d'infrastructure (Infrastructure Master)</b>	1 par domaine	Synchronise les changements inter-domaines.

## NOMMAGE

Active Directory prend en charge l'utilisation de noms **UNC** (\), **URL** (/), et **LDAP** pour l'accès aux objets. En interne, AD utilise la version LDAP de la structure de noms de X.500.

Chaque objet possède un identifiant unique, le nom unique (DN pour *Distinguished name*), ainsi un objet imprimante appelé *HPLaser3* dans l'OU *Marketing* et faisant partie du domaine *foo.org* aura comme DN : *CN=HPLaser3,OU=Marketing,DC=foo,DC=org* où *CN* est le nom commun (*Common Name* en anglais) et *DC* un composant de domaine. Un DN peut être constitué de bien plus de quatre éléments. L'objet peut ainsi également posséder un nom canonique (*Canonical name*), généralement le DN inversé, sans identifiants, et utilisant la barre oblique (slash) comme séparateur : *foo.org/Marketing/HPLaser3*. Afin d'identifier l'objet à l'intérieur de son conteneur, AD utilise un nom unique relatif (RDN pour *Relative distinguished name*) : *CN=HPLaser3*. Chaque objet possède également un identifiant global unique (**GUID**, pour *Globally Unique Identifier*) qui est une chaîne de caractères de 128 bits unique et non modifiable, utilisé par AD pour les opérations de recherche et de réPLICATION. Certains objets possèdent également un nom utilisateur principal (UPN, pour *User principal name*), se présentant sous la forme *nom\_objet@nom\_domaine*.

## RELATIONS D'APPROBATION

Afin de permettre aux utilisateurs d'un domaine d'accéder aux ressources d'un autre domaine, AD utilise un mécanisme de relations d'approbation.

Les relations d'approbation au sein d'une même forêt sont automatiquement créées au moment de la création des domaines. Les limites par défaut des relations d'approbation sont fixées au niveau de la forêt, et non du domaine, elles sont implicites, et automatiquement transitives pour tous les domaines d'une même forêt. Toutes les relations d'approbation au sein d'une forêt sont bidirectionnelles et transitives. Cependant, afin de se connecter à d'autres forêts ou à des domaines non-AD, AD met en œuvre d'autres types de relations d'approbation : les approbations de type *raccourci* (shortcut) (jointures de deux domaines appartenant à des arborescences différentes, transitives, uni ou bidirectionnelles), *forêt* (forest) (transitives, uni ou bidirectionnelles), *royaume* (realm) (transitives ou intransitives, uni ou bidirectionnelles) ou *externe* (intransitives, uni ou bidirectionnelles).

## APPROBATIONS DANS WINDOWS 2000 (MODE NATIF)

- **Unidirectionnelle** - Lorsqu'un domaine permet aux utilisateurs d'accéder à un autre domaine, mais que cet autre domaine n'autorise pas l'accès aux utilisateurs du premier domaine.
- **Bidirectionnelle** - Lorsque deux domaines permettent à leurs utilisateurs l'accès à l'autre domaine.
- **Domaine d'approbation** - Le domaine qui autorise l'accès aux utilisateurs d'un domaine approuvé.
- **Domaine approuvé** - Le domaine qui est approuvé, dont les utilisateurs ont accès au domaine d'approbation.
- **Approbation transitive** - Approbation qui peut s'étendre au-delà des deux domaines aux autres domaines approuvés de la même arborescence.
- **Approbation non transitive** - Approbation unidirectionnelle non étendue au-delà des deux domaines.
- **Approbation explicite** - Approbation créée par un administrateur. Non transitive et unidirectionnelle uniquement.
- **Approbation croisée** - Approbation explicite entre domaines de différentes arborescences ou faisant partie de la même arborescence lorsqu'aucune relation descendant/ancêtre (enfant/parent) n'existe entre les deux domaines.

Windows 2000 - prend en charge les types d'approbation suivants:

- Approbations transitives bidirectionnelles.
- Approbations non transitives unidirectionnelles.

D'autres types d'approbations peuvent être créés par les administrateurs. Ces approbations peuvent être de type:

- Raccourci

## APPROBATION SUPPLEMENTAIRE DANS WINDOWS 2003 (MODE NATIF)

Windows Server 2003 introduit un nouveau type d'approbation appelé approbation de forêt. Ce type d'approbation permet à tous les domaines d'une forêt d'approuver de manière transitive tous les domaines d'une autre forêt. Pour que cette nouvelle fonctionnalité soit disponible, il faut absolument que les deux forêts mises en relations aient un niveau fonctionnel Windows Server 2003. L'authentification à travers ce type d'approbation doit être basée sur [Kerberos](#) (et non [NTLM](#)). Les approbations de forêt sont transitives pour tous les domaines appartenant aux forêts approuvées.

## ADAM

ADAM (pour **Active Directory Application Mode**) est une version plus légère d'Active Directory spécifiquement dédiée à une utilisation au niveau applicatif. ADAM peut être exécuté en tant que service sur des ordinateurs équipés de Windows Server 2008, Windows Server 2003, Windows XP Professionnel, ou des Éditions Professionnelle, Entreprise ou Intégrale de Windows Vista. Développé sur la même base de code qu'Active Directory, ADAM fournit les mêmes fonctionnalités qu'AD, ainsi qu'une API identique, mais il ne requiert pas la création de domaines et ne nécessite pas de contrôleur de domaine pour fonctionner.

Tout comme Active Directory, ADAM fournit un espace de stockage utilisé pour stocker les données d'annuaire (le *Data Store*) ainsi qu'un service d'annuaire muni d'une interface de service d'annuaire LDAP. À la différence d'Active Directory, plusieurs instances d'ADAM peuvent être exécutées simultanément sur le même serveur, chaque instance étant spécifiquement adaptée aux besoins des applications auxquelles elle est destinée et utilisant le service d'annuaire ADAM.

## INTEGRATION D'UNIX DANS ACTIVE DIRECTORY

---

De nombreux éditeurs proposent des solutions d'intégration à Active Directory pour les plates-formes Unix (UNIX, Linux, Mac OS X, ainsi que nombre d'applications Java et UNIX). On peut citer ADmitMac de Thursby Software Systems, Vintela Authentication Services de Quest Software, DirectControl de Centrify et Likewise de Centeris Software. Microsoft propose également un produit gratuit, **Microsoft Windows Services for UNIX**. Les versions récentes des systèmes d'exploitation Linux et Unix fournissent des niveaux d'interopérabilité variés avec Active Directory comme la prise en charge des [stratégies de groupe](#). Une alternative possible est d'utiliser un autre service d'annuaire comme par exemple [389 Directory Server](#) (ex-Netscape Directory Server) capable d'effectuer une synchronisation bidirectionnelle avec Active Directory et fournir ainsi une intégration "déviée" consistant à faire s'authentifier sur FDS les machines Unix et Linux tout en conservant l'authentification Active Directory native pour les machines Windows.

## QUELQUES NOTIONS

---

### DOMAINE

---

#### LE CONCEPT DE DOMAINE CHEZ MICROSOFT

---

Chez Microsoft, un domaine est une entité logique vue comme une enveloppe étiquetée. Il reflète le plus souvent une organisation hiérarchique dans une entreprise. Par exemple, le domaine "COMPTA" désigne l'ensemble des machines réseau (stations, imprimantes, ...) du service Comptabilité, et les comptes utilisateurs qui sont autorisés à s'y connecter.

Le domaine permet à l'administrateur réseau de gérer plus efficacement les utilisateurs des stations déployées au sein de l'entreprise car toutes ces informations sont centralisées dans une même base de données.

Cette base de donnée est stockée sur des serveurs particuliers (Windows Server NT4, 2000, 2003), appelés Contrôleurs de Domaine (*Domain Controller*, en anglais).

#### ENVIRONNEMENT WINDOWS NT 3.5, 3.51 OU 4

---

On distingue le domaine de "comptes" d'un domaine de "ressources". Le premier maintient à jour et stocke la liste des utilisateurs (nom de login, mot de passe) et leur habilitation (droits à accéder à des ressources réseau, droits à partager ...). Le second définit plutôt un ensemble de partages réseau (disques, imprimantes, ...) qui sont mis à la disposition des autres stations (clients) du réseau (comme des Windows XP).

#### ENVIRONNEMENT WINDOWS 2000 OU 2003

---

Avec l'Active Directory de Microsoft, les notions de domaine de "comptes" et de "ressources" sont fusionnées. Il apparait de nouvelles notions :

- Les arbres réunissent plusieurs domaines qui peuvent communiquer
- Les forêts joignent des domaines disjoints ; la forêt réunit aussi des sites différents ;

**Attention : les concepts de sites et d'unités organisationnelles dans Active Directory sont deux concepts très différents de celui de domaine.**

## STRATEGIES DE GROUPE

Les **stratégies de groupe** (ou GPO pour *Group Policy Object*) sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement *Active Directory*. Les stratégies de groupe font parties de la famille des technologies IntelliMirror, qui incluent la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection des dossiers ainsi que la gestion des fichiers en mode déconnecté.

Bien que les stratégies de groupe soient régulièrement utilisées dans les entreprises, elles sont également utilisées dans les écoles ou dans les petites organisations pour restreindre les actions et les risques potentiels comme par exemple le verrouillage du panneau de configuration, la restriction de l'accès à certains dossiers, la désactivation de l'utilisation de certains exécutables, etc.

## PRESENTATION

Les stratégies de groupe peuvent contrôler des clés de registre, la sécurité NTFS, la politique de sécurité et d'audit, l'installation de logiciel, les scripts de connexion et de déconnexion, la redirection des dossiers, et les paramètres d'Internet Explorer. Les paramétrages sont stockés dans les stratégies de groupe. Chaque stratégie de groupe possède un identifiant unique appelé GUID (« *Globally Unique Identifier* »). Chaque stratégie de groupe peut être liée à un ou plusieurs domaine, site ou unité d'organisation *Active Directory*. Cela permet à plusieurs objets ordinateurs ou utilisateurs d'être contrôlés par une seule stratégie de groupe et donc de diminuer le coût d'administration globale de ces éléments.

Les stratégies de groupe utilisent des fichiers de modèle d'administration avec les extensions .ADM ou .ADMX qui décrivent les clés de registre modifiées par l'application des stratégies de groupe. Sur un ordinateur de travail, les modèles d'administration sont stockés dans le répertoire %WinDir%\Inf, alors que sur un contrôleur de domaine Active Directory, pour chaque domaine et pour chaque stratégie de groupe, ils sont stockés dans un répertoire individuel (Le « *group policy template* », ou GPT) au sein du répertoire Sysvol. Les fichiers .ADMX sont des fichiers basés sur le format XML et introduits par Windows Vista pour la gestion des stratégies de groupe.

Les stratégies de groupe sont analysées et appliquées au démarrage de l'ordinateur et pendant l'ouverture de session de l'utilisateur. Les ordinateurs rafraîchissent les paramètres transmis par les stratégies de groupe de façon périodique, généralement toutes les 60 ou 120 minutes, ce paramètre étant ajustable par un paramètre de stratégie de groupe.

Les stratégies de groupe sont supportées sur Windows 2000, Windows XP Pro, Windows Vista, Windows 2003, Windows 2008 et Windows 7.

En juin 2006, la société Centrify annonce la prise en charge des stratégies de groupe sur les systèmes Mac OS, Linux et UNIX en utilisant leur logiciel DirectControl.

## LES TROIS PHASES DE L'UTILISATION DES STRATEGIES DE GROUPE

Les stratégies de groupe peuvent être considérées en trois phases distinctes - Création de la stratégie de groupe, Liaison des stratégies de groupe et application des stratégies de groupe.

### CREATION ET EDITION DES STRATEGIES DE GROUPE

Les stratégies de groupe peuvent être éditées au travers de deux outils - le *Group Policy Object Editor* (`Gpedit.msc`) et la *Group Policy Management Console* (`gpmc.msc`). GPEdit est utilisé pour créer et éditer une stratégie de groupe de façon unitaire. La GPMC simplifie grandement la gestion des stratégies de groupe en fournissant un outil permettant une gestion centralisée et collective des objets. La GPMC inclut de nombreuses fonctionnalités telles que la gestion des paramètres, un panneau pour la gestion du filtrage par groupe de sécurité, des outils de sauvegarde et de restauration et d'autres outils graphiques intégrés à la MMC. Le nom d'une stratégie de groupe peut être déterminé en utilisant l'outil `GPOTool.exe`.

### LIAISON DES STRATEGIES DE GROUPE

Après avoir créé une stratégie de groupe, elle peut être liée à un site Active Directory, à un domaine ou à une unité d'organisation (OU).

### APPLICATION DES STRATEGIES DE GROUPE

Le client de stratégie de groupe du poste récupère la configuration (de base dans un intervalle aléatoire compris entre 60 et 120 minutes, mais cela est configurable via les stratégies de groupe) qui est applicable à l'ordinateur et à l'utilisateur connecté et l'applique en tenant compte des différents critères de filtre, de sécurité et d'héritage.

### LES STRATEGIES DE GROUPE LOCALES

Les stratégies de groupe locales sont une version plus basique des stratégies de groupe utilisées avec Active Directory. Dans les versions antérieures à Windows Vista, les stratégies de groupe locales peuvent être utilisées sur un ordinateur local, mais ne peuvent pas être utilisées pour des comptes utilisateur ou des groupes. La limitation liée aux utilisateurs peut être contournée en utilisant l'éditeur de base de registre pour modifier les clés sous `HKCU` ou `HKU`. Les stratégies de groupe locales réalisent des modifications sous la clé `HKLM`, ce qui affecte tous les utilisateurs ; les mêmes changements peuvent être effectués sous `HKCU` ou `HKU` pour affecter uniquement certains utilisateurs. Microsoft fournit des informations complémentaires sur le site Technet.

Windows Vista supporte les stratégies de groupe locales multiples, qui permettent de positionner les paramètres pour les utilisateurs individuels.

## QUELQUES COMMANDES

Il est possible de vérifier l'application des GPO manuellement avec les commandes `gpresult` (sous Windows 2003 et Windows XP)

`GPResult`

Il est possible de forcer l'application des GPO manuellement avec les commandes `gpupdate` (sous Windows 2003 et Windows XP)

`GPUpdate /Force`

`secedit (Windows 2000)`

*Secedit /RefreshPolicy machine\_policy /ENFORCE* pour les GPO s'appliquant aux ordinateurs.

*Secedit /RefreshPolicy user\_policy /ENFORCE* pour les GPO s'appliquant aux utilisateurs.

Les GPO sont supportées sur Windows 2008, Vista, Windows 2003, Windows XP Professionnel, Windows 2000.

## RAID

En informatique, le mot RAID désigne les techniques permettant de répartir des données de plusieurs disques durs afin d'améliorer soit la tolérance aux pannes, soit la sécurité, soit les performances de l'ensemble, ou une répartition de tout cela.

L'acronyme RAID a été défini en 1987 par l'Université de Berkeley, dans un article nommé « A Case for Redundant Arrays Of Inexpensive Disks (RAID) », soit « chaîne redondante de disques peu onéreux ». Aujourd'hui, le mot est devenu l'acronyme de « Redundant Array Of Independent (or Inexpensive) Disks, ce qui signifie « chaîne redondante de disques indépendants ». Le coût du mégaoctet des disques durs ayant diminué d'un facteur 1 300 000 en 29 ans, aujourd'hui le RAID est choisi pour d'autres raisons que le coût de l'espace de stockage.

### L'HISTORIQUE DU RAID

En 1978, un employé d'IBM, Norman Ken Ouchi, déposa un brevet concernant un « Système de récupération de données stockées dans une unité de stockage défectueuse », et dont la description était ce que deviendrait plus tard le RAID 5. Ce brevet fait également mention du miroitement de disque (qui sera appelé plus tard RAID 1), ainsi que de la protection avec une parité dédiée (qui sera appelé plus tard RAID 3 et 4).

La technologie RAID a été élaborée par un groupe de chercheurs de l'Université de Berkeley(Californie) en 1987. Ces derniers étudièrent la possibilité de faire reconnaître deux disques durs ou plus comme une seule unité par le système. Ils obtinrent pour résultat un système de stockage aux performances bien meilleures que celles des systèmes à disque dur unique, mais doté d'une très mauvaise fiabilité. Les chercheurs s'orientèrent alors vers des architectures redondantes, afin d'améliorer la tolérance aux pannes du système de stockage.

En 1988, les différents RAID, de type 1 à 5, étaient formellement définis par David Patterson, Garth Gibson et Randy Katz dans la publication intitulée « *A Case for Redundant Arrays of Inexpensive Disks (RAID)* ». Cet article introduisait le terme « RAID », dont l'industrie du disque s'est immédiatement emparée, dont elle proposait cinq niveaux différents, en les comparants au « SLED », chacun d'eux ayant ses avantages et ses inconvénients.

### DESCRIPTION ET CONCEPTS

#### COMPARAISON RAID/SLED

Depuis sa création, la particularité principale de l'architecture RAID est sa capacité à combiner de nombreux périphériques de stockage bon marché et d'une technologie courante dans une matrice unique, de sorte que ce groupement offre une capacité, une fiabilité et/ou des performances accrues, ce pour un coût largement inférieur à un périphérique de stockage unique équivalent exploitant des technologies de pointe. L'architecture RAID s'oppose donc à l'architecture SLED (Single Large Expensive Disk), qui est fondée sur l'utilisation d'un seul et même disque dur de grande capacité, donc d'un prix élevé, car celui-ci doit non seulement pouvoir stocker beaucoup d'informations, mais il doit de plus être d'excellente qualité pour garantir au mieux la pérennité et l'accèsibilité de son contenu.

En effet, dans une architecture de type SLED, la conne conservation des données est dépendante de la moindre défaillance du disque dur. Lorsqu'une panne survient, non seulement le système est inexploitable le temps du remplacement du matériel défectueux, mais la seule manière de récupérer les données est de procéder à une restauration de la dernière sauvegarde, ce qui peut prendre plusieurs heures durant lesquelles le système est toujours inutilisable.

Si un tel temps d'inactivité est acceptable pour l'ordinateur d'un particulier, il est en revanche rédhibitoire pour le système informatique d'une entreprise, pour qui une telle panne peut avoir des conséquences non négligeables sur sa santé financière. L'utilisation d'une architecture RAID du moins dans la plupart de ses niveaux fonctionnels, permet justement d'apporter une réponse à ces besoins car non seulement la défaillance d'un des disques de la grappe ne gêne pas le fonctionnement des autres disques dur, ce qui permet au système de continuer de fonctionner, mais de surcroît, une fois le disque en panne échangé, son contenu est reconstruit à partir des autres disques permettant le fonctionnement normal du système. Ainsi l'activité de l'entreprise continue de façon ininterrompue et transparente pendant toute la durée de l'incident.

Le RAID, suivant ses niveaux fonctionnels, s'il donne des de réponse identiques à ceux des disques s'ils étaient utilisés individuellement, offre des débits particulièrement soutenus, même en utilisant des disques durs bons marchés et de performances moyennes, tout en garantissant une bien meilleure fiabilité (sauf pour le RAID 0 qui la réduit d'autant que le nombre de disques). Dans de telles situations, les architectures RAID se révèlent donc idéales, tant du point de vue de leurs performances que de leur fiabilité. Dans tous les cas, le RAID reste complètement transparent à l'utilisateur qui, quel que soit le nombre de disques physiques utilisées pour construire le RAID, ne verra jamais qu'un seul grand volume logique, auquel il accédera de façon tout à fait habituelle.

## PARITE ET REDONDANCE

Le miroitage s'avère être une solution onéreuse, puisqu'il est nécessaire d'acquérir les périphériques de stockage en plusieurs exemplaires. Aussi, partant du principe que plusieurs unités ont une faible probabilité de tomber en panne simultanément, d'autres systèmes ont été imaginés, dont ceux permettant de régénérer les données manquantes à partir des données restant accessibles et d'une ou plusieurs données supplémentaires, dites de redondance.

Le système de redondance le plus simple et le plus largement utilisé est le calcul de parité. Ce système repose sur l'opération logique XOR (OU exclusif) et consiste à déterminer si sur n bits de données considérés, le nombre de bits à l'état 1 est pair ou impair. Si le nombre est pair, alors le bit de parité vaut 0. Si le nombre de 1 est impair, alors le bit de parité vaut 1. Lorsque l'un des n+1 bits de données ainsi formés devient indisponible, il est alors possible de régénérer le bit manquant en appliquant à nouveau la méthode sur les n éléments restants. Cette technique est utilisée dans les systèmes RAID 5.

Il existe des systèmes de redondances plus complexes et capables de générer plusieurs éléments de redondance afin de supporter l'absence de plusieurs éléments. Le RAID 6 utilise par exemple une technique de calcul de parité fondée sur des polynômes.

## LES DIFFERENTS TYPES DE SYSTEMES RAID

Le système RAID est :

- Soit un système de redondance qui donne au stockage des données une certaine tolérance aux pannes matérielles (ex : RAID 1) ;
- Soit un système de répartition qui améliore ses performances (ex : RAID 0) ;
- Soit les deux à la fois (ex : RAID 5) ;

Le système RAID est donc capable de gérer d'une manière ou d'une autre la répartition et la cohérence de ces données. Ce système de contrôle peut être purement logiciel ou utiliser un matériel dédié.

### RAID LOGICIEL

En RAID logiciel, le contrôle du RAID est intégralement assuré par une couche logicielle du système d'exploitation. Cette couche s'intercale entre la couche d'abstraction matérielle (pilote) et la couche du système de fichiers.

#### AVANTAGES

- C'est la méthode la moins onéreuse puisqu'elle ne demande aucun matériel supplémentaire.
- Cette méthode possède une grande souplesse d'administration (logicielle).
- Cette méthode présente l'avantage de la compatibilité entre toutes les machines équipées du même logiciel de RAID (c'est-à-dire du même système d'exploitation).

