**BACCALAUREAT PROFESSIONNEL**

**MICRO INFORMATIQUE ET RÉSEAUX :**

**INSTALLATION ET MAINTENANCE**

# EPREUVE E1

## Epreuve scientifique et technique

## SOUS-EPREUVE E11

## Etude des supports et protocoles de communication

**Ce dossier comprend 24 pages numérotées de *1/24* à *24/24*, dont :**



**A rendre obligatoirement avec votre copie**

**les feuilles document réponse :**

**DOCUMENTS REPONSE 1 à 7 (pages 22 à 24)**

# BARÈME :

| | |
|---|---|
| **PARTIE A : CABLAGE** | **44 points** |
| **PARTIE B : ADRESSAGE IP** | **56 points** |
| **PARTIE C : ETUDE DU ROUTEUR XFW** | **58 points** |
| **PARTIE D : RESOLUTION DNS** | **42 points** |

**Barème sur 200 points pour un coefficient 3**

**Dans cette épreuve, vous allez travailler sur le réseau de l'entreprise PAPYRUS présenté en annexe 1.**

## PARTIE A : CABLAGE

**A1.** D'après l'annexe 2 , citez les différentes mesures effectuées par la certification.

**A2.** Quel est le type du câble testé ?

**A3.** Relever la valeur du NVP et définissez ce paramètre.

**A4. Calcul de la longueur du câble**

**A4.1.** Quelle relation existe-t-il entre le NVP et la longueur du câble ? (Vitesse de la lumière : C = 300 000 Km/s)

**A4.2** Pour la paire 1-2, retrouvez par le calcul la longueur du câble affichée par l'appareil de certification.

**A5.** Lors d'une autre mesure, le certificateur indique : "SPLIT PAIR" (Cf.ANNEXE 4)

Voici la cartographie du câble utilisé :

| Numéro du fil (extrémité 1) | couleur | Numéro du fil |
|---|---|---|
| 1 | Blanc/orange | 1 |
| 2 | Orange | 2 |
| 3 | Blanc/vert | 3 |
| 4 | Vert | 4 |
| 5 | Blanc/bleu | 5 |
| 6 | Bleu | 6 |
| 7 | Blanc/marron | 7 |
| 8 | Marron | 8 |

**A5.1.** A quoi correspond le défaut "SPLIT PAIR" ?

**A5.2.** Pour éliminer le défaut "SPLIT PAIR", remplissez le document réponse 1 en respectant l'ordre des couleurs suivant :

- paire orange sur la paire 1
- paire verte sur la paire 2
- paire bleue sur la paire 3
- paire marron sur la paire 4

**A6.** Vous devez relier 2 concentrateurs (HUB) dotés de ports n'ayant pas la technologie de la reconnaissance automatique de type de câble, ni de port de cascade. Représentez sur le document réponse 2 la cartographie du câble à utiliser.

**A7.** Vous allez travailler sur le réseau d'une grosse agence présentée en annexe 5.

Si les trames T1 à T4 (tableau ci-dessous) traversent le commutateur A, quelles seront les adresses apprises par le commutateur de l'agence?

Les tables de commutation sont vides au moment où la première trame circule sur le réseau.
**Remplir le document réponse 3**

| Trames | Adresse destination MAC | Adresse source MAC | Adresse source IP | Adresse destination IP |
|---|---|---|---|---|
| T1 | FF :FF :FF :FF :FF | 02 :60 :8C :01 :01 | 192.168.1.1 | 192.168.1.2 |
| T2 | 02 :60 :8C :01 :01 | 02 :60 :8C :01 :04 | 192.168.1.4 | 192.168.1.1 |
| T3 | 02 :60 :8C :01 :01 | 02 :60 :8C :01 :02 | 192.168.1.2 | 192.168.1.1 |
| T4 | FF :FF :FF :FF :FF | 02 :60 :8C :01 :03 | 192.168.1.3 | 192.168.1.1 |

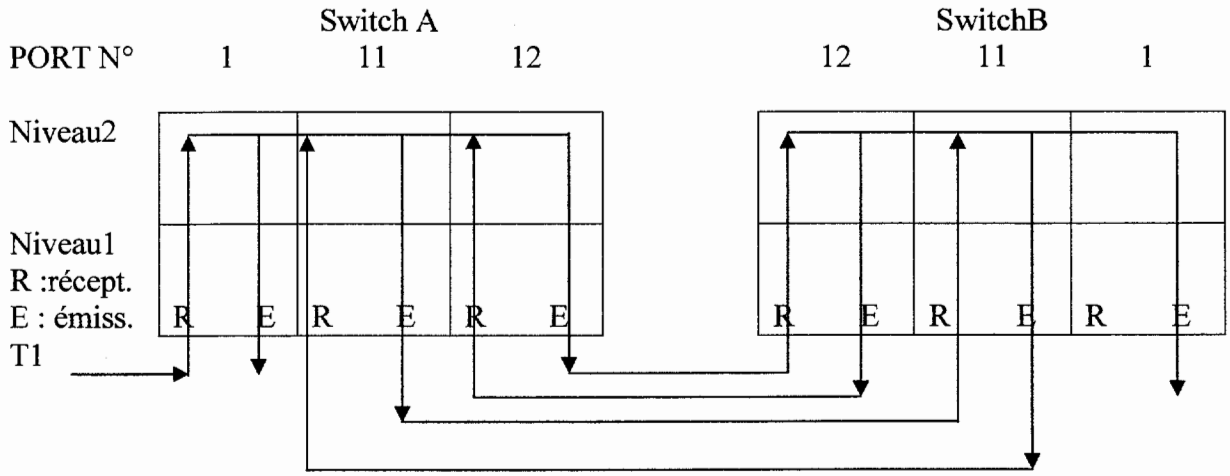
**A8.** Les liens 11 et 12 des deux commutateurs sont des liens doubles ou redondants.
Quels sont les intérêts d'employer ce type de lien ?

**A9.** Parmi les solutions A, B, C, proposées en page suivante, dites lesquelles utilisent un protocole d'aiguillage supplémentaire (en plus de celui utilisé par le commutateur).
Les liens 11 et 12 des deux commutateurs sont interconnectés par deux câbles ethernet.
Aidez-vous de l'annexe 3.

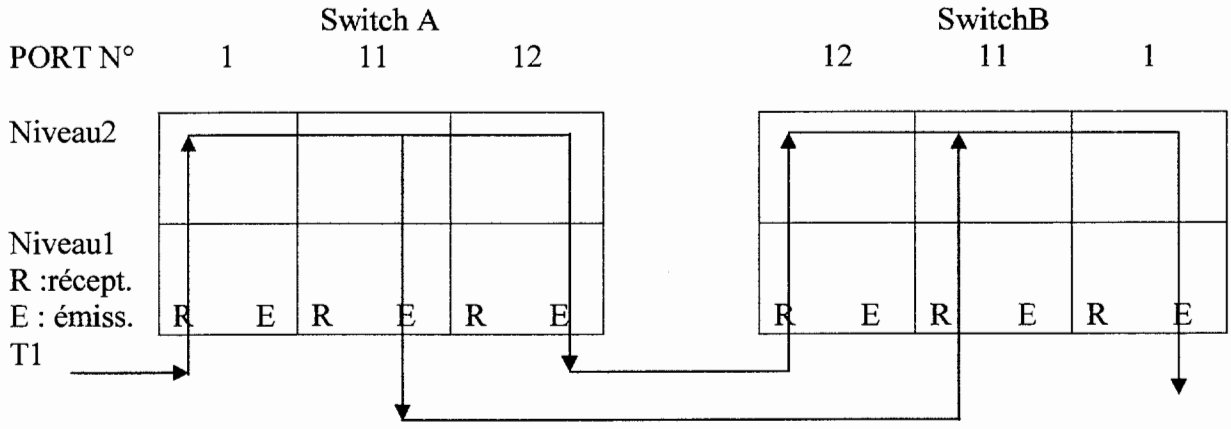
**A10.** Quel est l'inconvénient de ne pas utiliser de protocole d'aiguillage supplémentaire ?

Les schémas suivants représentent la circulation d'une trame entre le port 1 du switch A et le port 1 du switch B. Les switchs sont interconnectés par deux câbles ethernet entre les ports 11 et 12.