#### INCONVENIENTS

- L'inconvénient majeur réside dans le fait que cette méthode repose sur la couche d'abstraction matérielle des périphériques qui composent le volume RAID. Pour diverses raisons, cette couche peut être imparfaite et manquer de certaines fonctions importantes comme, par exemple, la détection et le diagnostic des défauts matériels et/ou la prise en charge du remplacement à chaud des unités de stockage.
- La gestion du RAID monopolise des ressources systèmes (légèrement le processeur et surtout le bus système) qui pourraient être employées à d'autres fins. La baisse de performances due à la gestion du RAID particulièrement sensible dans des configurations où le système doit transférer plusieurs fois les mêmes données comme, par exemple, en RAID 1, et, assez faible, dans des configurations sans redondance : exemple, le RAID 0.
- L'utilisation du RAID sur le disque système n'est pas toujours possible.

### RAID PSEUDO-MATERIEL

L'extrême majorité des contrôleurs RAID bon marché intégrés à de nombreuses cartes mères récentes en 2004/2005 gèrent souvent le RAID 0 et 1 sur des disques IDE ou SATA. Malgré le discours marketing qui tend systématiquement à induire en erreur sur ce point, il ne s'agit pas de RAID matériel à proprement parler mais plutôt d'un contrôle de disque doté de quelques fonctions avancées.

D'un point de vue strictement matériel, cette solution hybride n'est pas différente d'un RAID logiciel. Elle diffère cependant sur l'emplacement des routines logicielles de gestion du RAID.

## AVANTAGES

L'intérêt principal de ce type de RAID est d'apporter une solution au troisième du RAID logiciel, à savoir qu'il ne peut pas toujours servir à héberger les fichiers du système d'exploitation puisque c'est justement ce dernier qui permet d'y accéder.

Dans ce type de RAID, la présence d'un BIOS intégrant les routines logicielles basiques de gestion du RAID permet de charger en mémoire les fichiers essentiels du système d'exploitation (le noyau et les pilotes essentiels).

Puis, le pilote du contrôleur intègre les mêmes routines logicielles de gestion du RAID et fournit alors aux couches supérieures de l'OS non pas un accès aux périphériques mais un accès au volume RAID qu'il émule.

## INCONVENIENTS

En dehors de cet avantage important, ce type de RAID cumule les défauts des deux autres approches :

- Les limitations de performances sont les mêmes que pour le logiciel RAID car il s'agit effectivement d'un RAID logiciel camouflé.
- Un problème important posé par ces contrôleurs hybrides est leur piètre gestion des défauts matériels et leurs fonctionnalités BIOS généralement limitées.
- L'interopérabilité est très mauvaise surtout si l'on considère qu'il s'agit généralement de matériel intégré aux cartes mères des ordinateurs. Pire, le changement de carte mère (voire simplement de version de BIOS), si la nouvelle utilise des jeux de puces différents, peut imposer de reconstruire le RAID entièrement. De manière générale, une reconstruction est possible si l'on reste dans des contrôleurs RAID de même marque mais de modèles différents, mais il n'existe pas de règle définie de compatibilité.
- La fiabilité annoncée de ces dispositifs est assez controversée.

## RAID MATERIEL

Dans le cas du RAID matériel, une carte ou un composant est dédié à la gestion des opérations. Le contrôleur RAID peut être interne à l'unité centrale (carte d'extension) ou déporté dans une baie de stockage.

Un contrôleur RAID est en général doté d'un processeur spécifique, de mémoire, éventuellement d'une batterie de secours, et est capable de gérer tous les aspects du système de stockage RAID grâce au microcode embarqué (firmware).

Du point de vue du système d'exploitation, le contrôleur RAID matériel offre une virtualisation complète du système de stockage. Le système d'exploitation considère chaque volume RAID comme un disque et n'a pas connaissance de ses constituants physiques.

## AVANTAGES

- Les contrôleurs RAID matériels permettent la détection des défauts, le remplacement à chaud des unités défectueuses et offrent la possibilité de reconstruire de manière transparente les disques défaillants. Mais les systèmes d'exploitation permettent également cela si le matériel le permet.
- La charge système (principalement l'occupation du bus est allégée. (surtout dans des configurations avec beaucoup de disques et une forte redondance).

- Les vérifications de cohérence, les diagnostics et les maintenances sont effectués en arrière-plan par le contrôleur sans solliciter de ressources système.

### INCONVENIENTS

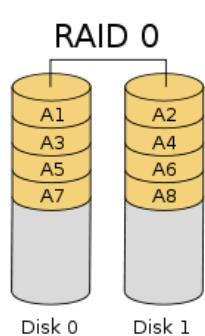
- Les contrôleurs RAID matériels utilisent chacun leur propre système pour gérer les unités de stockage. En conséquence, au contraire d'un RAID logiciel, des disques transférés d'un système à un autre ne pourront pas être récupérés si le contrôleur RAID n'est pas exactement le même (firmware compris). Il est donc conseillé de posséder une deuxième carte en cas de panne de la première.
- Les cartes d'entrée de gamme possèdent des processeurs de puissance bien inférieure à celle des ordinateurs actuels. On peut donc avoir de bien moins bonnes performances pour le même prix qu'un RAID logiciel.
- Le contrôleur RAID est lui-même un composant matériel, qui peut tomber en panne. Son logiciel (firmware) peut contenir des erreurs, ce qui constitue un autre risque de panne (un nouveau single-point-of-failure). Il est peu probable qu'un RAID actuel contient des erreurs de programmation (bugs) car ils sont garantis en moyenne une dizaine d'années.
- Les différents fabricants de contrôleurs RAID fournissent des outils de gestion logicielle très différents les uns des autres (et de qualité parfois inégale). A l'opposé, les outils de gestion du RAID logiciel fournis avec un système d'exploitation sont généralement bien intégrés dans ce système.
- La durée du support d'un contrôleur RAID par son constructeur (correction de bugs dans le firmware, par exemple), parfois liée à l'arrivée de nouveaux produits rendant les anciens obsolètes, peut-être moins longue ou plus volatile que le support RAID logiciel par le fournisseur du système d'exploitation. Le constructeur peut même disparaître (ce qui est assez rare parmi les fabricants de systèmes d'exploitation).
- Une moindre souplesse par rapport au RAID logiciel, qui dispose d'une couche d'abstraction permettant de gérer du RAID au-dessus de tout types de périphériques blocs supportés par le système d'exploitation, locaux ou distants (ATA, SCSI, ATA over Ethernet, iSCSI... et toutes les combinaisons possibles entre eux). Les contrôleurs RAID sont spécialisés pour un seul type de périphérique bloc.

## LES DIFFERENTS NIVEAUX DE RAID

### LES NIVEAUX STANDARD

Les différents types d'architecture RAID sont numérotés à partir de 0 et peuvent se combiner entre eux (on parlera alors de RAID 0+1, 1+0, etc.).

#### RAID 0 : VOLUME AGREGÉ PAR BANDES



Le RAID 0, également connu sous le nom d'« entrelacement de disques » ou de « volume agrégé par bandes » (striping en anglais) est une configuration RAID permettant d'augmenter significativement les performances de la grappe en faisant travailler  $n$  disques durs en parallèle (avec  $n \geq 2$ ).

- Capacité :

La capacité totale est égale à celle du plus petit élément de la grappe multiplié par le nombre d'éléments présent dans la grappe, car le système d'agrégation par bandes se retrouvera bloqué une fois que le

plus petit disque sera rempli (voir schéma). L'espace excédentaire des autres éléments de la grappe sera inutilisé. Il est donc conseillé d'utiliser des éléments identiques.

- **Fiabilité :**  
Le défaut de cette solution est que la perte d'un seul disque entraîne la perte de toutes les données.
- **Coût :**  
Le RAID 0 n'apportant pas de redondance, tout l'espace disque disponible est utilisé (tant que les deux disques ont la même capacité).

Dans cette configuration, les données sont réparties en bandes d'une taille fixe. Cette taille est appelée granularité.

Exemple : avec un RAID 0 ayant une bande de 64 Ko et composé de deux disques (disque Disk 0 et disque Disk 1), si l'on veut écrire un fichier A de 500 Ko, le fichier sera découpé en 8 bandes ( $\text{car } 7 < \frac{500}{64} \leq 8$ ), appelons-les 1, 2, 3, 4, 5, 6, 7 et 8, elles seront réparties sur l'ensemble des disques de la façon suivante :

Disk 0 : 1, 3, 5, 7

Disk 1 : 2, 4, 6, 8

Ainsi l'écriture du fichier pourra être effectuée simultanément sur chacun des disques en un temps équivalent à l'écriture de 256 Ko.

Ainsi, sur RAID 0 de  $n$  disques (avec  $n \geq 2$ ), chaque disque ne doit lire et écrire que  $\frac{1}{n}$  des données, ce qui a pour effet de diminuer les temps d'accès (lecture et écriture) aux données ; les disques se partagent le travail, les traitements se trouvent accélérés.

Ce type de RAID est parfait pour des applications requérant un traitement rapide d'une grande quantité de données. Mais cette architecture n'assure en rien la sécurité des données ; en effet, si l'un des disques tombe en panne, la totalité des données du RAID est perdue.

### RAID 1 : DISQUES EN MIROIR

Le RAID 1, consiste en l'utilisation de  $n$  disques redondants (avec  $n \geq 2$ ), chaque disque de la grappe contenant à tout moment exactement les mêmes données, d'où l'utilisation du mot « miroir » (mirroring en anglais).

- **Capacité :**

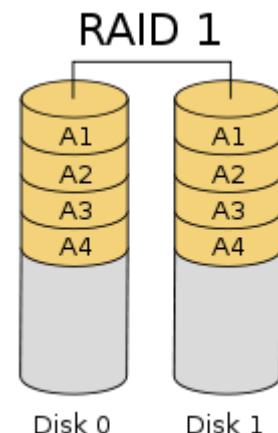
La capacité totale est égale à celle du plus petit élément de la grappe. L'espace excédentaire des autres éléments de la grappe restera inutilisé. Il est donc conseillé d'utiliser des éléments identiques.

- **Fiabilité :**

Cette solution offre un excellent niveau de protection des données. Elle accepte une défaillance de  $n-1$  éléments.

- **Coût :**

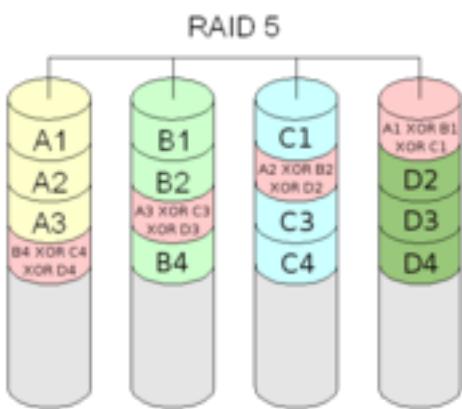
Les coûts de stockage sont élevés et directement proportionnels au nombre de miroirs utilisés alors que la capacité totale reste inchangée. Plus le nombre de miroirs est élevé, et plus la sécurité augmente, mais plus son coût devient prohibitif.



Les accès en lecture du système d'exploitation se font sur le disque le plus facilement accessible à ce moment-là. Les écritures sur la grappe se font de manière simultanée sur tous les disques, de façon à ce que n'importe quel disque soit interchangeable à tout moment. Lors de la défaillance de l'un des disques, le contrôleur RAID désactive, de manière transparente pour l'accès aux données, le disque incriminé. Une fois le disque défectueux

remplacé, le contrôleur RAID reconstitue, soit automatiquement, soit sur intervention manuelle, le miroir. Une fois la synchronisation effectuée, le RAID retrouve son niveau initial de redondance.

### RAID 5 : VOLUME AGREGÉ PAR BANDES A PARITE REPARTIE



Le RAID 5 combine la méthode du volume agrégé par bandes (striping) à une parité répartie. Il s'agit là d'un ensemble à redondance N+1. La parité, qui est incluse avec chaque écriture se retrouve répartie circulairement sur les différents disques. Chaque bande est donc constituée de N blocs de données et d'un bloc de parité. Ainsi, en cas de défaillance de l'un des disques de la grappe, pour chaque bande il manquera soit un bloc de données soit le bloc de parité. Si c'est le bloc de parité, ce n'est pas grave, car aucune donnée ne manque. Si c'est un bloc de données, on peut calculer son contenu à partir des N-1 autres blocs

de données et du bloc de parité. L'intégrité des données de chaque bande est préservée. Donc non seulement la grappe est toujours en état de fonctionner, mais il est de plus possible de reconstruire le disque une fois échangé à partir des données et des informations de partié contenues sur les autres disques.

On voit donc que le RAID 5 ne supporte la perte que d'un seul disque à la fois. Ce qui devient un problème depuis que les disques qui composent une grappe sont de plus en plus gros (1 To et plus). Le temps de reconstruction de la parité en cas de disque défaillant est allongé. Il est généralement de 2 h pour des disques de 300 Go contre une dizaine d'heure pour 1 To. Pour limiter le risque il est courant de dédier un disque dit de *spare*. En régime normal il est inutilisé. En cas de panne d'un disque il prendra automatiquement la place du disque défaillant. Cela nécessite une phase communément appelée "recalcule de parité". Elle consiste pour chaque bande à recréer sur le nouveau disque le bloc manquant (données ou parité).

Bien sûr pendant tout le temps du recalcule de la parité le disque est disponible normalement pour l'ordinateur qui se trouve juste un peu ralenti.

#### Exemple pratique :

Considérons quatre disques durs A, B, C et D, de tailles identiques. Le système va enregistrer les premiers blocs en les répartissant sur les disques A, B et C comme en mode RAID 0 (*striping*) et, sur le disque D, le résultat de l'opération OU exclusif entre les autres disques (ici  $A_1 \oplus B_1 \oplus C_1$ ). Ensuite le système va enregistrer les blocs suivants en les répartissant sur les disques D, A et B, puis la parité (soit  $D \oplus A \oplus B$ ) sur le disque C, et ainsi de suite en faisant permuter circulairement les disques, à chaque bloc. La parité se trouve alors répartie sur tous les disques.

En cas de défaillance d'un disque, les données qui s'y trouvaient pourront être reconstituées par l'opération xor. En effet, l'opération XOR ( $\oplus$ ) à la propriété suivante : si on considère N blocs de taille identique  $A_1, A_2, \dots, A_N$  et si  $A_1 \oplus A_2 \oplus \dots \oplus A_N = X$  alors  $X \oplus A_2 \oplus \dots \oplus A_N = A_1$ , et de façon générale,  $A_1 \oplus \dots \oplus A_{k-1} \oplus X \oplus A_{k+1} \oplus \dots \oplus A_N = A_k$ .

C'est-à-dire que n'importe quel bloc de données  $A_k$  perdu à cause d'un disque défaillant sur un RAID 5 de  $N + 1$  disques peut-être récupéré grâce au bloc X de données de contrôle.

On voit donc que si on veut écrire dans un bloc, il faut lire le bloc à modifier. Lire le bloc de parité de la bande. Écrire le bloc de données et le bloc de parité. L'opération xor permet

heureusement de calculer la nouvelle parité sans avoir besoin de lire les  $N$  blocs de données de la bande. Augmenter le nombre de disque d'une grappe RAID 5 n'allonge donc pas le temps de lecture ou d'écriture. Cependant si plusieurs processus veulent écrire simultanément dans un ou plusieurs blocs de données d'une même bande la mise à jour du bloc de parité devient un point de blocage. Les processus concurrents sont suspendus à la libération du bloc de parité et de fait cela limite le débit d'écriture. Plus le nombre de disque d'une grappe RAID 5 augmente plus le temps de reconstruction d'un disque défaillant augmente. Puisque pour reconstituer le bloc manquant d'une bande il faut lire tous les autres blocs de la bande et donc tous les autres disques.

Ce système nécessite impérativement un minimum de trois disques durs. Ceux-ci doivent généralement être de même taille, mais un grand nombre de cartes RAID modernes autorisent des disques de tailles différentes.

La capacité de stockage utile réelle, pour un système de  $X$  disques de capacité  $c$  identiques est de  $(X - 1) \times c$ . En cas d'utilisation de disques de capacités différentes, le système utilisera dans la formule précédente la capacité minimale.

Ainsi par exemple, trois disques de 100 Go en RAID 5 offrent 200 Go utiles ; dix disques, 900 Go utiles.

Ce système allie sécurité (grâce à la parité) et bonne disponibilité (grâce à la répartition de la parité), même en cas de défaillance d'un des périphériques de stockage.

Il existe une variante : le « RAID 5 orthogonal » où chaque disque a son propre contrôleur. Toutes les autres fonctionnalités sont identiques.

On a souvent tendance à croire qu'un système RAID 5 est totalement fiable. Il est en effet généralement admis que la probabilité de défaillance simultanée de plusieurs disques est extrêmement faible – on parle évidemment d'une défaillance entraînant la perte de données définitive sur plusieurs disques et non d'une simple indisponibilité de plusieurs disques.

Cela est vrai pour une défaillance générale d'une unité de disque. Cependant, cela est faux si l'on considère comme "défaillance" un seul secteur devenu illisible.

En effet, dans la pratique, il est très rare que toutes les données d'un volume soient lues régulièrement. Et quand bien même ce serait le cas, la cohérence de la parité n'est que très rarement vérifiée pour des raisons de performances. Il est donc probable que des défauts tels que des secteurs de parité illisibles ne soient pas détectés pendant une très longue période. Lorsque l'un des disques devient réellement défectueux, la reconstruction nécessite de parcourir l'intégralité des disques restants. On peut alors découvrir des défauts qui étaient restés invisibles jusque-là.

Tout ceci pourrait ne pas être bien grave et occasionner la perte d'une quantité de données minime (un secteur de disque), cependant, l'extrême majorité des contrôleurs RAID est incapable de gérer les défaillances partielles : ils considèrent généralement qu'un disque contenant un secteur illisible est totalement défaillant. À ce moment-là, 2 disques sont considérés défaillants simultanément et le volume RAID 5 devient inutilisable. Il devient extrêmement difficile de récupérer les données, et extrêmement coûteux.

Un système RAID 5 doit donc être vérifié et sauvegardé très périodiquement pour s'assurer que l'on ne risque pas de tomber sur ce genre de cas. D'autre part, en cas de défaillance, il est nécessaire de disposer de matériel très coûteux pour espérer récupérer les données, ce qui rend le RAID 5 très peu recommandable aux particuliers et aux petites entreprises.

Avantage :

- Performances en lecture aussi élevées qu'en RAID 0 et sécurité accrue
- Surcoût minimal (capacité totale de  $n - 1$  disques sur un total de  $n$  disques)

Inconvénients :

- Pénalité en écriture du fait du calcul de la parité
- Minimum de 3 disques

- En cas de défaillance, les coûts de récupération des données sont assez élevés

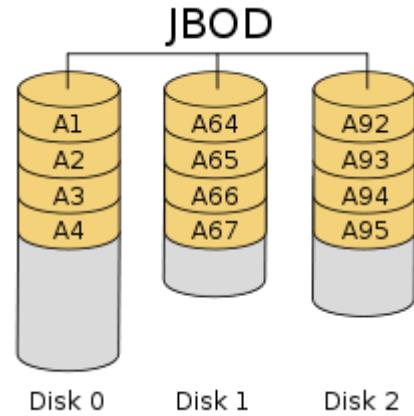
## LES NIVEAUX DE RAID PEU COURANTS

### NRAID (OU JBOD - JUST A BUNCH OF DISKS) : CONCATÉNATION DE DISQUES

*NRAID : Near/Non Redundant Array of Inexpensive/Independent Disk*

La concaténation de disques consiste à additionner les capacités de plusieurs disques durs en un volume logique d'une taille équivalente à la somme des tailles des disques durs. Cette méthode utilise une méthode d'écriture séquentielle : les données ne sont écrites sur le disque dur suivant que lorsqu'il ne reste plus de place sur le précédent.

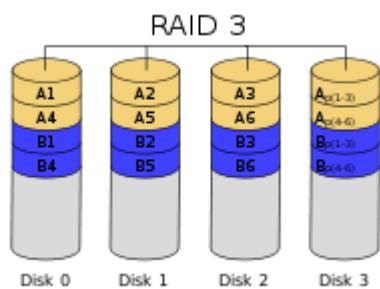
Le NRAID n'est pas à proprement parler un RAID, et il ne permet d'ailleurs aucune redondance de données, mais il offre cependant une tolérance aux pannes supérieure au RAID 0. On le rencontre souvent sous le nom de JBOD (*Just a Bunch Of Disks*).



### RAID 2 : VOLUME AGREGÉ PAR BANDES A PARITE

Le RAID 2 est aujourd'hui obsolète. Il combine la méthode du volume agrégé par bande à l'écriture d'un code de contrôle d'erreur par code de Hamming (code ECC) sur un disque dur distinct. Cette technologie offre un bon niveau de sécurité, mais de mauvaises performances.

### RAID 3 ET RAID 4



Le RAID3 et le RAID4 sont sensiblement semblables sauf que le premier travaille par octets et le second par blocs. Le RAID4 ne nécessite pas autant de synchronisme entre les disques. Le RAID3 tend donc à disparaître au profit du RAID4 qui offre des performances nettement supérieures. Ces niveaux de RAID nécessitent une matrice de  $n$  disques (avec  $n \geq 3$ ). Les  $n - 1$  premiers disques contiennent les données tandis que le dernier disque stocke la parité.

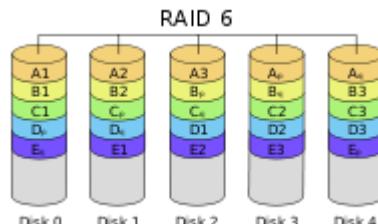
- Si le disque de parité tombe en panne, il est possible de reconstruire l'information de parité avec le contenu des autres disques de données.
- Si l'un des disques de données tombe en panne, il est possible de reconstruire l'information avec le contenu des disques de données restants et celui du disque de parité.

Il est important que le disque de parité soit de bonne qualité car il est à tout instant sollicité à l'écriture. Ce dernier point est une des limitations du RAID 3.