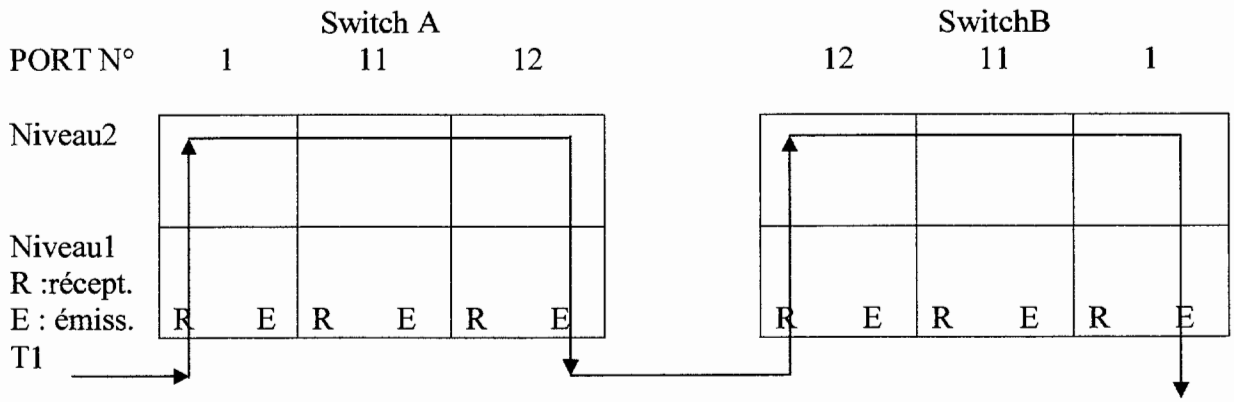
**SOLUTION A**




**SOLUTION B**




**SOLUTION C**



# PARTIE B : ADRESSAGE IP

**B1.** En fonction de l'annexe 7, retrouvez les différentes plages d'adresse IP en fonction de leur classe. (classe A, B et C)

**B2.** En fonction du réseau présenté en annexe 1, donnez le nombre de sous-réseaux reliés à la machine nommée XFW (firewall) et associez leur adresse IP et leur masque respectif.

**B3.** En fonction de l'annexe 6, citez les différents types d'adressage retenus par l'entreprise. Ce choix vous parait-t-il judicieux ? Dites pourquoi.

**B4.** Un utilisateur souhaite consulter le site WEB (www.qcmpub.fr) ayant pour adresse **193.156.3.1** à partir de la **machine PICTA HTTP.**
La passerelle pour sortir sur Internet est le routeur XWF.

**B4.1.** Donnez les paramètres réseaux à configurer sur la machine **PICTA HTTP** ?

**B4.2.** Décrivez comment la station va déterminer si l'adresse de destination est sur son réseau IP. Donnez le résultat.

**B4.3.** Décrivez la résolution ARP dans le document réponse 4, en considérant que toutes les mémoires caches ARP sont vides. Aidez-vous de l'annexe 5.

**B5.** Maintenant, l'utilisateur souhaite consulter le site WEB (www.schollpub.fr ) dont l'adresse IP est **128.156.10.10.**

**B5.1.** Décrivez comment la station va déterminer si l'adresse de destination est sur son réseau IP. Donnez le résultat.

**B5.2.** Expliquez pourquoi la résolution ARP ne donnera pas de résultat et pourquoi la connexion ne s'effectuera pas.

**B6.** L'administrateur vous donne l'adresse réseau 192.168.33.0/24 (masque sur 24 bits) à partager en plusieurs sous-réseaux. Il y aura 30 machines au maximum par sous-réseau.

**B6.1.** Combien de bits faudra-t-il réserver pour adresser vos machines ? En déduire le nombre de bits pour coder vos sous-réseaux.

**B6.2.** Sans tenir compte des recommandations sur le choix des adresses de sous-réseaux, combien pourrez-vous déclarer de sous-réseaux au maximum ? Expliquez votre calcul.

**B6.3.** Calculez le masque de sous-réseau.

**B6.4.** Remplir le tableau du document réponse 5 (Adresses IP des sous-réseaux).

**B7.** Après avoir configuré toutes les machines, l'ordinateur PICTA PHOTO n'est plus accessible à partir d'une station d'un autre sous-réseau (exemple XPI). Sa configuration est la suivante :

| | |
|---|---|
| IP | : 192.168.33.17 |
| Masque | : 255.255.255.0 |
| Passerelle | : 192.168.33.30 |

Remarque : les adresses des passerelles sont les dernières de chaque sous-réseau.

**B7.1.** Donnez la configuration correcte pour que cette machine soit de nouveau accessible à partir d'une station d'un autre sous-réseau.

**B7.2.** A quel sous-réseau cet ordinateur appartient-il ?

# PARTIE C : ETUDE DU ROUTEUR XFW

Se reporter aux annexes 1, 8 et 9.

La société de presse Papyrus utilise le routeur XFW (modèle : CISCO 4500) pour

- connecter son réseau intranet à l'Internet.
- interconnecter les sous-réseaux de l'intranet.

Les interfaces de ce routeur sont les passerelles des sous-réseaux auxquelles elles sont connectées.

Les journalistes, correspondants et agences régionales ont des accès aux ressources (messagerie, FTP, WEB ...) de la société PAPYRUS.

## C1. Etude du NAT/PAT :

La société dispose d'un pool de six adresses IP publiques gérée par l'IANA.
Une adresse publique est réservée pour le serveur de messagerie XMESS et une autre pour le serveur XLDAP (carnet d'adresses, FTP, DNS, antivirus).