De même, si plus d'un disque vient à défaillir, il est impossible de remédier à la perte de données.

### RAID 6

Le RAID 6 est une évolution du RAID 5 qui accroît la sécurité en utilisant  $n$  informations redondantes au lieu d'une. Il peut donc résister à la défaillance de  $n$  disques. Les fondements mathématiques utilisés pour les



informations de redondance du RAID 6 sont beaucoup plus complexes que pour le RAID 5 ; les implémentations de l'algorithme se limitent souvent à  $n = 2$  (soit la perte de 2 disques) de ce fait.

Des explications intéressantes mais un peu ardues sont disponibles dans la version anglaise de cet article<sup>5</sup> ainsi que dans *Les mathématiques du RAID 6*.

Si la sécurité est plus grande, le coût en matériel est plus élevé et la vitesse est moindre. La puissance CPU nécessaire pour calculer les redondances et surtout pour reconstruire un volume défectueux est également nettement plus importante.

Les défauts majeurs sont :

- Les temps d'écriture sont longs à cause des calculs de redondance complexes.
- Le temps de reconstruction en cas de défaillance simultanée de 2 disques est extrêmement long.

Le RAID 6 était peu utilisé du fait de son surcoût. La récente envolée des capacités des disques ainsi que la vulgarisation de solution professionnelle à base de disque SATA a montré un intérêt nouveau dans l'utilisation du RAID 6, que ce soit par le biais de contrôleur Raid Hardware ou via du raid logiciel (Linux-2.6 intègre le RAID 6).

La capacité utile totale ( $C_{Ut}$ ), pour un système avec  $k$  disques dont  $n$  réservés pour la redondance est de  $C_{Ut} = (k - n) \times c$ . ( $c$  = capacité du plus petit des disques dur).

## LES NIVEAUX DE RAID COMBINES

Fondamentalement, un niveau de RAID combiné est l'utilisation d'un concept de RAID classique sur des éléments constitutifs qui sont eux-mêmes le résultat d'un concept RAID classique. Le concept utilisé peut être le même ou différent.

La syntaxe est encore un peu floue mais on peut généralement considérer que le premier chiffre indique le niveau de raid des "grappes" et que le second indique le niveau de raid global. Dans l'absolu rien n'empêche d'imaginer des RAID combinés à 3 étages ou plus mais cela reste pour l'instant plus du domaine de la théorie et de l'expérimentation.

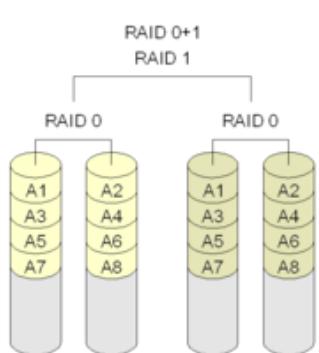
Le nombre important (et croissant) de permutations possibles fait qu'il existe une multitude de raid combinés et nous n'en ferons pas l'inventaire. Nous pouvons cependant présenter les avantages et les faiblesses des plus courants.

Pour les calculs suivants, on utilise les variables suivantes :

- $G$  : nombre de grappes ;
- $N$  : nombre de disques ;
- $C$  : capacité d'un disque (tous les disques sont supposés identiques) ;
- $V$  : vitesse d'un disque.

Les seuils de mise en défaut indiqués ci-dessous indiquent le nombre minimal de disques en panne pouvant entraîner une mise en défaut de l'ensemble du RAID (i.e. en dessous de ce nombre de disques en panne le RAID ne peut pas être en défaut). En pratique il est possible qu'un RAID ayant plus que ce nombre de disques en panne fonctionne toujours mais il est recommandé de changer les disques défectueux le plus rapidement possible.

### LE RAID 01 (OU RAID 0+1)



Il permet d'obtenir du *mirroring* rapide puisqu'il est basé sur des grappes en striping. Chaque grappe contenant au minimum 2 éléments, et un minimum de 2 grappes étant nécessaire, il faut au minimum 4 unités de stockage pour créer un volume RAID0+1.

La fiabilité est moyenne car un disque défectueux entraîne le défaut de toute la grappe qui le contient. Par ailleurs, cela

allonge beaucoup le temps de reconstruction et dégrade les performances pendant la reconstruction. L'intérêt principal est que dans le cas d'un miroir à 3 grappes ou plus, le retrait volontaire d'une grappe entière permet d'avoir une sauvegarde "instantanée" sans perdre la redondance.

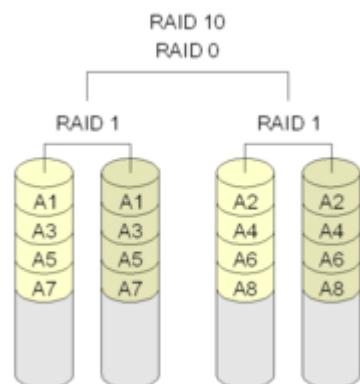
- Capacité totale :  $C_t = G \times C$
- Vitesse maximale :  $V_m = G \times V$
- Seuil de mise en défaut :  $N$  disques

### LE RAID 10 (OU RAID 1+0)

Il permet d'obtenir un volume agrégé par bande fiable (puisque'il est basé sur des grappes répliquées). Chaque grappe contenant au minimum 2 éléments et un minimum de 2 grappes étant nécessaire, il faut au minimum 4 unités de stockage pour créer un volume RAID10.

Sa fiabilité est assez grande puisqu'il faut que tous les éléments d'une grappe soient défectueux pour entraîner un défaut global. La reconstruction est assez performante puisqu'elle ne mobilise que les disques d'une seule grappe et non la totalité.

- Capacité totale :  $C_t = G \times C$
- Vitesse maximale :  $V_m = G \times V$
- Seuil de mise en défaut :  $G$  disques



### LE RAID 05

Même principe que pour le raid 0+1 mais en employant du RAID5 pour la partie globale. Chaque grappe contenant au minimum 2 disques, et un minimum de 3 grappes étant nécessaire, il faut au minimum 6 unités de stockage pour créer un volume RAID05. Ce mode ne présente pas d'intérêt majeur par rapport à un RAID5 classique à  $N * G$  disques. Il est donc très peu utilisé.

- Capacité totale :  $C_t = (N - 1) \times (G \times C)$
- Vitesse maximale :  $V_m = (N - 1) \times (G \times V)$  (cette formule néglige les temps de calcul de parité)
- Seuil de mise en défaut : 2 disques

### LE RAID 15

Il permet d'obtenir un volume agrégé par bandes avec redondance répartie très fiable (puisque'il est basé sur des grappes répliquées en miroir). Chaque grappe contenant au minimum 2 disques, et un minimum de 3 grappes étant nécessaire, il faut au minimum 6 unités de stockage pour créer un volume RAID15. Ce mode est très fiable puisqu'il faut que tous les disques de 2 grappes différentes cessent de fonctionner pour le mettre en défaut. Ce mode est cependant coûteux par rapport à la capacité obtenue.

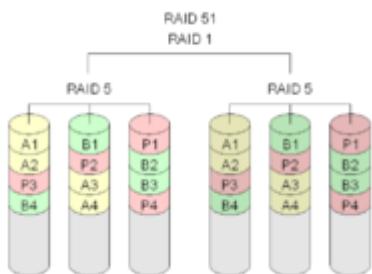
### LE RAID 50

Il permet d'obtenir un volume agrégé par bandes basé sur du RAID 5 + 0. Chaque grappe contenant au minimum 3 disques, et un minimum de 2 grappes étant nécessaire, il faut au minimum 6 unités de stockage pour créer un volume RAID 50. Un des meilleurs compromis lorsque l'on cherche la rapidité sans pour autant vouloir trop dégrader la fiabilité. En effet,

l'agrégat par bande (fragile) repose sur des grappes redondantes. Il suffit cependant que 2 disques d'une même grappe tombent en panne pour le mettre en défaut.

- Capacité totale :  $C_t = N \times (G - 1) \times C$
- Vitesse maximale :  $V_m = N \times (G - 1) \times V$  (cette formule néglige les temps de calcul de parité)
- Seuil de mise en défaut : 2 disques

### LE RAID 51



Il permet d'obtenir un volume répliqué basé sur des grappes en RAID5. Chaque grappe contenant au minimum 3 disques, et un minimum de 2 grappes étant nécessaire, il faut au minimum 6 unités de stockage pour créer un volume RAID51. C'est un mode coûteux (faible capacité au regard du nombre de disques).

- Capacité totale :  $C_t = (G - 1) \times C$
- Vitesse maximale en

écriture :  $V_Mw = (G - 1) \times V$  (cette formule néglige les temps de calcul de parité)

- Vitesse maximale en lecture :  $V_Mr = N \times (G - 1) \times V$  (cette formule théorique suppose une optimisation maximale qui n'est jamais atteinte)
- Seuil de mise en défaut :  $2 \times (N - 1)$  disques

## DOMAIN NAME SERVER (DNS)

### HISTORIQUE DU SYSTEME DE NOMS DE DOMAINE

Durant les années 70 ARPAnet est demeurée une petite communauté de quelques centaines d'hôtes. La table de correspondances entre Hôtes et adresses était entretenue par le "Network Information Consortium" ( NIC ) au "Stanford Research Institute" ( SRI ) dans un fichier unique HOSTS.TXT. Ce fichier n'était téléchargeable qu'à partir d'une machine unique SRI-NIC. Les administrateurs ARPANET envoient leurs modifications par e-mail au NIC, et récupèrent périodiquement le dernier HOSTS.TXT par connexion ftp au SRI-NIC. Les mises à jour du fichier HOSTS.TXT se font à la cadence de l'ordre de une à deux fois par semaine. La taille de HOSTS.TXT a augmenté proportionnellement à l'arrivée de nouveaux hôtes sur le réseau, et le trafic généré, s'est envolé, un nouvel hôte entraînant non seulement, une nouvelle entrée dans HOSTS.TXT, mais également une nouvelle diffusion potentielle par SRI-NIC.

Lors de l'évolution du réseau ARPAnet vers l'utilisation de TCP/IP développé par l'université de Berkeley, la taille des hôtes connectés a explosé, engendrant ainsi une série de problèmes dans l'utilisation de HOSTS.TXT.

### LE TRAFIC ET LA CHARGE

Le coût en termes de charge du réseau et du processeur, est devenu bien trop élevé.

### LES CONFLITS DE NOMS

Dans HOSTS.TXT deux hôtes ne pouvaient avoir le même nom. Même si le NIC garantissait l'unicité de l'attribution des adresses IP. Il ne pouvait en revanche empêcher quelqu'un d'utiliser un nom d'hôte déjà présent sur le réseau. Ainsi si un nouvel hôte apparaissait sur le réseau avec par exemple un nom déjà utilisé par un serveur de messagerie, ceci engendrait une interruption du service dans la zone concernée.

### COHERENCE

La gestion d'un fichier HOSTS.TXT statique dans un réseau en pleine expansion est devenue quasiment impossible. Le temps mis par le fichier HOSTS.TXT pour atteindre les hôtes en périphérie du réseau ne garantissait pas son exactitude. En effet, entre temps un nouvel hôte a pu, soit faire son apparition, soit avoir changé son adresse, ou encore avoir disparu du réseau.

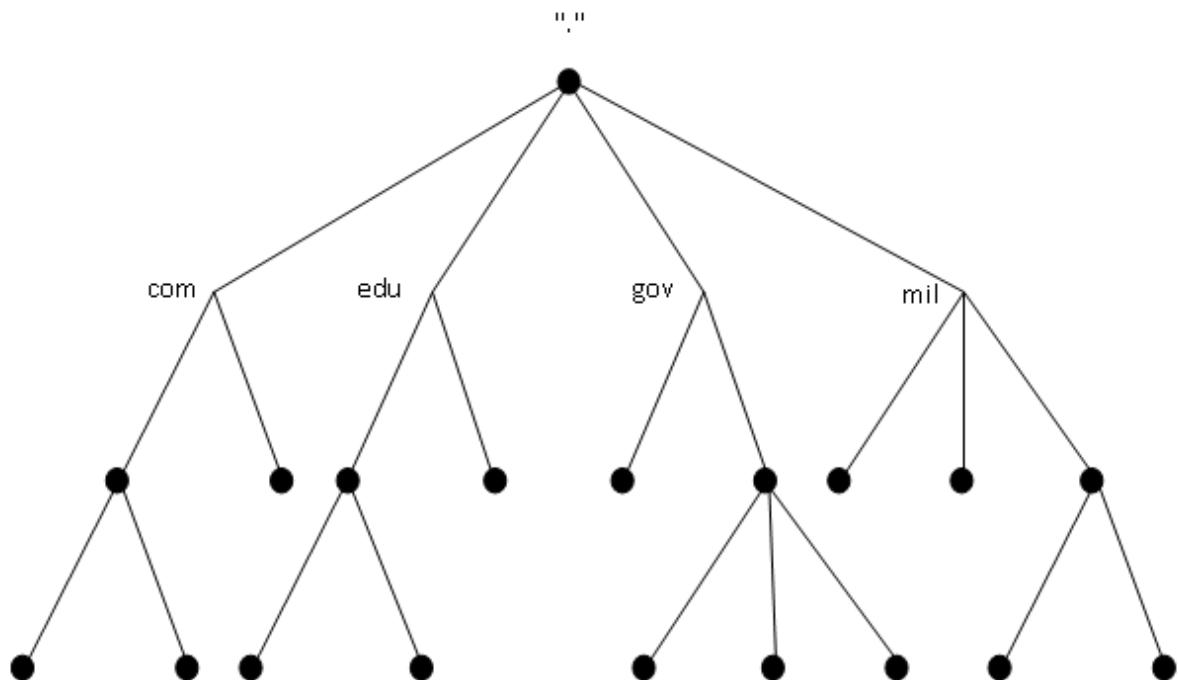
Une réflexion a alors été lancée par les autorités de ARPAnet avec les points de réflexion suivants :

- Trouver un système permettant de résoudre les problèmes engendrés par l'utilisation d'un système central de descriptions d'hôtes
  - Données gérées localement, mais accessibles globalement
  - Décentralisation de la gestion pour éliminer le goulet d'étranglement sur SRI-NIC
  - Gestion locale permettant ainsi d'avoir des informations plus facilement mises à jour.
  - Espace de nom hiérarchique garantissant l'unicité des noms.

La conception hiérarchique du nouveau système fut alors confiée à PAUL MOCKAPETRIS en 1983, alors en poste à l' Information Science Institute de l' USC.

En 1984, il produisit les RFC 882 et 883 qui décrivaient le système de nom de domaine. Ces deux RFC furent ultérieurement remplacées par les RFC 1034 et 1035 toujours d'actualité. Les RFC 1034 et 1035, sont aujourd'hui complétées par d'autres RFC traitant de mise en œuvre, de gestion de sécurisation et de mises à jours automatiques des serveurs de noms.

## LE SYSTEME DE NOMS DE DOMAINE



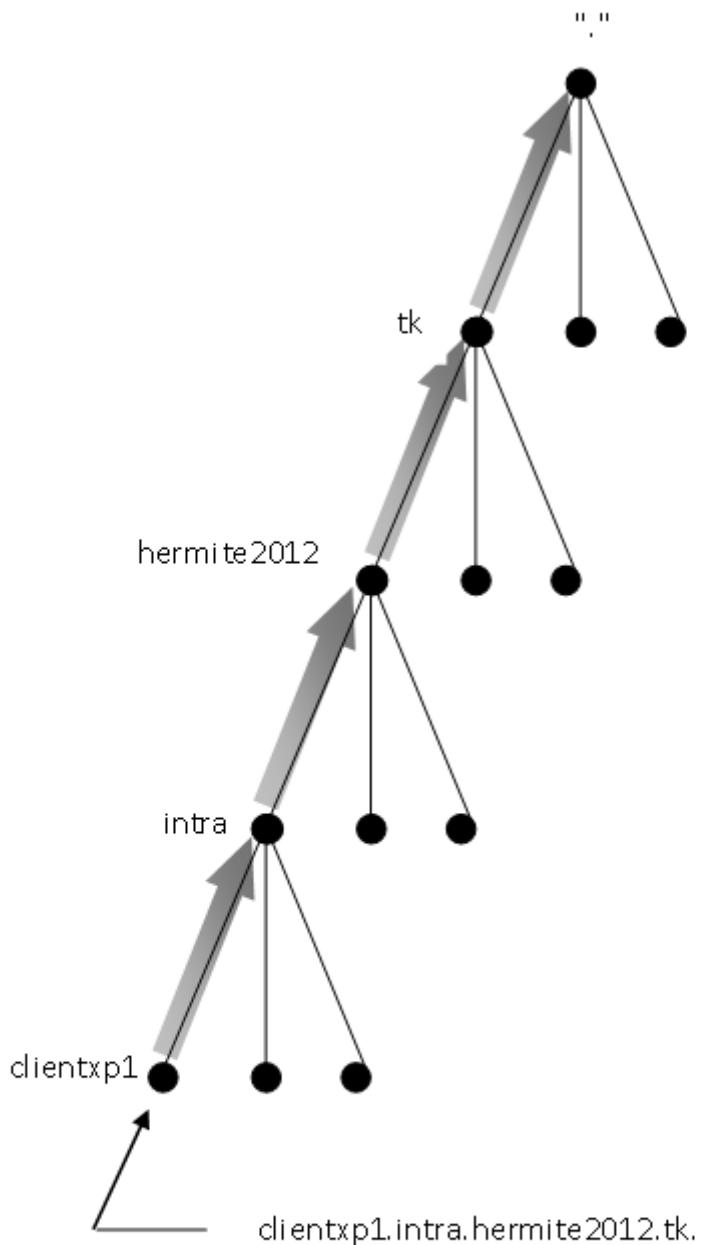
Base de données du DNS

Le système de noms de domaine est une base de données distribuée, ceci permet un contrôle local de la base de données globale, les données de chaque segment étant accessibles de partout par un mécanisme client-serveur. Des duplications et des mémoires caches règlent les problèmes de robustesse et de performance.

La base de données du DNS est représentée comme un arbre inversé, avec le nœud racine en haut, un nom unique identifie chaque nœud de l'arbre relativement à son nœud parent. Le nœud racine est représenté par un point unique ( ". " ).

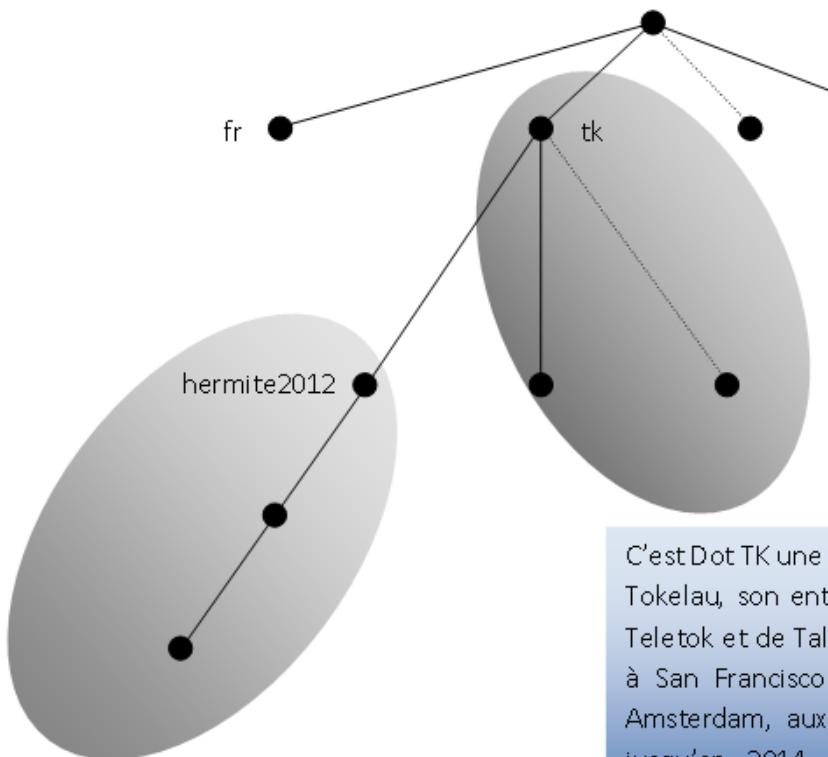
Chaque nœud est aussi la racine d'un nouveau sous arbre de l'arbre global. Chaque sous arbre, représente une partie de la base de données globale. Chaque domaine peut être divisé en sous-domaines. Les sous domaines sont représentés comme des enfants de leur domaine parent.

Chaque domaine possède un nom unique, et indique sa position dans la base de données. Le nom de est la réunion de tous les noms de nœud séparés par un " . " en partant de la feuille jusqu'à la racine de l'arbre inversé.



Base de données du DNS

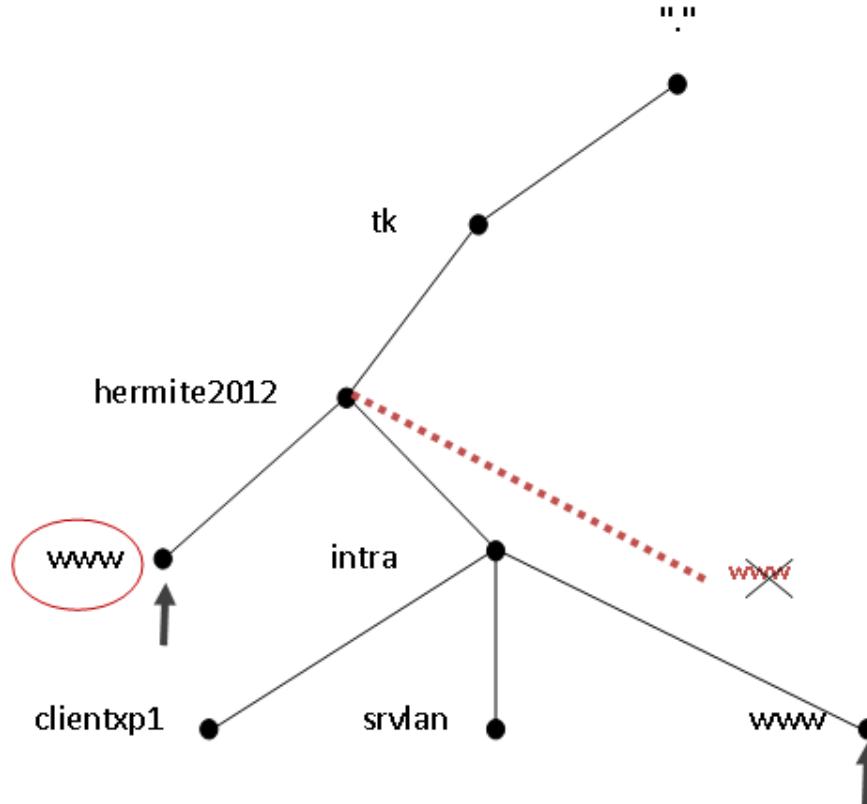
Dans le DNS chaque domaine peut être géré par un organisme différent, chaque organisme peut scinder son domaine en sous-domaines, et distribuer la responsabilité des sous domaines à d'autres organismes



C'est VANLERBERGHE Nicolas un stagiaire de TSRIT à l' AFPA de DUNKERQUE qui gère le hermite2012.tk. Dans le cadre de son miniprojet de fin d'apprentissage on lui a demandé de présenter DNS, il a donc enregistré son domaine gratuitement auprès de DOT.tk. Et a demandé la délégation de la gestion de son domaine en indiquant à DOT.TK l'adresse IP et le nom des serveurs DNS de sa zone.

C'est Dot TK une filiale du gouvernement de Tokelau, son entreprise de communication Teletok et de Taloha Inc, une société basée à San Francisco (USA) avec une filiale à Amsterdam, aux Pays-Bas qui gère le .TK jusqu'en 2014. Il distribue actuellement gratuitement les noms de domaine en .TK.

Un domaine peut contenir simultanément des hôtes, des sous domaines, des alias pointant vers des noms canoniques.



Dans l'exemple ci-dessus:

- "intra" est un sous domaine de hemite2012.tk.
- "www.intra" est un alias pointant vers "srvlan.intra"
- clientxp1 et srvlan sont des noms d'hôtes.

Illustration en rouge :

Nous voyons que nous ne pouvons pas avoir deux nœuds possédant le même nom au même niveau, par analogie aux fichiers et dossier d'un système d'exploitation, nous ne pouvons pas avoir deux fichiers portant le même nom au sein d'un même dossier.

Par contre rien n'empêche au sein d'un domaine à partir du moment où les enregistrements de se situent pas au même niveau de l'arborescence, d'avoir deux fois un même nom :

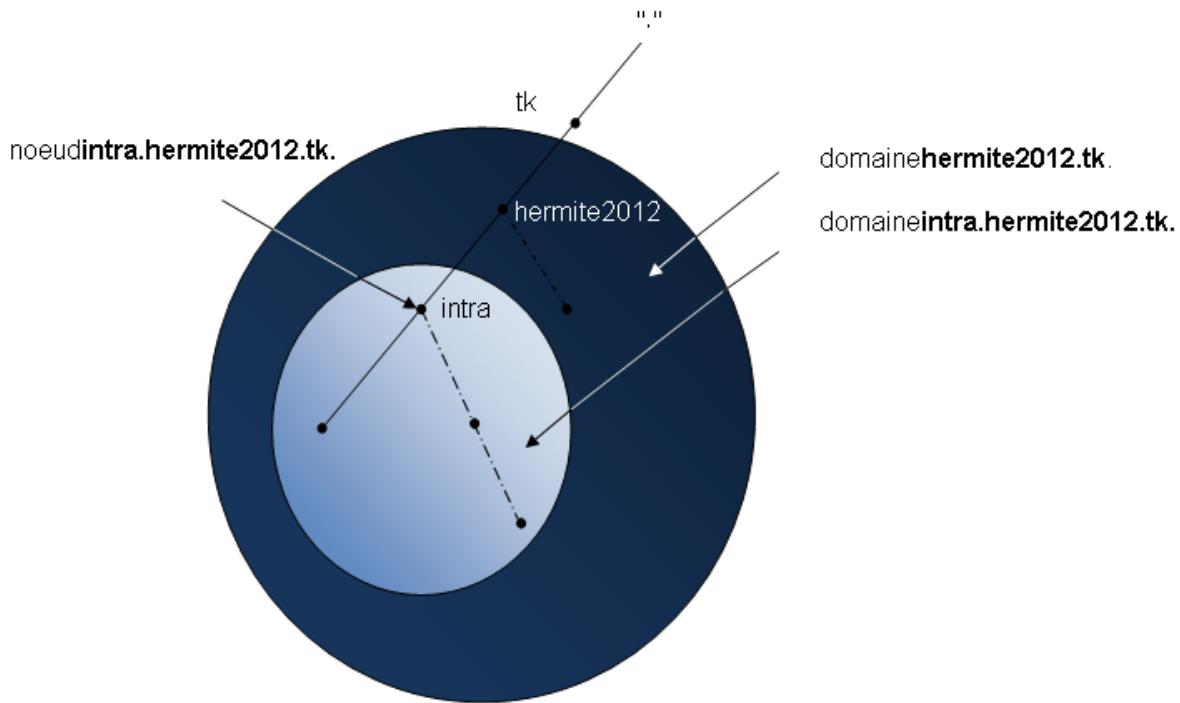
- www.hermite2012.tk.
- www.intra.hermite2012.tk.

## PRINCIPE DE DNS

---

## DOMAINES

---

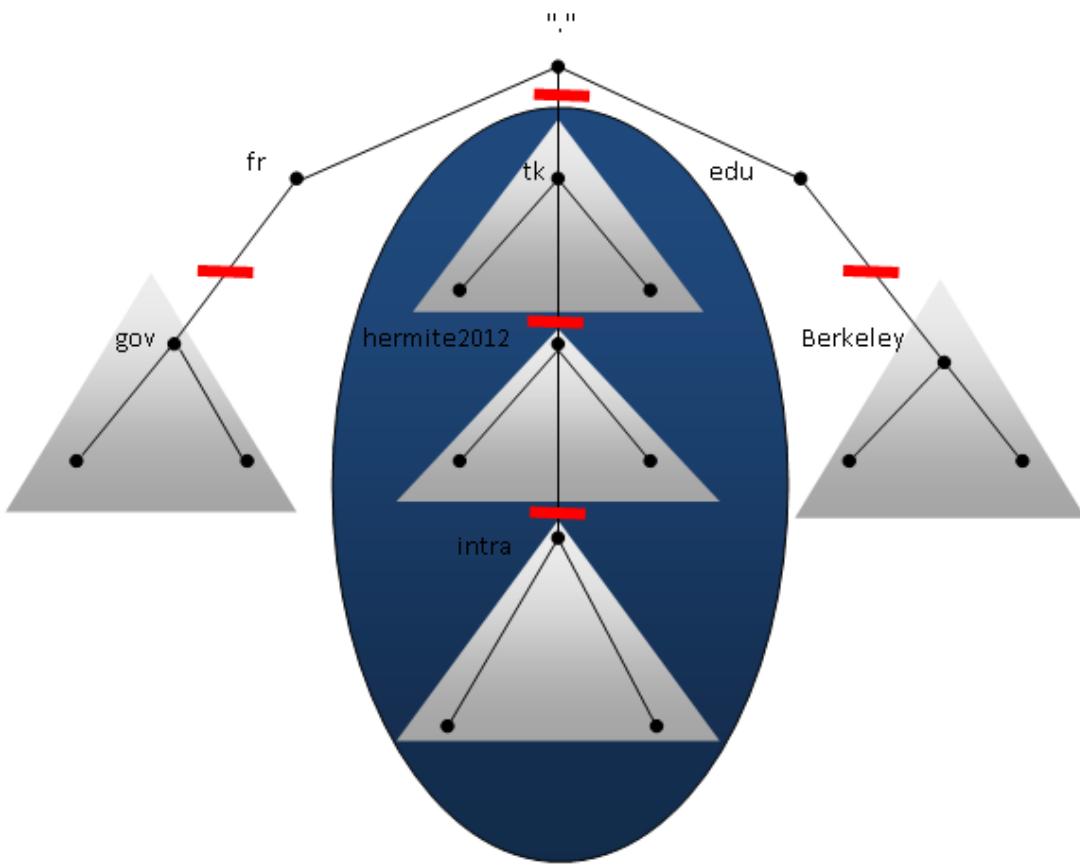


Un domaine est tout simplement un sous arbre de l'espace de nommage, le nom d'un domaine est le nom du noeud se situant au sommet de l'arbre. Ainsi le sommet du domaine hermite2012.tk. est le noeudhermite2012.tk.

Tout nom du sous arbre est considéré comme faisant partie du domaine, ainsi le nom intra.hermite2012.tk. fait partie du domaine hermite2012.tk et fait également partie intégrante du domaine .tk.

Dans la figure ci-dessus nous pouvons différencier les domaines par leur niveau, " tk " est un domaine de premier niveau " Top Level Domain " car enfant direct de la racine " . ", et hermite2012 est un domaine de second niveau car enfant du domaine " tk ".

## DELEGATION D'AUTORITE ET DE ZONES



La distinction entre domaines et zones est pour le moins subtile et mérite que l'on s'y attarde un instant. Les domaines de niveau supérieur ainsi que de nombreux domaines de niveau inférieur sont divisés en unités plus petites et plus faciles à gérer par délégation d'autorité. On voit dans la figure ci-dessus que le domaine ".tk" scindé en zones :

- La zone ".tk"
- La zone "hermite2012.tk", elle-même subdivisée avec la zone "intra.hermite2012.tk"

Il est normal que ce soit aux administrateurs de "hermite2012.tk" de gérer leur propre base de donnée et non à ceux de la zone ".tk." de le faire.

La base de données de la zone ".tk." contiendra essentiellement les informations de délégations des zones de niveau inférieur.

Exemple :

- la zone ".tk" contiendra les noms et adresses des serveurs de noms de la zone "hermite2012.tk"
  - la zone "hermite2012.tk" contiendra les informations concernant les serveurs de noms de sa zone, les informations de délégation pour la zone "intra.hermite2012.tk.", les correspondances noms, adresses, services mail, pour sa propre zone...

- la zone "intra.hermite2012.tk" quant à elle contiendra une base de données des hôtes de son réseau local et les directives indiquant à qui retransmettre les requêtes ne concernant pas la zone dont elle a autorité...

## SERVEURS DE NOMS DE LA RACINE

Les serveurs de noms de la racine savent où se trouvent les serveurs de noms de chaque domaine de niveau supérieur (la plupart des serveurs de noms de la racine ont autorité sur les domaines de niveau supérieur). Lorsqu'ils répondent à une requête quelconque les serveurs de la racine renvoient au minimum des informations concernant les serveurs de noms du domaine inférieur, qu'il faudra alors contacter pour poursuivre la résolution de noms.

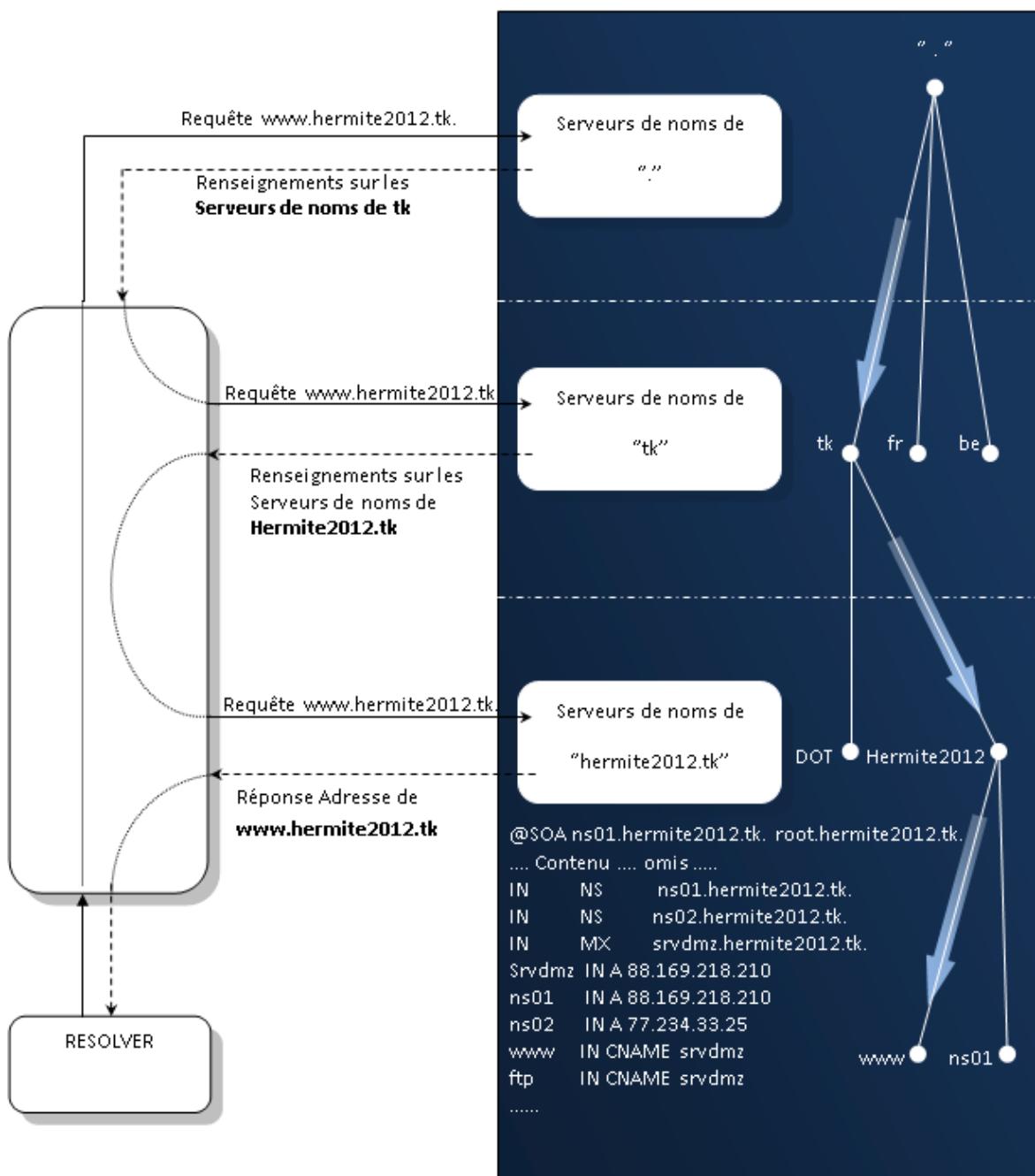
En absence d'informations supplémentaires, un serveur DNS local qui effectuera une recherche pour un résolveur, interrogera en premier lieu les serveurs de la racine. En effet, chaque serveur de noms a connaissance des adresses des serveurs de noms de la racine. S'il arrivait que tous les serveurs de la racine deviennent indisponibles pendant un grand laps de temps, plus aucune requête n'aboutirait et toute communication serait alors interrompue. Les serveurs de noms de la racine occupent une position centrale dans l'architecture d'internet, ils peuvent recevoir plusieurs milliers de requêtes à la seconde, on voit par là qu'ils sont soumis à un trafic très dense.

La position stratégique centrale des serveurs de noms de la racine, les expose à des attaques organisées visant à les inonder de requêtes simultanées afin de les faire tomber en déni de service.

Une attaque est survenue en 2002 sur les serveurs ROOT, 7 sur les 13 serveurs sont devenus inopérants après une attaque massive en deni de service. Une technique de duplication de serveurs a été mise en place. Le serveur logique F possède 46 répliques toutes accessibles à la même adresse IP grâce à une technique de routage dite anycast, c'est le réseau qui se chargera de router au mieux les demandes de résolutions vers le serveur le plus approprié. Certains [serveurs DNS racine](#) sont en fait de grosses [grappes de serveurs](#) utilisant anycast.

Les serveurs C, F, I, J, K et M sont éparpillés sur plusieurs continents et utilisent anycast pour fournir un service décentralisé. Du coup, la plupart des serveurs racine physiques sont en dehors des États-Unis. La [RFC 3258](#) décrit comment anycast est utilisé pour fournir un service DNS. Plusieurs [ccTLD](#) utilisent également cette technique, comme le [.fr](#) [\[1\]](#). Cette technique est aussi utilisée sur le registre suisse qui gère le nom de domaine de premier niveau .

## LA RESOLUTION DE NOMS



Processus de résolution de l'adresse **www.hermite2012.tk**.

```
Administrator : C:\Windows\system32\cmd.exe

C:\Users\tsrit>nslookup www.hermite2012.tk. a.root-servers.net
198.in-addr.arpa    nameserver = D.ILL.ARIN.NET
198.in-addr.arpa    nameserver = U.ARIN.NET
198.in-addr.arpa    nameserver = U.ARIN.NET
198.in-addr.arpa    nameserver = T.ARIN.NET
198.in-addr.arpa    nameserver = Y.ARIN.NET
198.in-addr.arpa    nameserver = Z.ARIN.NET
198.in-addr.arpa    nameserver = X.ARIN.NET
198.in-addr.arpa    nameserver = W.ARIN.NET
Serveur : Unknown
Address: 198.41.0.4

Nom : www.hermite2012.tk
Served by:
- root-c.taloha.tk
  207.36.228.217
  tk
- root-g.taloha.tk
  217.68.243.17
  tk
- root-f.taloha.tk
  202.125.44.173
  tk
- root-d.taloha.tk
  217.199.176.121
  tk
- root-b.taloha.tk
  85.214.136.249
  tk
- root-a.taloha.tk
  194.109.152.138
  tk
- root-e.taloha.tk
  66.36.231.236
  tk

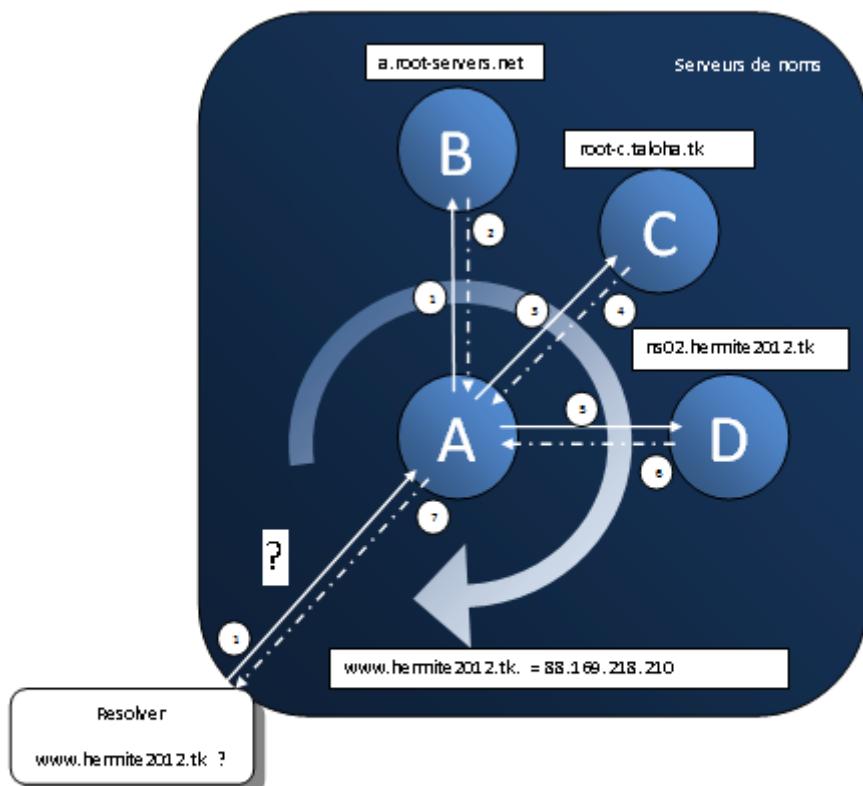
C:\Users\tsrit>nslookup www.hermite2012.tk. root-c.taloha.tk
Serveur : Unknown
Address: 207.36.228.217

Nom : www.hermite2012.tk
Served by:
- NS01.hermite2012.tk
  88.169.218.210
  hermite2012.tk
- NS02.hermite2012.tk
  78.234.33.25
  hermite2012.tk

C:\Users\tsrit>nslookup www.hermite2012.tk. ns01.hermite2012.tk.
Serveur : ns01.hermite210.tk
Address: 88.169.218.210
Aliases: www.hermite2012.tk

C:\Users\tsrit>
```

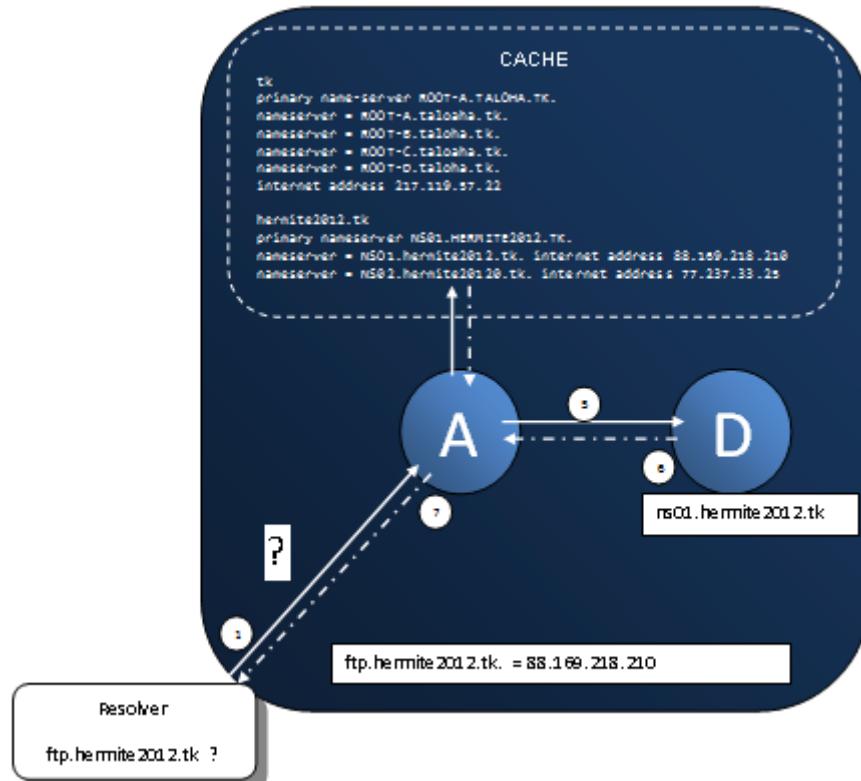
Résolution itérative manuelle de www.hermite2012.tk.