Pour accéder à Internet les paquets IP passeront par l'interface « e0 » du routeur dont l'adresse IP publique est 195.151.64.226.

**C1.1.** A partir d'Internet, peut-on joindre le serveur de messagerie ? Dites pourquoi ?

**C1.2.** Quelle est la fonction supplémentaire que doit remplir le routeur XFW pour que le serveur de messagerie soit accessible depuis Internet ? Justifier votre réponse ?

**C1.3.** Lorsqu'on accède à Internet, que se passe-t-il lorsque la totalité du pool d'adresses IP publique est utilisé ?

**C1.4.** Quelle autre fonction doit-on mettre en œuvre pour que toutes les stations aient toujours accès à Internet sans problèmes?

## C2. Etude de la table de routage de XFW :

On souhaite que les postes situés en agences puissent :

- rapatrier les Emails provenant du serveur XMESS,
- accéder aux serveurs PICTA,
- accéder aux serveurs de fichiers situés sur le réseau 172.17.170.0,
- sortir sur Internet.

Remarque : le cœur de réseau est constitué d'un routeur (modèle: passport 8600) l'adresse IP de l'interface eth0 est 128.156.100.210

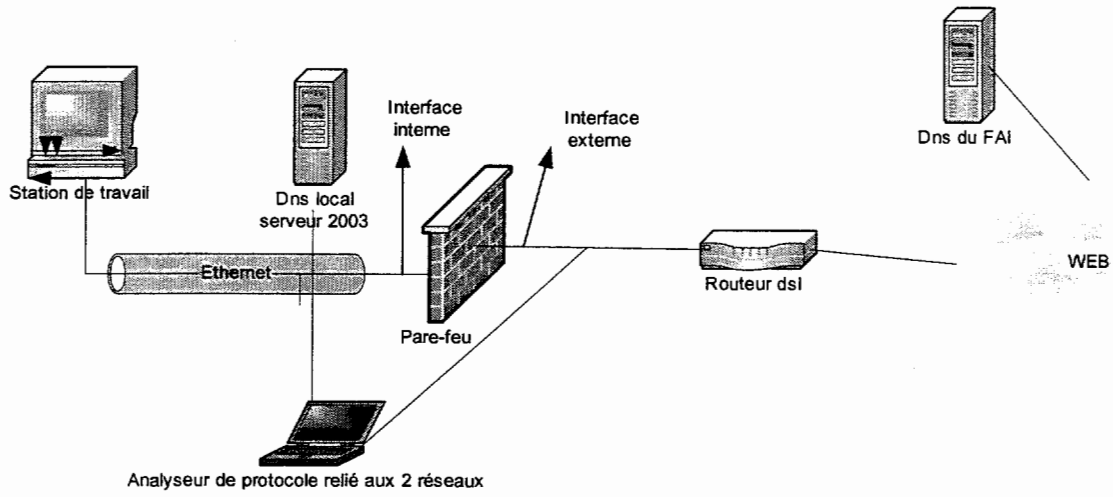
**C2.1** En vous aidant de l'annexe 1 et en respectant les conditions précédentes, vous devez compléter le document réponse 6.

**C2.2** Quelle est l'avantage du routage dynamique par rapport au routage statique?

**C2.3** L'administrateur décide de mettre en place un protocole de routage sur tous les routeurs de la société. Le protocole de routage utilisé par les routeurs est RIP version 2.
Justifier ce choix, par rapport à RIP version 1.

# PARTIE D: Résolution DNS.

Soit le schéma du réseau d'une agence, suivant :




On se propose d'étudier la procédure de résolution de nom FQDN, lorsque la station de travail accède au site **www.ulb.ac.be.**
Vous disposez des documents nécessaires à votre étude en annexe 10 et 11.

Voici la capture réalisée par un analyseur situé en amont et en en aval du pare-feu :