Processus de résolution sans cache

## LES SERVEURS CACHE

La plupart des serveurs DNS jouent également le rôle de serveur cache, le serveur apprend beaucoup de ses précédentes requêtes. A chaque fois qu'il se réfère à une nouvelle zone il apprend quels serveurs en ont autorité. Le serveur placera donc dans son cache toutes ses précieuses informations qui lui serviront probablement pour une requête ultérieure.



Lors de sa précédente recherche le serveur DNS A a appris, non seulement l'adresse correspondant à www.hermite2012.tk., mais également de nombreuses autres informations précieuses :

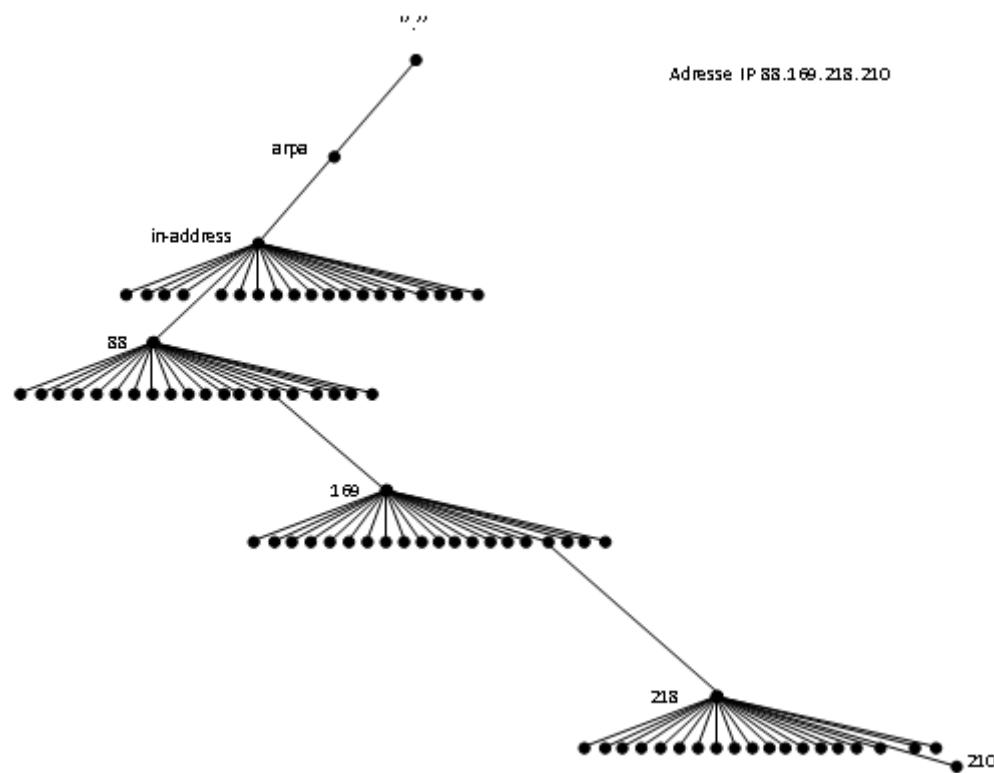
La liste des serveurs ayant autorité sur la zone tk, et également la liste des serveurs de noms ayant autorité sur la zone hermite2012.tk.

Sachant que sa recherche porte sur la zone hermite2012.tk, il va directement aller interroger l'un des serveurs ayant autorité sur la zone, sa résolution de noms se voit ainsi considérablement raccourcie.

---

## LA RESOLUTION INVERSE

---



Machine : ns01.hermite2012.tk.

Domain : 210.218.169.88.in-address.arpa.

Etant donné qu'il est ais  de retrouver une adresse lorsque l'on dispose du nom, une section de l'espace de nommage a  t  cr e , cette zone utilise les adresses comme des noms.

Dans la figure ci-dessus, nous voyons une adresse IP de 32 de bits repr sent e par 4 nombres en d cimal point , allant de 0   255 s par s par des points.

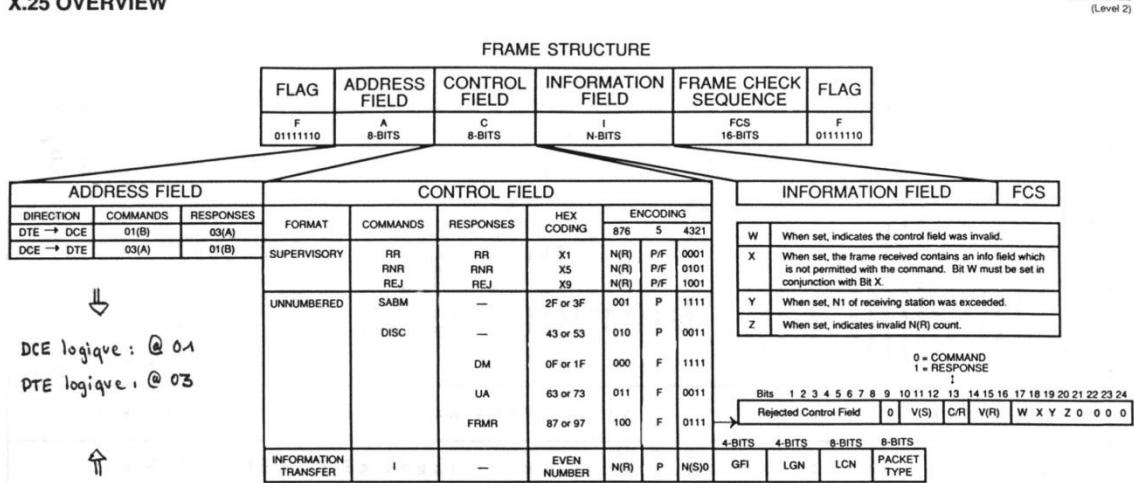
Le domaine in-address .arpa. par exemple, peut contenir 256 sous domaines correspondants   la valeur que peut prendre le premier octet d'une adresse IP. Chacun de ses sous domaines peuvent eux m me contenir 256 sous domaines correspondantes aux valeurs de leurs octets respectifs, et ce, jusqu'au 4eme niveau o  l'enregistrement de ressource attach    cette valeur fait correspondre le nom complet de l' h te

Ex : 210.218.169.88.in-addr.aprpa. PTR ns01.hermite2012.tk.

Au final le domaine in-address.arpa. est suffisamment spacieux pour contenir toutes les adresses IPV4 existantes(soit  $254^4 = 41 \quad 623\ 142\ 565$  adresses.....)

## HDLC ET X25 (OVERVIEW)

### X.25 OVERVIEW



CALL REQUEST	4-BITS	4-BITS	VARIABLE LENGTHS	8-BITS	109 BYTE MAX	16-BYTES MAX
	0B	CALLING ADDR. LGH.	CALLED ADDR.	CALLING ADDR.	FACILITIES 00	FACILITIES 4
CALL ACCEPT	0F	CALLING ADDR. LGH.	CALLED ADDR.	CALLING ADDR.	FACILITIES 00	FACILITIES 4
DATA	876 5 432 1	P(R) M P(S) 0 DATA (UP TO 4096 BYTES)	8-BITS	8-BITS		
RESET REQUEST	1B	RESET CAUSE	DIAGNOSTIC CODE			
RESTART REQUEST	FB	RESTART CAUSE	DIAGNOSTIC CODE			
CLEAR REQUEST	13	CLEARING CAUSE	DIAGNOSTIC CODE			
DIAGNOSTIC	F1	DIAGNOSTIC CODE	DIAGNOSTIC EXPLANATION UP TO 3 OCTETS			
INTERRUPT	23	USER DATA FIELD UP TO 32 OCTETS				
RECEIVE READY	P(R) 00001					
RECEIVE NOT READY	P(R) 00101					
REJECT	P(R) 01001					
INTERRUPT CONFIRMATION	27					
CLEAR CONFIRMATION	17					
RESTART CONFIRMATION	FF					
RESET CONFIRMATION	1F					
REGISTRATION REQUEST	F3	DTE ADDR. LGH.	DCE ADDR. LGH.	CALLED ADDR.	REGISTRATION 0	REGISTRATION FIELD UP TO 109 OCTETS
REGISTRATION CONFIRMATION	F7	8-BITS CAUSE	8-BITS DIAGNOSTIC	DTE ADDR. LGH.	DCE ADDR. LGH.	REGISTRATION 0 REGISTRATION FIELD UP TO 109 OCTETS

PROTOCOL IDENTIFIER TABLE	
BITS 8 7	RECOMMENDED USE
0 0	For CCITT use
0 1	For national use
1 0	Reserved for international users
1 1	For DTE — DTE use

GFI (General Format Identifier)	
BIT 8	0 BIT (Data Qualifier) DATA PKTS ONLY
Q=0:	DATA PACKET contains user data
Q=1:	DATA PACKET contains control data
BIT 7	D BIT (Delivery Confirmation)
D=0:	End to End ACK not required
D=1:	End to End ACK required
BIT 6	When set, P(S) and P(R) counters in the DATA packets are modulo 128
BIT 5	When set, P(S) and P(R) counters in the DATA packets are modulo 8

CLEARING CAUSE TABLE	
HEX VALUE	REASON
00	DTE Originated
8F — FF	DTE Originated
01	Number Busy
03	Invalid Facility Request
05	Network Congestion
09	Out of Order
0B	Access Barred
0D	Not Obtainable
11	Remote Procedure Error
13	Local Procedure Error
15	RPOA Out of Order
19	Collect Call Refused
21	Incompatible Destination
29	Fast Select Not Subscribed

Numéro interne

RESTART CAUSE TABLE	
HEX VALUE	REASON
00	Local Procedure Error
03	Network Congestion
07	Network Operational
7F	Registration/Cancellation Confirmed

FACILITY CODE CLASSES			
CLASS	FACILITY CODE ONE OCTET	PARAM LENGTH	PARAMETER FIELD
A	00 — 3F	—	1 OCTET
B	40 — 7F	—	2 OCTETS
C	80 — BF	—	3 OCTET
D	C0 — FF	1 OCTET	More than 3 OCTETS

RESET CAUSE TABLE	
HEX VALUE	REASON
00	DTE Originated
8F — FF	DTE Originated
1D	Network Out of Order (PVC)
01	Out of Order (PVC)
03	Remote Procedure Error
05	Local Procedure Error
07	Network Congestion
09	Remote DTE Operational (PVC)
0F	Network Operation (PVC)
11	Incompatible Destination

REGISTRATION CONFIRMATION CAUSES	
HEX VALUE	REASON
13	Local Procedure Error
7F	Registration/Cancellation Confirmed
03	Invalid Facility Request
05	Network Congestion

FACILITY FIELD		
FACILITY TYPE	FACILITY CODE	PARAMETER LENGTH/FIELD
Flow Control Parameter Negotiation	42	0X XX
■ Packet Size	43	XX XX
■ Window Size		
Throughput Class Negotiation	02	XX —
Closed User Group Selection	03	XX XX
■ Basic Format	47	XX XX
■ Extended Format		
Closed User Group with Outgoing Access Selection	09	XX —
■ Basic Format	48	XX XX
■ Extended Format		
Bilateral Closed User Group Selection	41	XX XX
Reverse Charging	01	01 —
Fast Select	01	XX —
NUI Selection	C6	XX XX
Charging Information	04	01 XX
■ Requesting Service	C5	XX XX
■ Receiving Information	Further Study	— —
a) Monetary Unit	C2	XX XX
b) Distance	C1	04 XX
c) Segment Count		
d) Call Duration		
RPOA Selection	44	XX XX
■ Basic Format	C4	XX XX
■ Extended Format		
Call Redirection Notification	C3	0X XX
Called Line Address Modified Notification	08	XX —
Transit Delay Selection and Indication	49	XX XX
National Options Marker	00	XX —

Et n'oubliez pas : dans 99% des cas, le problème se situe entre le clavier et la chaise !

Classe débit (bits/s)

8765 → Appelant ← Appelé

4321 Appelant → Appelé

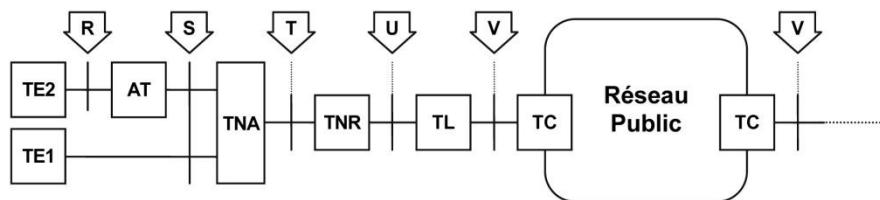
0 0 0	Réserve
0 0 1	Réserve
0 1 0	Réserve
0 1 1	75
0 1 0 0	150
0 1 0 1	300
0 1 1 0	600
0 1 1 1	1200
1 0 0 0	2400
1 0 0 1	4800
1 0 1 0	9600
1 0 1 1	19200
1 1 0 0	48000
1 1 0 1	64000
1 1 1 0	Réserve
1 1 1 1	Réserve

CCITT X.3 SUMMARY		
PARAMETER NUMBER	PARAMETER	DYNATECH VALUES
1	PAD Recall Defined Character	0 or 1 32 - 126
2	Local Echo	0 or 1
3	Data Forwarding Characters	0, 1, 2, 4, 6, 8, 16, 18, 32, 64, 128, 127 - n
4	Data Forwarding Timeout	0 - 255
5	PAD to Terminal Flow Control	0 - 4
6	Control of PAD Service Signals	0, 1, 4, 5, 8 - 15
7	PAD Action on Receipt of Break from Terminal	0, 1, 2, 4, 5, 8, 16, 21
8	Discard Output	0 or 1
9	Padding after Carriage Return	0 - 255
10	Line Folding	0 - 255
11	Async Speed (Read Only Parameter)	0 - 18
12	Terminal to PAD Flow Control	0, 1,
13	Line Feed Insertion	0, 1, 2, 4 - 7
14	Padding after Line Feed	0 - 255
15	Editing	0 or 1
16	Character Delete Defined Character	0 - 127
17	Buffer Delete Defined Character	0 - 127
18	Buffer Display Defined Character	0 - 127
19	Editing Service Signals	0, 1, 2, 6, 32-126
20	Echo Mask	0 - 128+
21	Parity Treatment	0, 1, 2, 3
22	Page Wait	0 - 255

DIAGNOSTIC CAUSE TABLE		
Continued		
DIAGNOSTIC CODE	MEANING	
DECIMAL	HEX	
37	25	Reject not Subscribed to
38	26	Packet too Short
39	27	Packet too Long
40	28	Invalid GFI
41	29	Restart or Registration Packet with Non-Zero in Bits 1 to 4 of Octet1, or Bits 1 to 8 of Octet 2
42	2A	Packet Type Not Compatible with Facility
43	2B	Unauthorized Interrupt Confirmation
44	2C	Unauthorized Interrupt
45	2D	Unauthorized Reject
47	2F	
48	30	Time Expired
49	31	Incoming Call
50	32	Clear Indication
51	33	Reset Indication
52	34	Restart Indication
53	3F	
64	40	Call Setup, Call Clearing or Registration Problem
65	41	Facility/Registration Code Not Allowed
66	42	Facility Parameter Not Allowed
67	43	Invalid Called Address
68	44	Invalid Calling Address
69	45	Invalid Facility/Registration Length
70	46	Incoming Call Barred
71	47	No Logical Channel Available
72	48	Call Collision
73	49	Duplicate Facility Request
74	4A	Non-Zero Address Length
75	4B	Non-Zero Facility Length
76	4C	Facility Not Provided when Expected
77	4D	Invalid CCITT-Specified DTE Facility
79	4F	
80	50	Miscellaneous
81	51	Improper Cause Code from DTE
82	52	Non-Aligned Octet
83	53	Inconsistent Q Bit Setting
95	5F	
96	60	Not Assigned
111	6F	
112	70	International Problems
113	71	Remote Network Problems
114	72	International Protocol Problems
115	73	International Link Out of Order
116	74	International Link Busy
117	75	Transit Network Facility Problem
118	76	Remote Network Facility Problem
119	77	International Routing Problem
120	78	Temporary Routing Problem
121	79	Unknown Called DNIC
122	7A	Maintenance Action
128	80	Reserved for Network Specific Diagnostic Information
255	FF	dece de 80 à FF, réservé pour l'information de diag propre au réseau.

## RNIS (OVERVIEW)

### Les Groupements Fonctionnels et les Points de référence



#### Groupements Fonctionnels

- TE : terminal
- AT : adaptateur de terminal
- TNA : terminaison numérique d'abonné
- TNR : terminaison numérique de réseau
- TL : terminal de ligne
- TC : terminal de commutation

#### Points de référence

- R : point de référence générique
- T : marque la frontière entre domaine public et domaine privé
- S et T peuvent être confondus (fonctionnement sans TNA)
- U correspond pratiquement à la boucle d'abonné

### RNIS et le modèle OSI

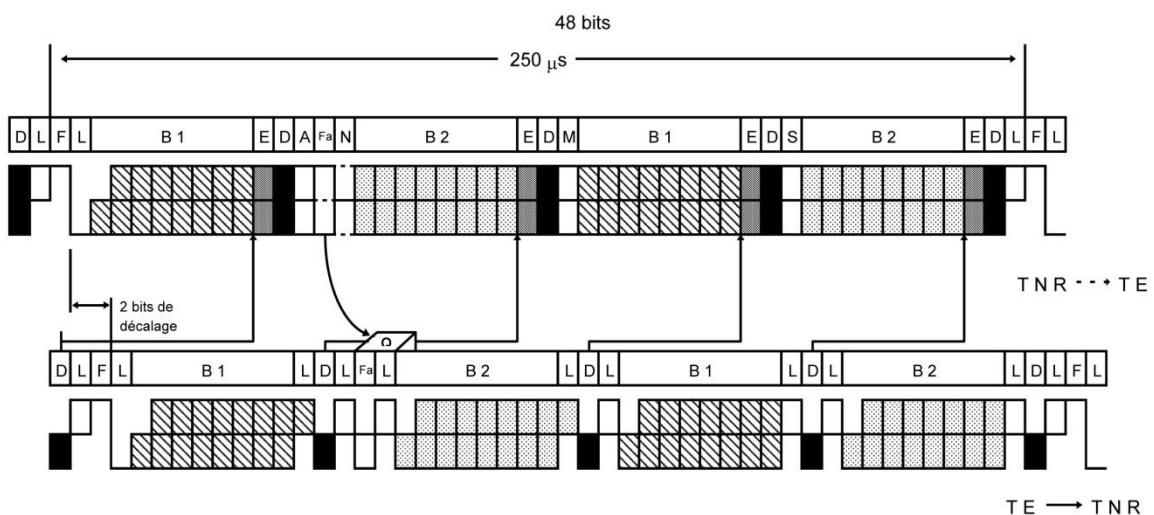
#### Modèle OSI

7 - Application
6 - Présentation
5 - Session
4 - Transport
3 - Réseau
2 - Liaison
1 - Physique

#### RNIS

Q.931 Procédures d'établissement d'appel sur le canal D	
Q.921 LAP D	
I.430 Accès de base	I.431 Accès Primaire

### Structure de la trame aux points de référence S et T



### LAP D Couche liaison suivant la recommandation Q.921

FLAG	Adresse	Contrôle	Information	FCS	FLAG
01111110	2 octets	1 ou 2 octets	0 ou N octets	2 octets	01111110
Champs contrôle Q.921 (modulo 128)					
8 7 6 5 4 3 2 1					
SAPI	C/R	EA 0			
TEI		EA 1			

**SAPI :** Service Accès Point Identifier  
 0 = Signalisation réseau (commande d'appel) ("s")  
 16 = Paquets d'usager (X25 dans D) ("p")  
 24 = Téléaction ("t")  
 63 = Gestion TEI, associé à TEI = 127 ("m")  
 Autres = Réserves pour le futur

**TEI :** Terminal Endpoint Identifier  
 0-63 = Affectation non-automatique (déterminé par avance)  
 64-126 = Affectation automatique  
 127 = Diffusion, associé à SAPI = 63 (gestion)

**C/R :** Bit Commande/Réponse

Direction	Commande	Réponse
U → R	0	1
U ← R	1	0

**EA :** Bit d'extension du champ d'adresse  
 1 = Fin d'octet d'adresse  
 0 = Un octet d'adresse suit

\* Les trames XID peuvent également être utilisées à des fins de négociations de paramètres de la connexion de données.