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.33.121 | Broadcast | ARP | Who has 192.168.33.253? Tell 192.168.33.121 |
| 2 | 0.000153 | 192.168.33.253 | 192.168.33.121 | ARP | 192.168.33.253 is at 00:04:75:c2:03:ad |
| 3 | 0.000182 | 192.168.33.121 | 192.168.33.253 | DNS | Standard query A www.ulb.ac.be |
| 4 | 0.000435 | 192.168.33.253 | Broadcast | ARP | Who has 192.168.33.254? Tell 192.168.33.253 |
| 5 | 0.000661 | 192.168.33.254 | 192.168.33.253 | ARP | 192.168.33.254 is at 00:02:b6:15:4c:2e |
| 6 | 0.000671 | 192.168.33.253 | 194.199.33.1 | DNS | Standard query A www.ulb.ac.be |
| 7 | 0.001116 | 10.133.128.252 | 194.199.33.1 | DNS | Standard query A www.ulb.ac.be |
| 8 | 0.050102 | 194.199.33.1 | 10.133.128.252 | DNS | Standard query response A 164.15.59.215 |
| 9 | 0.050519 | 194.199.33.1 | 192.168.33.253 | DNS | Standard query response A 164.15.59.215 |
| 10 | 0.050641 | 192.168.33.253 | 192.168.33.121 | DNS | Standard query response A 164.15.59.215 |
| 11 | 0.052868 | 192.168.33.121 | Broadcast | ARP | Who has 192.168.33.254? Tell 192.168.33.121 |
| 12 | 0.053289 | 192.168.33.254 | 192.168.33.121 | ARP | 192.168.33.254 is at 00:02:b6:15:4c:2e |
| 13 | 0.053319 | 192.168.33.121 | 164.15.59.215 | TCP | 1507 > http [SYN] Seq=0 Ack=0 Win=25200 Len=0 |
| 14 | 0.053848 | 10.133.128.252 | 164.15.59.215 | TCP | 1507 > http [SYN] Seq=0 Ack=0 Win=25200 Len=0 |
| 15 | 0.053949 | 164.15.59.215 | 10.133.128.252 | TCP | http > 1507 [SYN, ACK] Seq=0 Ack=1 Win=5840 |
| 16 | 0.054420 | 164.15.59.215 | 192.168.33.121 | TCP | http > 1507 [SYN, ACK] Seq=0 Ack=1 Win=5840 |
| 17 | 0.054486 | 192.168.33.121 | 164.15.59.215 | TCP | 1507 > http [ACK] Seq=1 Ack=1 Win=25200 Len=0 |

D-1 En analysant les échanges capturés par l'analyseur de protocole, complétez le document réponse 7 de manière à décrire sous forme de diagramme fléché uniquement les échanges liés au DNS.

D-2 Quel est l'adresse IP du serveur DNS qui a fait la résolution ? Expliquez pourquoi la requête a t-elle été résolue par ce serveur ?

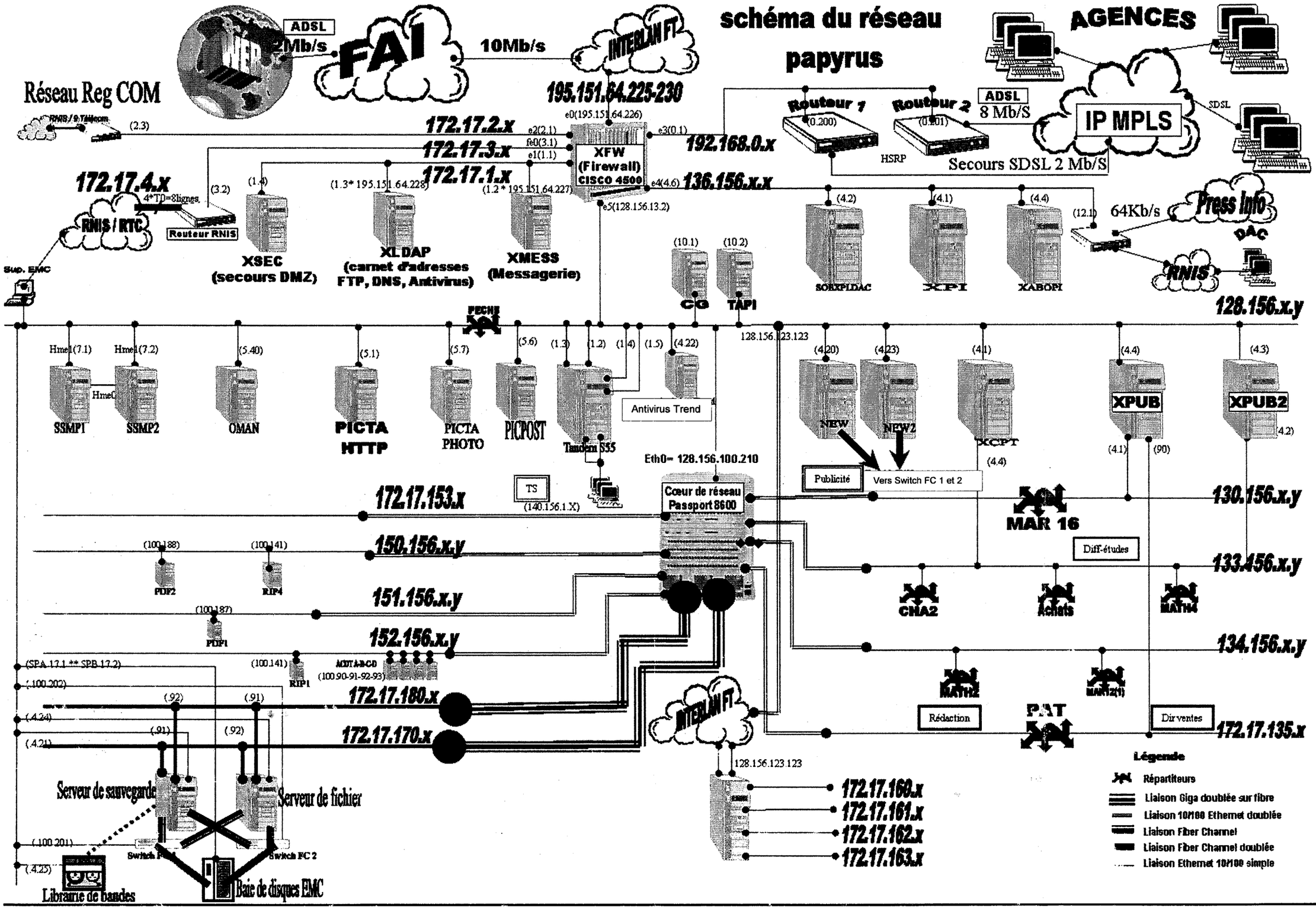
D-3 Donnez le type de requête DNS utilisé sur le serveur DNS local.

D-4 Situez dans le modèle TCP/IP (modèle D.O.D.) tous les protocoles utilisés lors de la résolution de nom.

# E11 Étude des supports et protocoles de communication

## ANNEXES

## ANNEXE 1 : ASCHEMA DU RESEAU PAIPRUS



ID Câble: 621-27
GSO
SITE: BORDEAUX BASTIDE
OPERATEUR:
Version des normes: 2.2
Version du logiciel: 2.2
NVP: 69.0%  SEUIL DE DETECTION D'ERREUR: 15%
TEST DE BLINDAGE/ECRAN: N/V

Résumé de test: CORRECT
MARGE DE SECURITE: 7.5 dB (NEXT 36-78)
Date / Heure: 02/08/2004  14:44:18
Norme de test: TIA Cat 5 Channel
Type de Câble: UTP 100 Ohm Cat 5
FLUKE DSP-4000  Num. Sér.: 7370038 LIA013
FLUKE DSP-4000SR Num. Sér.: 7370038 LIA012

Schéma de câblage CORRECT  Résult.  Broche RJ45: 1 2 3 4 5 6 7 8 B

Broche RJ45: 1 2 3 4 5 6 7 8 B

| Paire | Longueur (m) | Longueur Lim. | Délai de prop. ns | Délai de prop. Lim. | Divergen. de prop. ns | Divergen. de prop. Lim. | Résistance ohms | Résistance Lim. | Impédance ohms | Impédance Lim. | Impédance Anom. (m) | Atténuation Résult. (dB) | Atténuation Fréq. MHz | Atténuation Lim. (dB) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 55.2 | 100.0 | 267 | | 4 | 50 | | | 103 | 80-120 | | 11.5 | 100.0 | 24.0 |
| 36 | 54.4 | 100.0 | 263 | | 0 | 50 | | | 105 | 80-120 | | 11.6 | 100.0 | 24.0 |
| 45 | 55.4 | 100.0 | 268 | | 5 | 50 | | | 102 | 80-120 | | 11.6 | 100.0 | 24.0 |
| 78 | 54.6 | 100.0 | 264 | | 1 | 50 | | | 101 | 80-120 | | 11.5 | 100.0 | 24.0 |

| | Résultats du testeur | | | | | | Résultats de l'injecteur | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Marge la plus faible | | | Pire valeur | | | Marge la plus faible | | | Pire valeur | | |
| Paire NEXT | Résult. (dB) | Fréq. MHz | Lim. (dB) | Résult. (dB) | Fréq. MHz | Lim. (dB) | Résult. (dB) | Fréq. MHz | Lim. (dB) | Résult. (dB) | Fréq. MHz | Lim. (dB) |
| 12-36 | 41.5 | 69.8 | 29.8 | 41.5 | 69.8 | 29.8 | 46.4 | 38.0 | 34.2 | 40.5 | 93.2 | 27.7 |
| 12-45 | 46.5 | 35.6 | 34.8 | 42.3 | 80.2 | 28.8 | 66.1 | 3.6 | 51.3 | 45.6 | 87.4 | 28.1 |
| 12-78 | 56.1 | 11.9 | 42.8 | 43.3 | 99.4 | 27.2 | 48.0 | 32.0 | 35.6 | 42.1 | 86.4 | 28.2 |
| 36-45 | 60.7 | 4.5 | 49.7 | 42.8 | 63.8 | 30.5 | 60.5 | 4.3 | 50.1 | 40.2 | 82.0 | 28.6 |
| 36-78 | 35.5 | 88.6 | 28.0 | 35.5 | 88.6 | 28.0 | 37.3 | 82.0 | 28.6 | 37.3 | 82.0 | 28.6 |
| 45-78 | 42.8 | 45.4 | 33.0 | 41.1 | 89.2 | 28.0 | 47.1 | 24.8 | 37.5 | 40.5 | 84.0 | 28.4 |