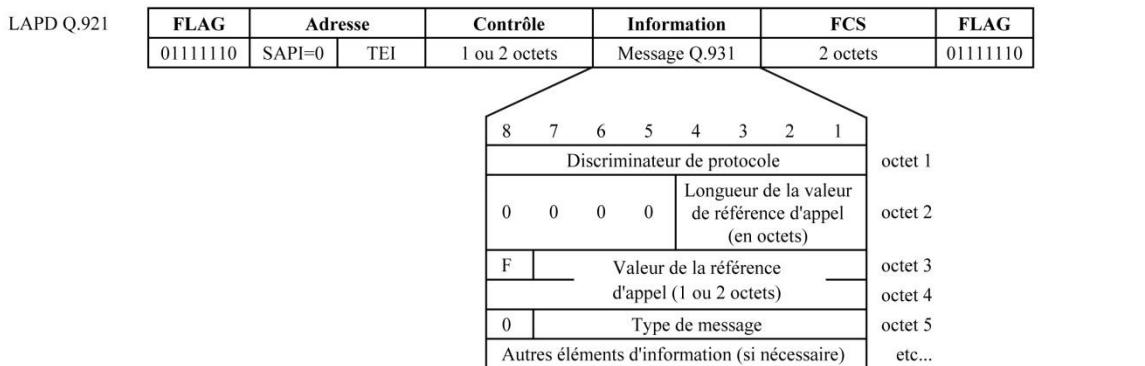
Applications	Format	Commandes	Réponse	Codage
				8 7 6 5 4 3 2 1
Trames d'information		I (informations)		N(S) 0 N(R) P
Transfert d'information à trames multiples avec accusé de réception et sans accusé de réception		RR (prêt à recevoir)	RR (prêt à recevoir)	0 0 0 0 0 0 0 1 N(R) P/F
		RNR (non prêt à recevoir)	RNR (non prêt à recevoir)	0 0 0 0 0 1 0 1 N(R) P/F
		REJ (rejet)	REJ (rejet)	0 0 0 0 1 0 0 1 N(R) P/F
		SABME (mettre en mode asynchrone, équilibré étendu)		0 1 1 P 1 1 1 1
		DM (mode déconnecté)		0 0 0 F 1 1 1 1
		UI (informations non numérotées)		0 0 0 P 0 0 1 1
		DISC (déconnexion)		0 1 0 P 0 0 1 1
		UA (accusé de réception non numéroté)		0 1 1 F 0 0 1 1
		FRMR (rejet de trame)		1 0 0 F 0 1 1 1
		XID* (échange d'identificateur)	XID* (échange d'identificateur)	1 0 1 P/ 1 1 1 1

### Structure de la trame pour la gestion du TEI

FLAG	Adresse de diffusion			Contrôle : UI	Information	FCS	FLAG
7E	SAPI 63	C	0	TEI 127	1	000 P 0011	5 octets
Identificateur de l'entité de gestion 0000 1111							
	Numéro de référence "RI" 0 à 65535 (n° aléatoire)						octet 1
	Type de message "MI" 1 à 7						octet 2
	Identificateur d>Action "AI"				1		octet 3
							octet 4
							octet 5

### Messages définis pour la gestion des TEI

Nom du message	Direction	Identificateur de l'entité de gestion	N° de référence	Type de message	Identificateur d>Action	
Demande d'identité	U → R	0000 1111	0 à 65535	0000 0001	AI = 127	Toute valeur de TEI acceptable
Identité affectée	U ← R	0000 1111	0 à 65535	0000 0010	AI = 64 à 126	Valeur de TEI affectée
Identité refusée	U ← R	0000 1111	0 à 65535	0000 0011	AI = 64 à 126	Valeur de TEI refusée
					AI = 127	Pas de valeur de TEI disponible
Demande de contrôle d'identité	U ← R	0000 1111	non utilisé codé 0	0000 0100	AI = 0 à 126	Valeur de TEI à vérifier
					AI = 127	Vérifier toutes les valeurs de TEI
Réponse au contrôle d'identité	U → R	0000 1111	0 à 65535	0000 0101	AI = 0 à 126	Valeur de TEI utilisée
Suppression d'identité	U ← R	0000 1111	non utilisé codé 0	0000 0110	AI = 127	Supprimer toutes les valeurs de TEI
					AI = 0 à 126	Les valeurs de TEI sont à supprimer
Vérification d'identité	U → R	0000 1111	non utilisé codé 0	0000 0111	AI = 0 à 126	Valeur de TEI dont la vérification est demandée

**L A P D C o u c h e r é s e a u s u i v a n t la r e c o m m a n d a t i o n Q . 9 3 1****D i s c r i m i n a t e u r d e P r o t o c o l e**

8	7	6	5	4	3	2	1	Signification
0	0	0	0	1	0	0	0	Discriminateur de protocole pour les messages de commande d'appel usager-réseau Q.931 (I.451)

Les valeurs codées 0100 0011 et 0100 0111 sont réservées pour usage privé (Terminals derrière une TNA) ou pour usage national.

**R é f é r e n c e d ' a p p e l**

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	X	X	Longueur de la valeur de référence d'appel (en octet)
Fanion	Valeur de la référence d'appel (début)							octet 1
	Valeur de la référence d'appel (fin)							octet 2
								octet 3

Longueur de la valeur de référence d'appel :  
01 = 1 octet (pour l'accès de base)

10 = 2 octets (pour l'accès primaire)

Fanion de la référence d'appel à émettre dans les messages d'établissement/rupture

0 = côté d'origine de l'appel

1 = côté récepteur de l'appel

**T y p e s d e m e s s a g e s**

Hex	87654321	Message
01	000 -----	<b>Messages d'établissement de l'appel</b>
02	00001	Alerte
07	00010	Appel en cours
0F	00111	Connexion
03	01111	Accusé de réception de connexion
05	00011	Appel acheminé
0D	00101	Etablissement
	01101	Accusé de réception d'établissement
26	001 -----	<b>Messages en phase d'information de l'appel</b>
2E	00110	Reprise
22	01110	Accusé de réception de reprise
25	00010	Refus de reprise
2D	00101	Suspension
21	01101	Accusé de réception de suspension
20	00001	Refus de suspension
	00000	Information d'usage
45	010 -----	<b>Messages de libération de l'appel</b>
4D	00101	Déconnexion
5A	01101	Libération
	11010	Fin de libération
7B	011 -----	<b>Messages divers</b>
62	11011	Information
64	00010	Facilité
7D	00100	Enregistrement
	11101	Etat

**F o r m a t d e s o c t e t s d e s a u t r e s élém e n t s d ' i n f o r m a t i o n**

Format sur un octet (Type 1)		
1	Identificateur de l'élément d'information	Contenu de l'élément d'information
1	Identificateur de l'élément d'information	
Format sur un octet (Type 2)		
0	Identificateur de l'élément d'information	
Format à longueur variable		
0	Identificateur de l'élément d'information	octet 1
	Longueur du contenu de l'élément d'information (en octets)	octet 2
	Contenu de l'élément d'information	octet 3

## COMMUTATION

---

### QUE FAUT-IL POUR PASSER EN FULL DUPLEX ?

---

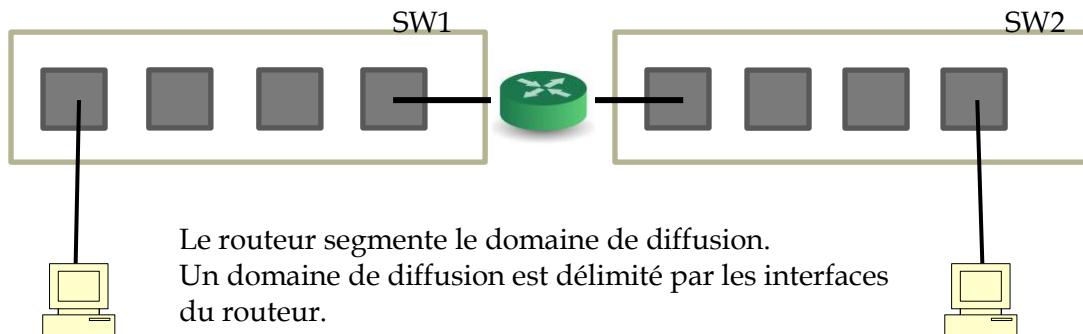
Il faut être au minimum deux et débrayer CSMA/CD.

### NOUVELLE FRONTIERE ?

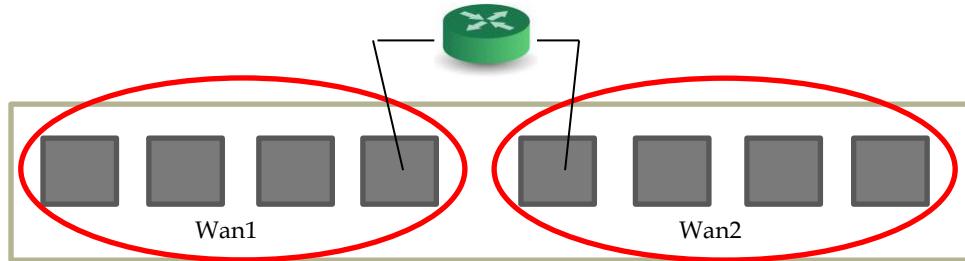
---

Le domaine de diffusion

#### Alternative 1



#### Alternative 2



Solution 1 : routeur.

Solution 2 : commutateur de niveau 3.

## NUMEROTATION DES INTERFACES

---

type slot\_#/port\_#

ou type {ethernet | fastethernet | gigabitethernet | tengigabitethernet}.

slot\_# : numéro de carte fille, démarre à 0. (Série 2900, slot toujours à 0).

Port\_# : le port 0 n'existe pas.

Exemple : sur un 2900 équipé giga, le 1<sup>er</sup> port disponible est gigabitethernet 0/1.

### CONFIGURATION IP (NECESSAIRE POUR TELNET OU SSH)

---

```
Switch>en
Switch#conf t
```

```

Switch(config)#hostname SW100
SW100(config)#interface vlan 1
SW100(config)#ip address {dhcp | 192.168.1.254 255.255.255.0}
SW100(config)#no shut
SW100(config)#ip default gateway 192.168.1.1
SW100(config)#CTRL+Z
SW100#wr

```

## CONFIGURATION DES INTERFACES COMMUTÉES

```

SW100(config)#int f0/1
SW100(config-if)#duplex {full |half|auto}
SW100(config-if)#speed {10|100|1000|auto}
SW100(config-if)#description .....
SW100(config-if)#no shutdown

```

```

SW100(config)#interface range F0/11 - 20
SW100(config-if-range)#

```

Une commande show utile: `sh interfaces status`

Port	Name	Station	Vlan	Duplex	Speed	Type
------	------	---------	------	--------	-------	------

Show interfaces F0/1 status → compteur de paquets

## SECURISATION

A la sortie du carton, tous les ports appartiennent à Vlan1, auto, no shut → plug and play.

1. Sécuriser les ports utilisés

`SW100(config-if)#switchport mode access` → le contraire de Trunk le port appartient à un seul Vlan.

`SW100(config-if)#switchport port-security` → active la fonction sécurité.

`SW100(config-if)#switchport port-security mac-address 0200.1111.2222`

Autant de fois qu'il y a de stations connues sur ce port.

Ou

`SW100(config-if)#switchport port-security mac-address sticky` → on "colle" l'adresse mac.

`SW100(config-if)#port-security violation {protect|restrict|shutdown}`

Par défaut

	Protect	Restrict	shutdown
Rejette le traffic	✓	✓	✓
Envoie un message syslog et SNMP		✓	✓
Désactive l'interface			✓

2. Sécuriser les ports inutilisés

- `shutdown`
- `switchport mode access` → empêcher le Trunk
- Affecter le port à un Vlan « poubelle »

## CONFIGURATION D'UN VLAN D'ACCÈS

---

- ```

>1. show vlan brief
 2. Ajouter un vlan
    SW100(config)#vlan 200
    SW100(config-vlan)#name vlan-compta
    SW100(config-vlan)#exit
 3. Affectation d'une interface au vlan200
    SW100(config)#interface range F0/3 - 5
    SW100(config-range)#switchport mode access
    SW100(config-range)#switchport acces vlan 200
    SW100(config-range)#exit
4.
```

## ORGANISATION DE LA MEMOIRE

---

|       | Router               | Commutateur                                                                                    |
|-------|----------------------|------------------------------------------------------------------------------------------------|
| NVRAM | Startup-config       | Pas de partition NVRAM c'est la Flash qui héberge<br>Config.text ≡ startup-config<br>+vlan.dat |
| RAM   | Travail              |                                                                                                |
| ROM   | IOS Réduit<br>ROMMON | Bootloader invite switch:                                                                      |
| FLASH | IOS                  | IOS<br>Ou<br>Catos → haut de gamme                                                             |

## COMMANDES SUR LES SWITCHS

---

### DEPANNAGE D'UN SWITCH

---

```

Switch: flash_int
Switch: load_helper
Switch: help cde
Switch: dir Flash
Switch: format Flash:
Switch: set BAUD 115200
→ régler l'hyperterminal à 115200
[Optionnel: mkdir flash:/IOS]
Switch: copy xmodem: Flash: c3560-ipservicesk9-mz-122-50.se3.bin
Switch: boot (ou reset)
```

### RECUPERATION D'UN MOT DE PASSE

---

Maintenir le bouton poussoir « mode » enfoncé, puis mettre sous tension → bootloader switch :

```
Switch: flash_int
```

```

Switch: load_helper
Switch: dir Flash
Switch: rename flash: config-text flash: config.old
Switch: boot
Le switch propose le mode setup → no
Switch>en
Switch#dir flash
Switch#rename flash: config.old flash: config-text
Switch#show start

```

---

### RECUPERER ET CHANGER LES MOTS DE PASSE

---

```

Switch#copy start run
Switch#enable secret ...
.
.
.
Switch#wr

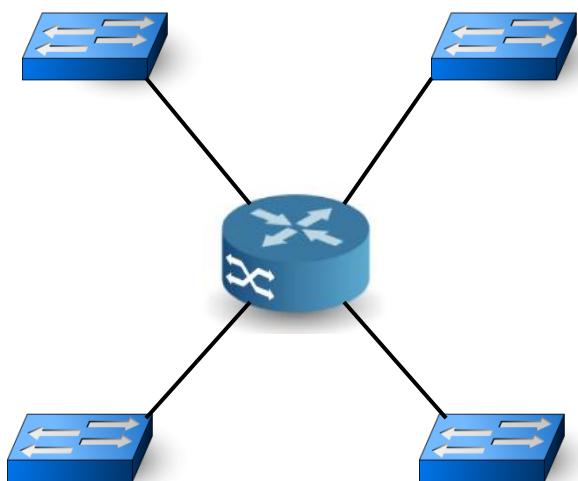
```

---

### SPANNING-TREE

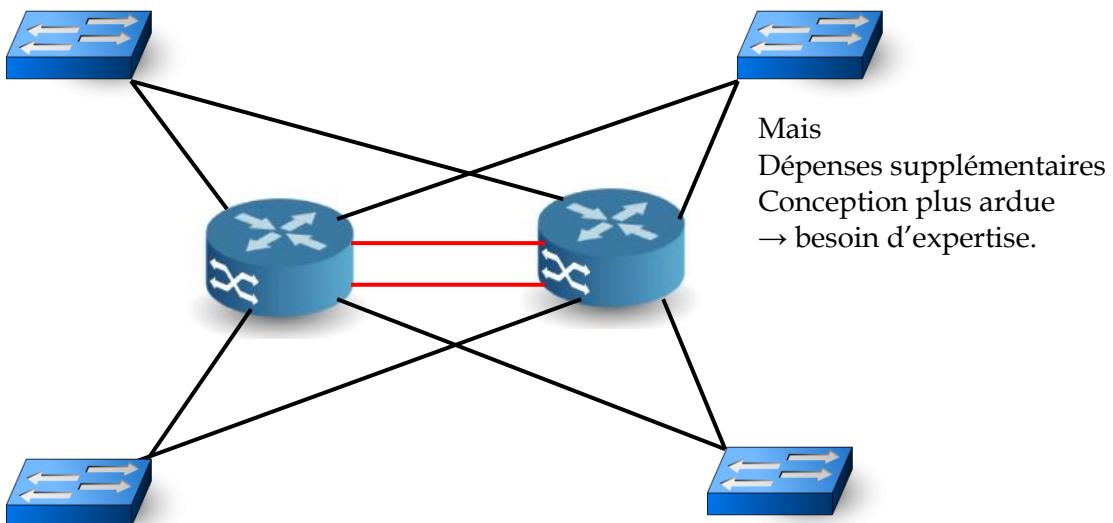
---

Problème : la disponibilité ?

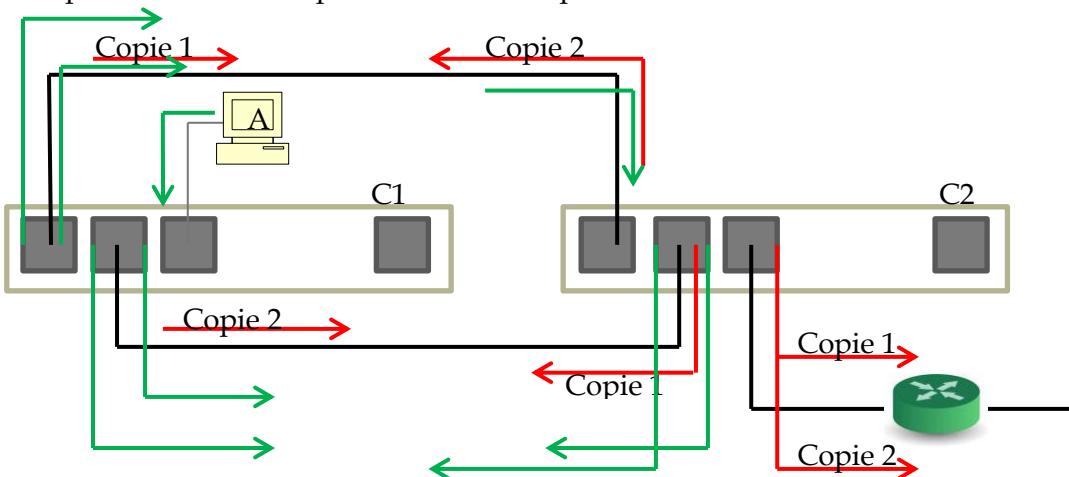


Arborescence à 3 couches  
Core  
Distribution  
Accès

Solution : ajouter de la redondance.



Que se passe-t-il s'il existe plusieurs chemins possibles ?



Ni la station A, ni le routeur ne sont connus des tables CAM des commutateurs.  
A émet une trame destiné au routeur, unicast.

C1 apprend →

|    |   |
|----|---|
| @A | 1 |
|    |   |

Problème 1 : instabilité des correspondances en CAM

C2 reçoit une copie 1 sur son port 1  
Et quasi immédiatement  
C2 reçoit une copie 2 sur son port 2

|    |   |
|----|---|
| @A | 1 |
|    |   |
| @A | 2 |

Problème 2 : le routeur reçoit 2 exemplaires de la même trame.  
Comment se comporte le protocole ?  
Si c'est bien écrit ok !

A émet une trame diffusée

Problème 3 : création de boucles infinies. En effet, il n'existe pas l'équivalent du TTL en couche 2.

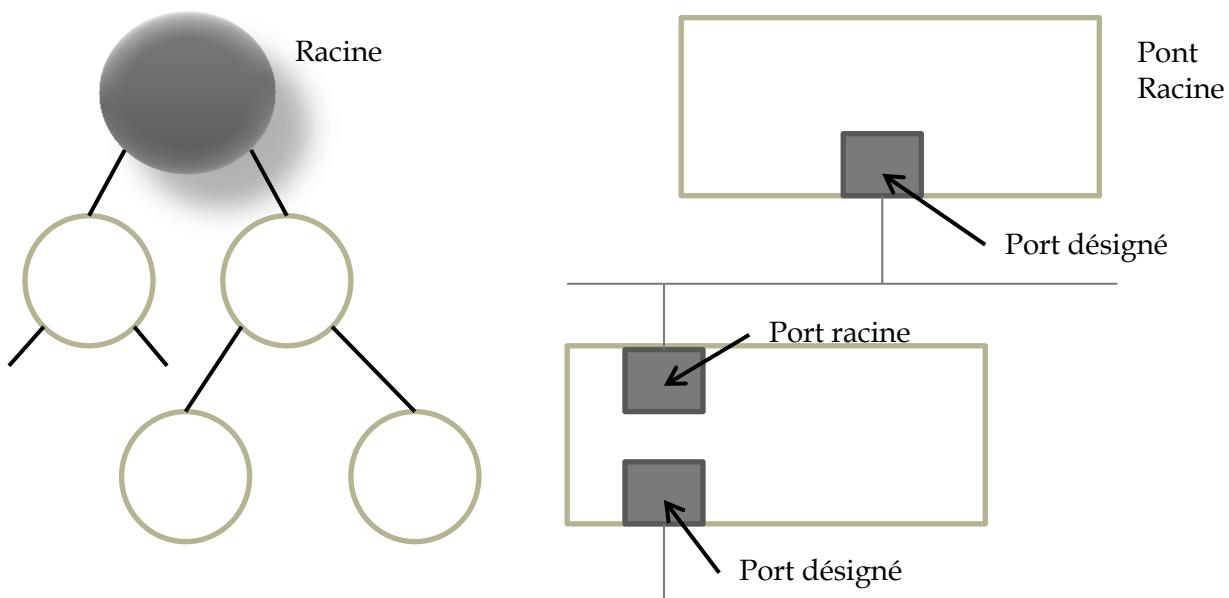
## OBJECTIF DE SPANNING-TREE

- Etablir un seul chemin entre tout couple de stations (topologie sans boucle).
- Déterminer l'arbre de recouvrement avec le minimum de trafic.
- Puis maintenir cet arbre à jour.
- Sans que les systèmes d'extrémités en aient connaissance → Transparent

Méthode :

Activer ou désactiver les ports convenables (IEEE 802.1D).

## VOCABULAIRE STP (SPANNING-TREE PROTOCOL)



### 1 - Détermination de la Racine.

Un seul pont est élu pont racine (root bridge).

Tous ports du pont racine sont placés dans un état passant (Forwarding).

→ Le port participe au trafic

### 2 - Détermination d'un meilleur chemin pour atteindre la racine.

Chaque port **non** racine désigne parmi ses ports, un seul port racine.

Critère : moindre coût.

Si 2 ports ont des coûts identiques, c'est le port de numéro le moins élevé qui est choisi.

Le port racine est placé dans un état passant.

### 3 - Blocage des chemins alternatifs.

Chaque segment ne disposant pas d'un port racine est doté d'un et d'un seul port désigné.

Critère : moindre coût vers le port racine.