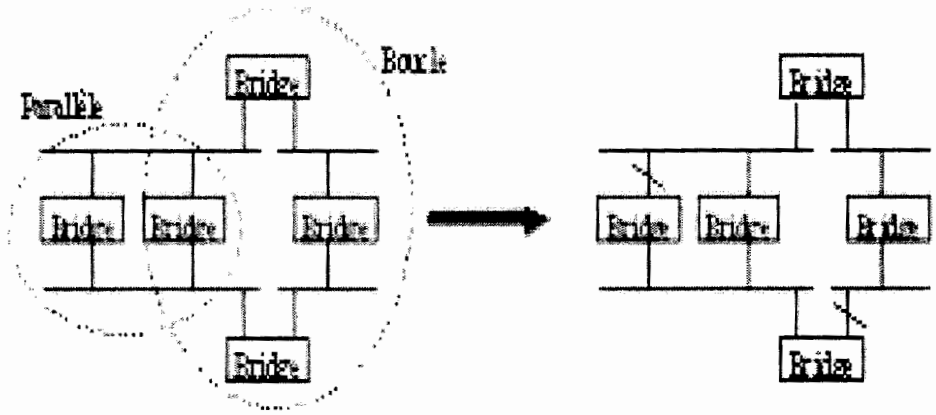
# ANNEXE 3 : SPANNING TREE

## Qu'est ce que le "Transparent Spanning Tree" ?

Si deux (2) bridges sont installés en parallèle, les conséquences sont fatales : chaque bridge retransmettant les "broadcasts" de l'autre, le trafic augmente car TOUS les broadcasts continuent à circuler. De plus, la réponse est de plus en plus lente et le "crash" du réseau est assuré.
En outre, une station DOIT se manifester pour pouvoir être connue du bridge (data base). C'est-à-dire qu'à la mise sous tension du bridge, toutes les trames sont retransmises sur tous les ports jusqu'à ce que les bases de données dynamiques soient définies par le processus d'auto apprentissage.

## Le "TRANSPARENT SPANNING TREE"

Le Transparent Spanning Tree a été défini pour éviter les problèmes de boucles et de bridges montés en parallèle. Si des boucles ou des bridges en parallèle sont présents, l'algorithme désactive les bridges non-nécessaires et crée alors une structure en "arbre".




L'idée générale est que la structure en arborescence puisse être influencée par l'administrateur du réseau pour qu'elle puisse être le mieux adaptée à la stratégie du réseau de l'entreprise. Le moyen d'influence est la priorité du bridge définie par l'administrateur .

# ANNEXE 4 : SPLIT PAIR

**Paires permutés (ou SPLIT PAIR)**

C'est un problème grave et fréquent qui n'est pas détectable par un simple contrôle de continuité. La section de câble a des paires permutées lorsque les deux conducteurs de la paire d'un câble sont connectées à des broches de connecteur qui ne forment pas une paire.

Par exemple, sur un jack modulaire, les broches 4 et 5 forment une paire ; il en va de même pour les broches 3 et 6. On parle de paires permutées lorsqu'une paire du câble est raccordée aux broches 3 et 4 et une autre paire aux broches 5 et 6, comme dans l'illustration ci-dessous.