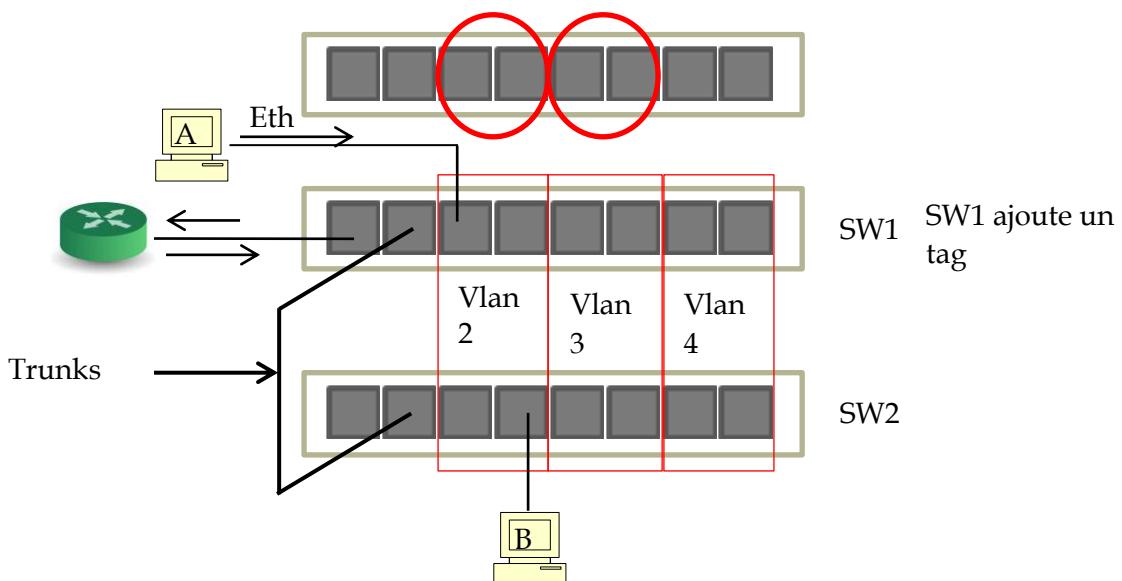
Un port qui n'est ni désigné, ni racine reste dans l'état bloquant (blocking).

### COUTS

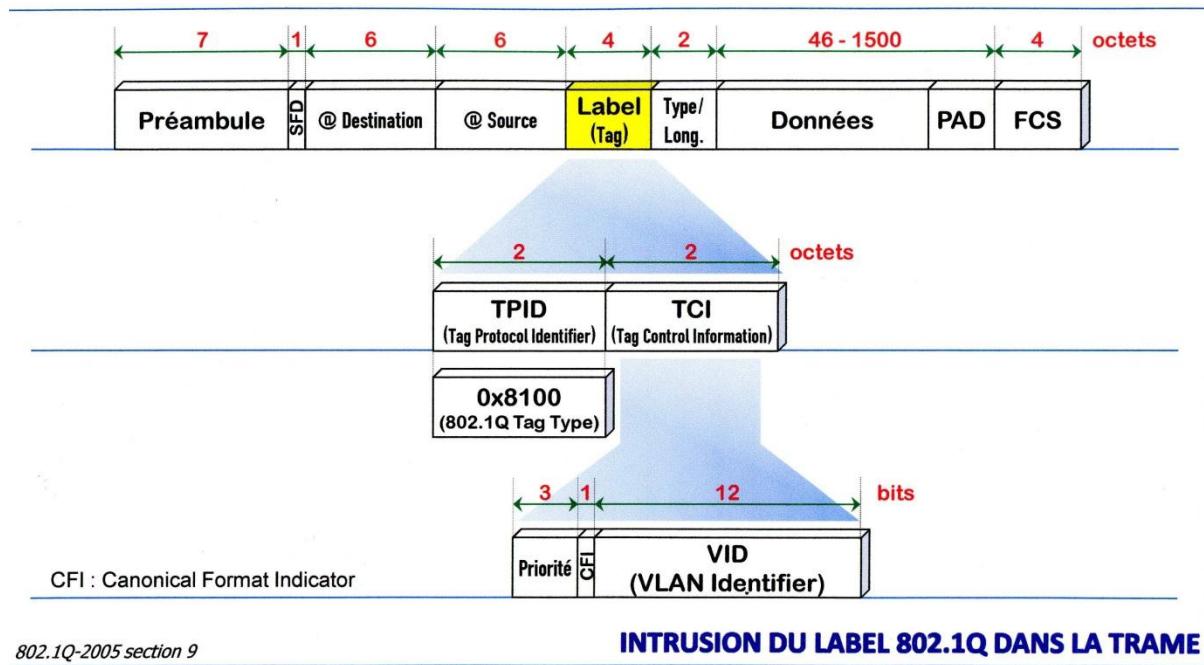
| débits   | coûts | Initial ( $\frac{10^9}{\text{débit}}$ ) | Révisé |
|----------|-------|-----------------------------------------|--------|
| 10Mbps   |       | 100                                     | 100    |
| 16 Mbps  |       |                                         | 62     |
| 45 Mbps  |       |                                         | 39     |
| 100 Mbps |       | 10                                      | 19     |
| 155 Mbps |       |                                         | 14     |
| 622 Mbps |       |                                         | 6      |
| 1 Gbps   |       | 1                                       | 4      |
| 10 Gbps  |       |                                         | 2      |

} ATM

### ROUTAGE INTER-VLAN



Un lien trunk, définition du métier : agrégation de canaux. Définition donnée par CISCO : transporte des trames issues de plusieurs VLAN.



## CONFIGURATION DES INTERFACES APPARTENANT A 1 VLAN

```
SW1#conf t
SW1(config)#int F0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
.
.
```

## CONFIGURATION / CREATION DES VLAN

```
SW1(config)#vlan 2
SW1(config-vlan)#name vlan_compta
```

## CONFIGURATION DU LIEN TRUNK

```
SW1(config)#int f0/2
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan {add|all|except|remote}
liste_vlan
```

## CONFIGURATION DU ROUTEUR

On ne peut pas affecter plusieurs adresses IP à une interface de routeur.

```
RTR(config)#interface F0/0.2
RTR(config-subif)#encapsulation dot1q x → 802.1q
RTR(config-subif)#ip address @IP masque → sous-réseau affecté au vlan x. ← N° de vlan
```

```
RTR(config)#interface F0/0.2
```

```
RTR(config-subif)#encapsulation dot1q y  
RTR(config-subif)#ip address @IP masque → sous-réseau affecté au vlan y.
```

## COMMANDES SUR LES SWITCHS

---

|                                                                              |                                                                                                                                                    |
|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Switch#terminal history</b>                                               | Active l'historique du terminal. Vous pouvez exécuter cette commande en mode utilisateur ou en mode d'exécution privilégié.                        |
| <b>Switch#terminal history size 50</b>                                       | Configure la taille de l'historique du terminal. L'historique du terminal peut conserver entre 0 et 256 lignes de commande.                        |
| <b>Switch#terminal no history size</b>                                       | Rétablissement la taille de l'historique du terminal d'après sa valeur par défaut, soit 10 lignes de commande.                                     |
| <b>Switch#terminal no history</b>                                            | Désactive l'historique du terminal.                                                                                                                |
| <b>Switch(config-if)#switchport mode access</b>                              | Définissez le mode d'interface en accès. Vous ne pouvez pas configurer une interface en tant que port sécurisé selon le mode dynamique par défaut. |
| <b>Switch(config-if)#switchport port-security</b>                            | Activez la sécurité des ports sur l'interface.                                                                                                     |
| <b>Switch(config-if)#switchport port-security maximum 50</b>                 | Définissez le nombre maximal d'adresses sécurisées à 50.                                                                                           |
| <b>Switch(config-if)#switchport port-security mac-address sticky</b>         | Activez l'apprentissage rémanent.                                                                                                                  |
| <b>Switch(config-if)#switchport port-security mac-address 0200.1111.2222</b> | Autant de fois qu'il y a de stations connues sur ce port.                                                                                          |

## PROTOCOLE VTP

---

### ADMINISTRATION DES VLAN ?

---

- Pour ajouter un VLAN sur un réseau
  - L'administrateur doit l'ajouter sur chaque switch !
  - Nécessite beaucoup de manipulation sur de grands réseaux.
- Pour éviter cela, sur des switchs CISCO, la manipulation peut être faite sur un seul switch :
  - La modification sera alors diffusée sur les autres via le protocole VTP : VLAN Trunking Protocol.
  - Nous distinguons dans ce cas, des switchs VTP server et des VTP client.
  - La VTP server va diffuser la modification vers les autres switchs VTP client.

### LE VOCABULAIRE

---

- **Le VTP domain :**
  - Tous les switchs appartenant au même VTP domain échangeront leurs informations sur les VLAN.
- **Les VTP Mode :**
  - Un switch peut être en mode server :
    - Il diffuse ses informations sur les VLAN à tous les autres switchs appartenant au même VTP domain.
    - Ces informations sont stockés en NVRAM et sur un tel switch, il est possible de créer, modifier ou détruire un VLAN du VTP domain.
  - En mode client :
    - Il stocke uniquement les informations sur les VLAN, transmises par le switch en mode VTP server sur le même domaine.
  - Ou bien en mode transparent :
    - Il transmet les informations VTP aux autres switchs mais ne les traitent pas. Ces switchs sont autonomes et ne participent pas aux VTP.
  - Le VTP Pruning :
    - Supprime la propagation des messages de broadcast, multicast et autres messages inconnus unicast sur les liens trunks afin d'optimiser la bande passante.

### LA CONFIGURATION PAR DEFAUT

---

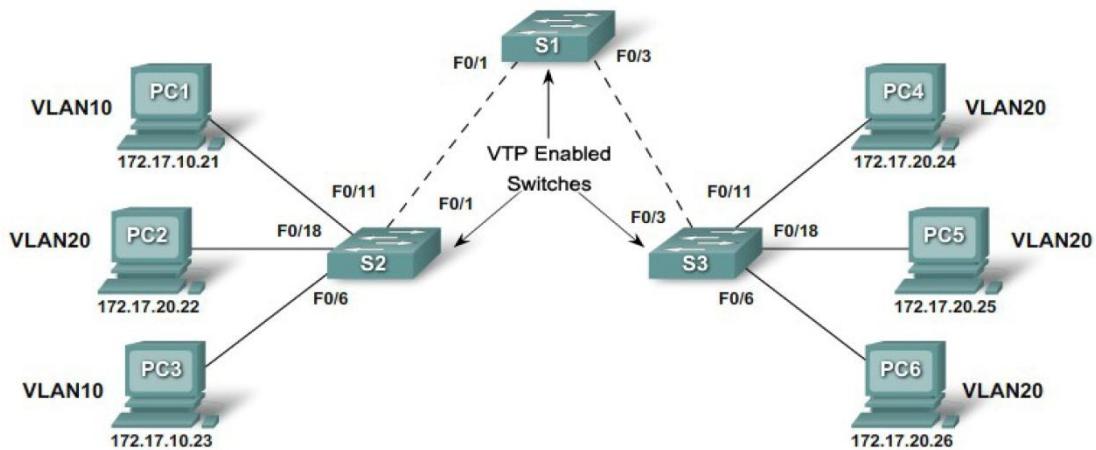
- Par défaut, un switch est en :
  - Mode server.
  - Le VTP domain name est égal à null.
  - Tous les ports sont dans le VLAN 1.
  - Le numéro de révision de la configuration VTP est 1.
  - La version du protocole VTP est 1 :
    - Il existe 3 versions. Pour un VTP domain, tous les switchs doivent être dans la même version.
- La commande `show vtp status` permet de visualiser la configuration d'un switch.

## LA PROPAGATION DU DOMAINE

- Les VTP Server propagent leur domaine VTP vers les autres switchs via des messages VTP advertisement.
- Ces messages de type advertisement sont utilisés pour transporter :
  - Les informations sur les domaines VTP.
  - Les informations sur les modifications des VLAN.
- Chaque message est composé :
  - D'un VTP header et
  - D'un VTP data field.
- Chaque message VTP est inséré dans le champ de données des trames Ethernet qui sont elles-mêmes encapsulées dans une trame 802.1q ou ISL.
- Chaque switch envoie périodiquement, par multicast, sur ses liens trunk des VTP advertisement.

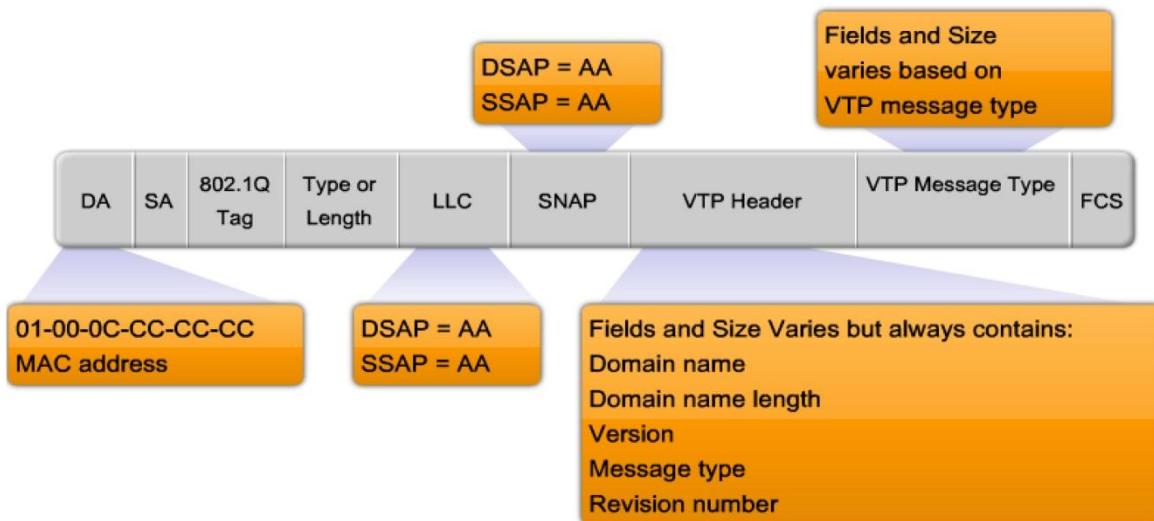
## VTP PRUNING

- Dans certain cas, il est inutile de propager les informations vers tous les switchs comme dans l'exemple suivant :



- Il est inutile de propager vers le switch S1 dans les informations du VLAN 10.

## LES VTP ADVERTISEMENT MESSAGES



## LES INFORMATIONS D'UN MESSAGE ADVERTISEMENT

### VTP FRAME STRUCTURE

**VTP advertisements send this global domain information:**

- VTP domain name.
- Updater identity and update timestamp.
- MD5 digest.
- Frame format.

**VTP advertisements send this VLAN information:**

- VLAN ID.
- VLAN name.
- VLAN type.
- VLAN state.
- Additional VLAN configuration information specific to the VLAN type.

**Les VTP revision number**

- Code sur 32 bit.
- Par défaut, c'est la valeur 0.
- A chaque ajout ou suppression d'un VLAN, ce nombre est incrémenté de 1 par le switch VTP server.
- Au changement du nom du VTP domain, ce nombre est mis à 0.
- Permet de connaître le message VTP le plus récent.

## LES TYPES DE MESSAGE ADVERTISEMENT.

- Summary Advertisement :
  - Message utilisé dans la plupart des cas.

**Summary Advertisement**

| Version                                          | Code | Followers | MgmtD Len |
|--------------------------------------------------|------|-----------|-----------|
| Management Domain Name (Zero-Padded to 32 Bytes) |      |           |           |
| Configuration Revision Number                    |      |           |           |
| Updater Identity                                 |      |           |           |
| Update Timestamp (12 Bytes)                      |      |           |           |
| MD5 Digest (16 Bytes)                            |      |           |           |

**Followers** - The Followers field indicates that this packet is followed by a Subset Advertisement packet.

**MgmtD Len** – Indicated the length of the management domain name.

**Updater Identity** - The Updater Identity is the IP address of the switch that is the last to have incremented the configuration revision.

- Subset Advertisement :
  - Contienne le détail de chaque VLAN.

**Advertisements Details****Subset Advertisements**

| Version                                          | Code | Seq-Number | Domain Name Length |
|--------------------------------------------------|------|------------|--------------------|
| Management Domain Name (zero-padded to 32 bytes) |      |            |                    |
| Configuration Revision Number                    |      |            |                    |
| VLAN-info Field 1                                |      |            |                    |
| :                                                |      |            |                    |
| VLAN-info Field N                                |      |            |                    |

The VLAN-info field contains information for each VLAN and is formatted as follows:

**VLAN-Info**

| Info Length                                        | Status | VLAN-Type | VLAN-name Len |
|----------------------------------------------------|--------|-----------|---------------|
| ISL VLAN-id                                        |        |           | MTU Size      |
| 802.10 Index                                       |        |           |               |
| VLAN-name (Padded with 0s to Multiples of 4 bytes) |        |           |               |

- Request Advertisement :
  - Utilisé quand un switch n'a pas reçu les informations sur tous les VLAN.
    - Quand il est en mode client et démarre par exemple.

**Advertisement Request**

| Version                                          | Code | Rvsd | MgmtD Len |
|--------------------------------------------------|------|------|-----------|
| Management Domain Name (zero-padded to 32 bytes) |      |      |           |
| Start Value                                      |      |      |           |

**StartValue** – This field is used when there are several subset advertisements. If the first (n) subset advertisement has been received and the subsequent one (n+1) has not been received, the VTP enabled switch only requests advertisements from the (n+1)th one.

## EN RESUME

|                                                 | VTP Server                                 | VTP Client                                                                           | VTP Transparent                                                                                 |
|-------------------------------------------------|--------------------------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Description                                     | Manage Domain and VLAN configurations      | Updates VTP configurations<br>VTP client switches cannot change VLAN configurations. | Able to manage local VLAN configurations. Local VLAN configurations not shared with VTP network |
| Respond to VTP advertisements?                  | Participates fully                         | Participates fully                                                                   | Only Forwards VTP advertisements                                                                |
| Global VLAN configuration preserved on restart? | Yes, global configurations stored in NVRAM | No, global configurations stored in RAM, not in NVRAM                                | No, local VLAN configuration only is stored in NVRAM                                            |
| Update other VTP enabled switches?              | Yes                                        | Yes                                                                                  | No                                                                                              |

## CONFIGURATION DU PROTOCOLE VTP

### VTP Configuration Guidelines

#### On the VTP Server:

- Confirm default settings
- Configure 2 switches as VTP servers
- Configure the VTP domain on the first switch in the network
- Ensure all switches are in the same VTP protocol version mode
- Configure VLANs and trunk ports

#### On the VTP Client:

- Confirm default settings
- Configure VTP client mode
- Configure trunks
- Connect to VTP server
- Verify VTP status
- Configure access ports

## LES COMMANDES

### CHANGER LE MODE VTP

```
Switch(config)# vtp mode { client | server | transparent }
```

### CHANGER LA VERSION DE VTP

```
Switch(config)# vtp version { 1 | 2 }
```

Sur les switchs Cisco 2960, seules les versions 1 et 2 sont disponibles

### CHANGER LE VTP DOMAIN

```
Switch(config)# vtp domain Le-domaine
```

### DEFINIR UN MOT DE PASSE

```
Switch(config)# vtp password mot-de-passe
```

---

**RESET DU REVISION NUMBER**

---

Il faut effectuer un changement de nom du VTP domaine

---

**POUR VOIR LES INFORMATIONS SUR LE PROTOCOLE VTP**

---

**Switch# show vtp status**

---

**POUR VISUALISER LES LIAISONS TRUNK**

---

**Switch# show interfaces trunk**

## MÉTHODE D'AUTHENTIFICATION RADIUS

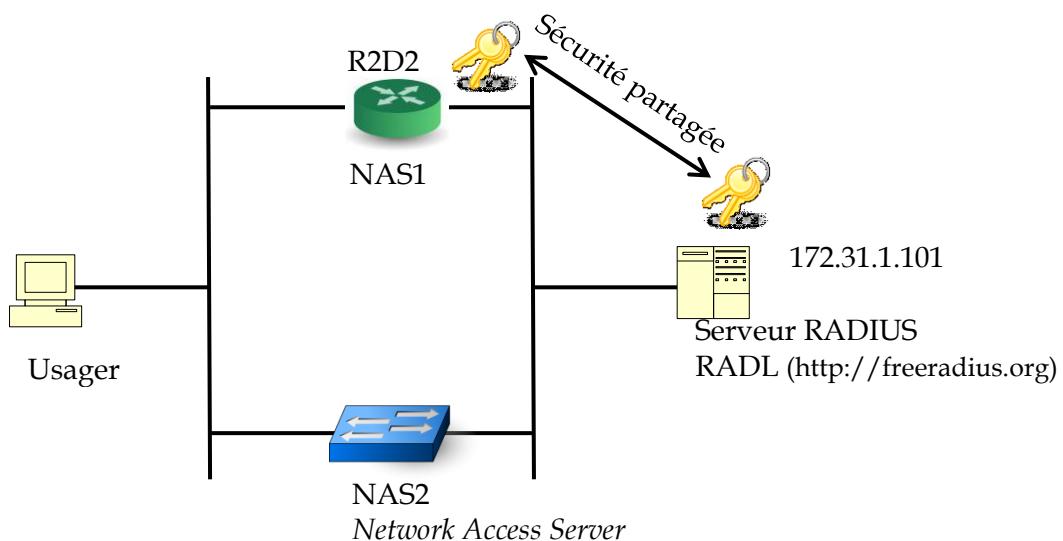
RADIUS: Remote Authentication Dual In User Service.

2 technologies

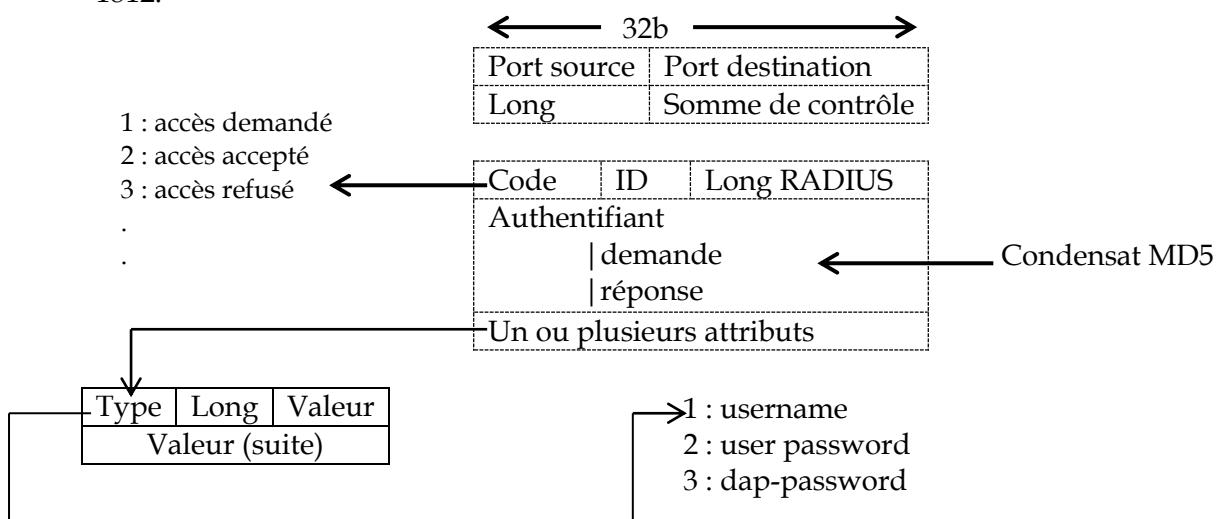
1. RADIUS:

- Authentification (RFC 2865)
- Accounting (RFC 2866)

2. TACACS+ → propriété de CISCO.



RADIUS s'appuie sur UDP, d'abord n° de port 1645 mais actuellement le n° de port officiel 1812.



## MISE EN ŒUVRE DE RADL

- 1 - Menu Setup | Server  
Régler les ports (laisser à 1645).
- 2 - Menu Setup | Clients  
Chercher la clé ClientName Key  
Localhost secret  
172.31.1.1 macleradius
- 3 - Créer la base de compte  
Menu Setup | User  
ycousin Password= « sangria »  
user-service-type=login-user

## CONFIGURATION DU NAS1

```
R2D2(config)#aaa new-model
R2D2(config)#aaa authentication login liste_tsrit radius local
R2D2(config)#radius-server host 172.31.1.101
R2D2(config)#radius-server login macleradius
R2D2(config)#line vty 0 4
R2D2(config-line)#login authentication liste_tsrit
R2D2(config-line)#exit
```

## CREATION DE LA BASE DES COMPTES LOCAUX

```
R2D2(config)#username ycousin {password|secret} sangria
```

## QUELQUES OUTILS POUR ANALYSER DES TRAMES

---

### STRUCTURE DE LA TRAME ETHERNET (SANS PREAMBULE)

---

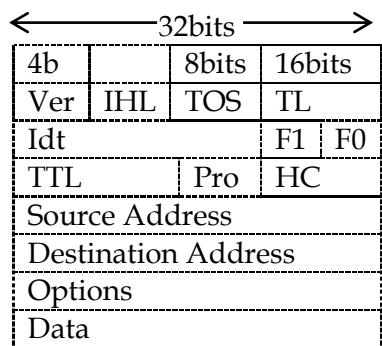
| 48bits              | 48bits         | 16bits | 32bits      |
|---------------------|----------------|--------|-------------|
| Adresse destination | Adresse source | Type   | Données CRC |

Quelques types :

0x0200 = XEROX PUP  
 0x0800 = DoD Internet  
 0x0803 = ECMA Internet  
 0x0806 = ARP  
 0x8035 = RARP  
 0x8098 = Appletalk

### STRUCTURE DU PAQUET IP

---



Ver = Version d'IP

IHL = Longueur de l'en-tête IP (en mots de 32 bits)

TOS = Type de service (zéro généralement)

TL = Longueur totale du paquet (en octets)

Idt = Identificateur pour la fragmentation

F1 (3 premiers bits) = bits pour la fragmentation

1<sup>er</sup> = réservé

2<sup>ème</sup> = ne pas fragmenter

3<sup>ème</sup> = fragment suivant existe

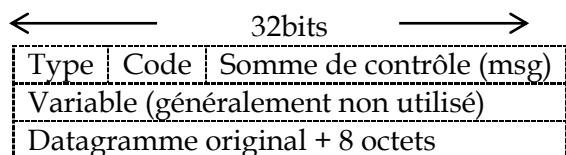
F0 (13 bits suivants) = décalage du fragment

TTL = durée de vie

Pro = Protocole transporté

|                        |           |
|------------------------|-----------|
| 1 = ICMP               | 8 = EGP   |
| 2 = IGMP               | 9 = IGP   |
| 4 = IP (encapsulation) | 17 = UDP  |
| 5 = Stream             | 36 = XTP  |
| 6 = TCP                | 46 = RSVP |

## STRUCTURE DU PAQUET ICMP



Quelques types ICMP :

0 = réponse d'écho

3 = Signalisation

Code 0 - réseau inaccessible

Code 1 - hôte inaccessible

Code 2 - port inaccessible

8 = demande d'écho

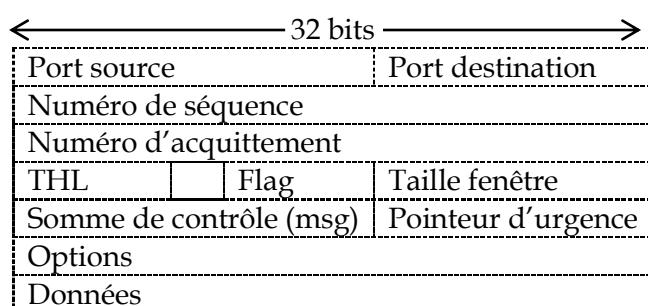
11 = durée de vie écoulée (TIME\_EXCEEDED)

Code 0 - TTL nul avant la destination

Code 1 - temps de rassemblement dépassé

12 = erreur de paramètre

## STRUCTURE DE SEGMENT TCP



THL = longueur de l'entête TCP

Flags = indicateur codé sur 6 bits

1<sup>er</sup> = données urgentes

2<sup>ème</sup> = acquittement (ACK)

3<sup>ème</sup> = données immédiates (Push)

4<sup>ème</sup> = réinitialisation (Reset)

5<sup>ème</sup> = synchronisation (SYN)

6<sup>ème</sup> = fin

Option = de type TLV

T = un octet type

2 = négociation de la taille max. du segment

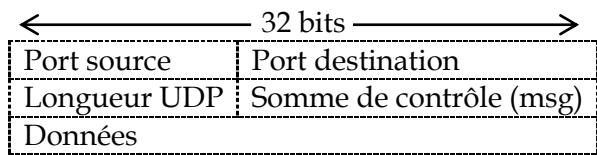
4 = autorisation des acquittements sélectifs

8 = estampilles temporelles

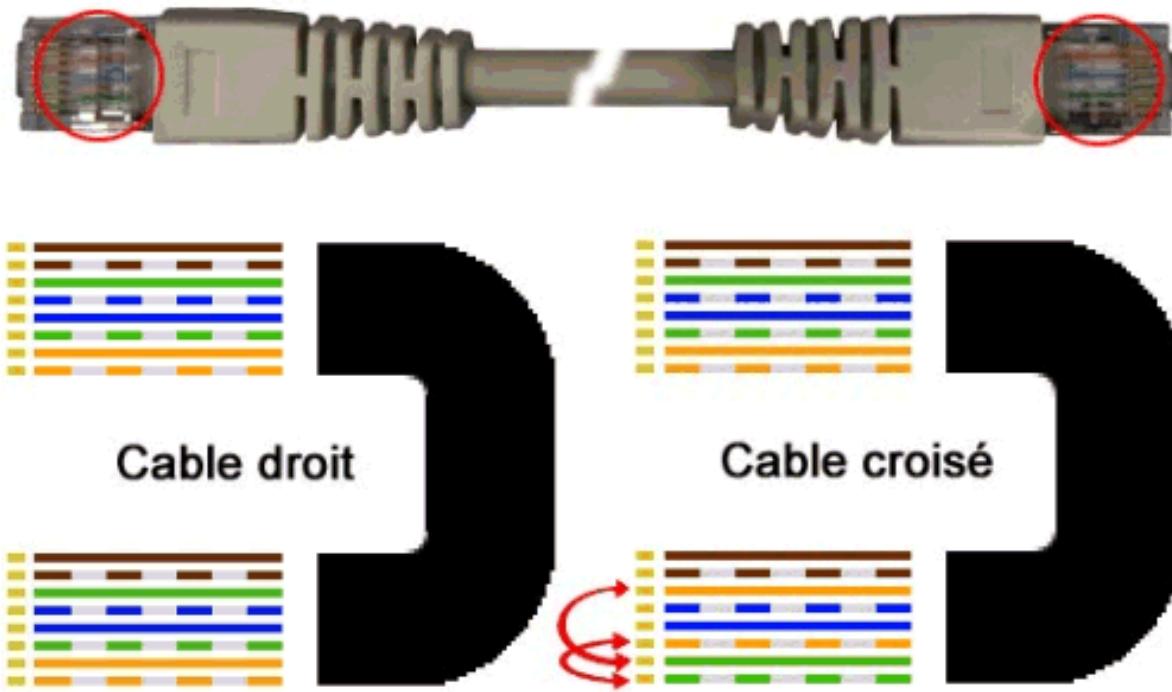
L = un octet longueur (nombre d'octet total)

V = valeur de l'option

### STRUCTURE DE SEGMENT UDP



## COMMENT FAIRE UN CORDON DROIT ET CROISE



## PUISANCE DE 2

|          |          |
|----------|----------|
| $2^0$    | 1        |
| $2^1$    | 2        |
| $2^2$    | 4        |
| $2^3$    | 8        |
| $2^4$    | 16       |
| $2^5$    | 32       |
| $2^6$    | 64       |
| $2^7$    | 128      |
| $2^8$    | 256      |
| $2^9$    | 512      |
| $2^{10}$ | 1024     |
| $2^{11}$ | 2048     |
| $2^{12}$ | 4096     |
| $2^{13}$ | 8192     |
| $2^{14}$ | 16384    |
| $2^{15}$ | 32768    |
| $2^{16}$ | 65536    |
| $2^{17}$ | 131072   |
| $2^{18}$ | 262144   |
| $2^{19}$ | 524288   |
| $2^{20}$ | 10048576 |

Et n'oubliez pas : dans 99% des cas, le problème se situe entre le clavier et le dossier de la chaise !

## CONVERSION DECIMAL / HEXADECIMAL / OCTAL / BINAIRE

---

| Décimal | Hexadécimal | Octal | Binaire |
|---------|-------------|-------|---------|
| 0       | 0           | 000   | 0000    |
| 1       | 1           | 001   | 0001    |
| 2       | 2           | 002   | 0010    |
| 3       | 3           | 003   | 0011    |
| 4       | 4           | 004   | 0100    |
| 5       | 5           | 005   | 0101    |
| 6       | 6           | 006   | 0110    |
| 7       | 7           | 007   | 0111    |
| 8       | 8           | 010   | 1000    |
| 9       | 9           | 011   | 1001    |
| 10      | A           | 012   | 1010    |
| 11      | B           | 013   | 1011    |
| 12      | C           | 014   | 1100    |
| 13      | D           | 015   | 1101    |
| 14      | E           | 016   | 1110    |
| 15      | F           | 017   | 1111    |

## MASQUE DE SOUS-RESEAU

---

| /   | Masque de sous-réseau | Maque générique * | Nombre de machines                       |
|-----|-----------------------|-------------------|------------------------------------------|
| /8  | 255.0.0.0             | 0.255.255.255     | $2^{24} = 16777216 - 2 \text{ machines}$ |
| /9  | 255.128.0.0           | 0.127.255.255     | $2^{23} = 8388608 - 2 \text{ machines}$  |
| /10 | 255.192.0.0           | 0.63.255.255      | $2^{22} = 4194304 - 2 \text{ machines}$  |
| /11 | 255.224.0.0           | 0.31.255.255      | $2^{21} = 2097152 - 2 \text{ machines}$  |
| /12 | 255.240.0.0           | 0.15.255.255      | $2^{20} = 1048576 - 2 \text{ machines}$  |
| /13 | 255.248.0.0           | 0.7.255.255       | $2^{19} = 524288 - 2 \text{ machines}$   |
| /14 | 255.252.0.0           | 0.3.255.255       | $2^{18} = 262144 - 2 \text{ machines}$   |
| /15 | 255.254.0.0           | 0.1.255.255       | $2^{17} = 131072 - 2 \text{ machines}$   |
| /16 | 255.255.0.0           | 0.0.255.255       | $2^{16} = 65536 - 2 \text{ machines}$    |
| /17 | 255.255.128.0         | 0.0.127.255       | $2^{15} = 32768 - 2 \text{ machines}$    |
| /18 | 255.255.192.0         | 0.0.63.255        | $2^{14} = 16384 - 2 \text{ machines}$    |
| /19 | 255.255.224.0         | 0.0.31.255        | $2^{13} = 8192 - 2 \text{ machines}$     |
| /20 | 255.255.240.0         | 0.0.15.255        | $2^{12} = 4096 - 2 \text{ machines}$     |
| /21 | 255.255.248.0         | 0.0.7.255         | $2^{11} = 2048 - 2 \text{ machines}$     |
| /22 | 255.255.252.0         | 0.0.3.255         | $2^{10} = 1024 - 2 \text{ machines}$     |
| /23 | 255.255.254.0         | 0.0.1.255         | $2^9 = 512 - 2 \text{ machines}$         |
| /24 | 255.255.255.0         | 0.0.0.255         | $2^8 = 256 - 2 \text{ machines}$         |
| /25 | 255.255.255.128       | 0.0.0.127         | $2^7 = 128 - 2 \text{ machines}$         |
| /26 | 255.255.255.192       | 0.0.0.63          | $2^6 = 64 - 2 \text{ machines}$          |
| /27 | 255.255.255.224       | 0.0.0.31          | $2^5 = 32 - 2 \text{ machines}$          |
| /28 | 255.255.255.240       | 0.0.0.15          | $2^4 = 16 - 2 \text{ machines}$          |
| /29 | 255.255.255.248       | 0.0.0.7           | $2^3 = 8 - 2 \text{ machines}$           |
| /30 | 255.255.255.252       | 0.0.0.3           | $2^2 = 4 - 2 \text{ machines}$           |

\* Uniquement quand l'espace d'adressage est contiguë

## TABLES DE VERITE

| Table de vérité de ET |   |        |
|-----------------------|---|--------|
| a                     | b | a ET b |
| 0                     | 0 | 0      |
| 0                     | 1 | 0      |
| 1                     | 0 | 0      |
| 1                     | 1 | 1      |

| Table de vérité de OU |   |        |
|-----------------------|---|--------|
| a                     | b | a OU b |
| 0                     | 0 | 0      |
| 0                     | 1 | 1      |
| 1                     | 0 | 1      |
| 1                     | 1 | 1      |

| Table de vérité XOR (OU EXCLUSIF) |   |         |
|-----------------------------------|---|---------|
| a                                 | b | a XOR b |
| 0                                 | 0 | 0       |
| 0                                 | 1 | 1       |
| 1                                 | 0 | 1       |
| 1                                 | 1 | 0       |

## TABLE ASCII

**A S C I I**

|            |  | 0 | 0 | 0 | 0 | 1 | 1       | 1        | 1   |
|------------|--|---|---|---|---|---|---------|----------|-----|
|            |  | 0 | 0 | 1 | 1 | 0 | 0       | 1        | 1   |
|            |  | 0 | 1 | 0 | 1 | 0 | 1       | 0        | 1   |
|            |  | 0 | 1 | 2 | 3 | 4 | 5       | 6        | 7   |
|            |  | 0 | 0 | 0 | 0 | 0 | NUL     | TC7/DLE  | SP  |
| Poids fort |  | 0 | 0 | 0 | 1 | 1 | !       | 1        | A   |
|            |  | 0 | 0 | 1 | 0 | 2 | TC1/SOH | DC1/XON  | Q   |
|            |  | 0 | 0 | 1 | 1 | 3 | TC2/STX | DC2      | a   |
|            |  | 0 | 1 | 0 | 0 | 4 | TC3/ETX | DC3/XOFF | q   |
|            |  | 0 | 1 | 0 | 1 | 5 | TC4/EOT | DC4      | b   |
|            |  | 0 | 1 | 1 | 0 | 6 | TC5/ENQ | DC5/NAK  | r   |
|            |  | 0 | 1 | 1 | 1 | 7 | TC6/ACK | DC6/SYN  | s   |
|            |  | 1 | 0 | 0 | 0 | 8 | BEL     | TC10/ETB | c   |
|            |  | 1 | 0 | 0 | 1 | 9 | FE0/BS  | CAN      | t   |
|            |  | 1 | 0 | 1 | 0 | A | FE1/HT  | EM       | d   |
|            |  | 1 | 0 | 1 | 1 | B | FE2/LF  | SUB      | e   |
|            |  | 1 | 1 | 0 | 0 | C | FE3/VT  | ESC      | u   |
|            |  | 1 | 1 | 0 | 1 | D | FE4/FF  | IS4/FS   | f   |
|            |  | 1 | 1 | 1 | 0 | E | FE5/CR  | IS3/GS   | v   |
|            |  | 1 | 1 | 1 | 1 | F | SO      | IS2/RS   | y   |
|            |  |   |   |   |   |   | SI      | IS1/US   | z   |
|            |  |   |   |   |   |   |         |          | DEL |

## DESCRIPTION DES BEEP EMIS LORS DU DEMARRAGE DU PC

---

Le beep est un signal sonore envoyé par le BIOS de la carte mère au démarrage du PC. Selon les séquences de beep, ceci permet de déterminer les erreurs rencontrées au boot et de les dépanner. Les beep dépendent du BIOS installés sur la carte mère. Le type de BIOS est généralement noté sur l'EPROM ou la Flash ROM, même si ceci peut varier d'un fabriquant d'ordinateur à l'autre.

### Beep BIOS AMI

| Beep Code               | Description                                        |
|-------------------------|----------------------------------------------------|
| <b>1 court</b>          | Erreur de rafraîchissement de la mémoire           |
| <b>2 courts</b>         | Erreur de parité mémoire                           |
| <b>3 courts</b>         | Mémoire de base 64 KB en défaut (ROM)              |
| <b>4 courts</b>         | Erreur du circuit d'horloge interne                |
| <b>5 courts</b>         | Erreur de processeur                               |
| <b>6 courts</b>         | Contrôleur port clavier A20 en erreur              |
| <b>8 courts</b>         | Erreur mémoire carte écran                         |
| <b>9 courts</b>         | Erreur checksum de la mémoire ROM de la carte mère |
| <b>10 courts</b>        | Erreur mémoire CMOS du setup (→ clear CMOS)        |
| <b>11 courts</b>        | Erreur mémoire cache                               |
| <b>1 long, 3 courts</b> | Erreur mémoire (pas implantée, en panne)           |
| <b>1 long, 8 courts</b> | Carte graphique défectueuse, mal enfoncee          |

### Beep PHOENIX - AWARD

| Beep Code                  | Description                                                 |
|----------------------------|-------------------------------------------------------------|
| <b>1 court</b>             | Démarrage normal (sans erreur)                              |
| <b>3 courts</b>            | Erreur CMOS, Setup mal configuré (→ clear CMOS)             |
| <b>1 long, 1 court</b>     | Erreur mémoire RAM                                          |
| <b>1 long, 2 courts</b>    | Erreur d'initialisation de la carte graphique               |
| <b>1 long, 3 courts</b>    | Erreur d'initialisation du clavier                          |
| <b>1 long, 9 courts</b>    | Erreur de mémoire ROM (BIOS)                                |
| <b>Long beep continu</b>   | Problème de mémoire (généralement mal connectée ou absente) |
| <b>Beep courts continu</b> | Alimentation défectueuse                                    |

### Beep IBM

| Beep Code                                             | Description                                             |
|-------------------------------------------------------|---------------------------------------------------------|
| <b>Pas de beep</b>                                    | Pas d'alimentation                                      |
| <b>1 beep court</b>                                   | Démarrage normal                                        |
| <b>Beep continu ou beep répétitifs</b>                | Problème d'alimentation, carte mal enfoncee dans un bus |
| <b>1 beep long, 1 beep court</b>                      | Erreur de carte mère                                    |
| <b>3 beep longs</b>                                   | Erreur clavier                                          |
| <b>1 beep, pas d'affichage ou affichage incorrect</b> | Erreur de la carte écran                                |

## SITES UTILES AUX TSRIT

---

- <http://security.practitioner.com/>
- <http://www.developpez.net/forums/f177/systemes/autres-systemes/reseaux/>
- <http://standards.iso.org/iso/>
- <http://gallica.bnf.fr/>
- <http://www.gns3.net/>
- <http://www.rfc-editor.org/>
- <http://www.iana.org/>
- <http://www.ieee.org/index.html>
- <http://www.cisco.com/web/learning/netacad/index.html>
- [http://www.editions-eni.fr/Livres/andre-Vaucamps/.7\\_3a6222cf-b921-41f5-886c-c989f77ba994\\_78796316-671e-4312-a8f6-9c0ba69d1893\\_1\\_0\\_0\\_0\\_d9bd8b5e-f324-473fb1fc-b41b421c950f.html](http://www.editions-eni.fr/Livres/andre-Vaucamps/.7_3a6222cf-b921-41f5-886c-c989f77ba994_78796316-671e-4312-a8f6-9c0ba69d1893_1_0_0_0_d9bd8b5e-f324-473fb1fc-b41b421c950f.html)
- <http://tsrit.perso.sfr.fr>