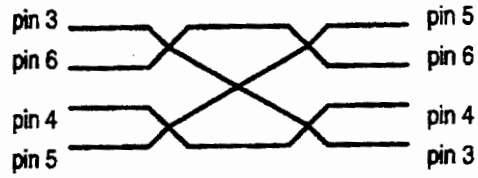
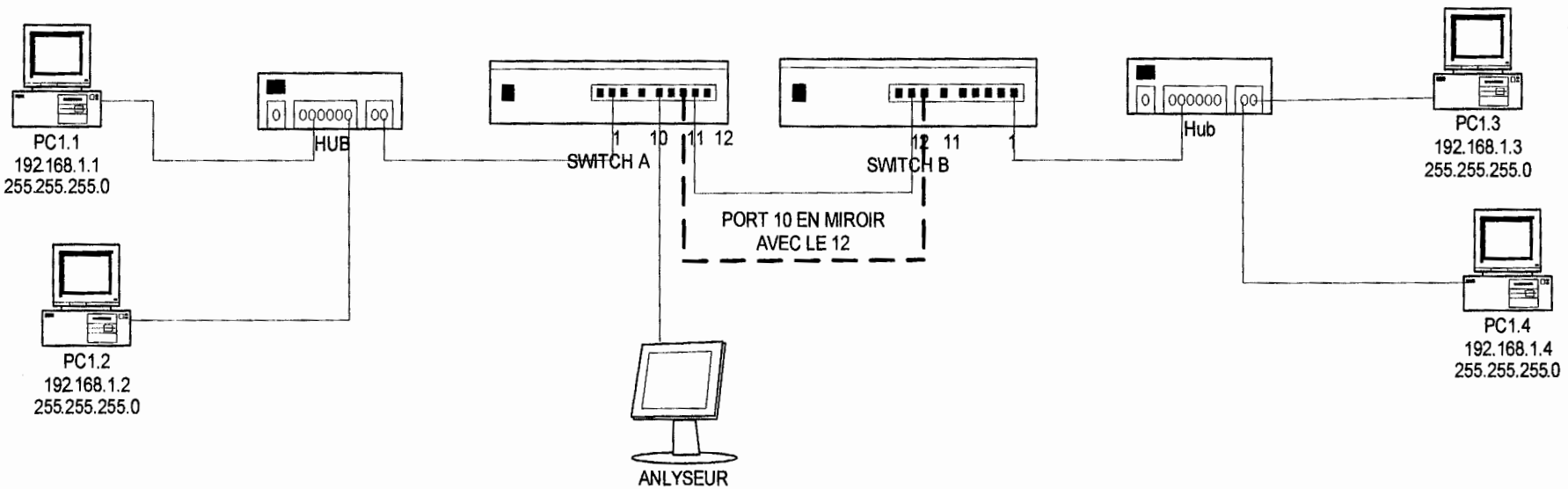



*Illustration Chapitre 5 -3 : Dans cet exemple, le test de continuité est correct, mais les conducteurs de paires torsadées sont permutés. Les outils qui ne testent que la continuité ne détectent pas ce problème sérieux et fréquent.*

Le WireScope vérifie et signale automatiquement la présence de paires permutées.

| |
|---|
| Si le WireScope vous signale des paires permutées, le câble testé est probablement inutilisable pour toute transmission de données à grande vitesse. |

# ANNEXE 5 : RESEAU D'UNE AGENCE



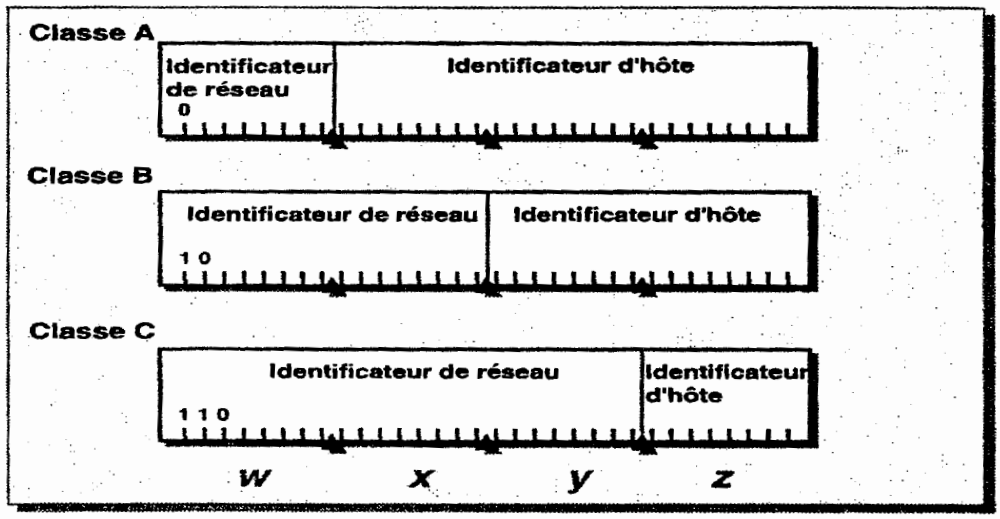

| Adresses IP | Adresses MAC |
|---|---|
| 128.156.6.1 | 08 :00 :5A :12 :45 :05 |
| 128.156.5.6 | 1F :44 :40 :55 :74 :12 |
| 128.156.13.2 | 00 :00 :0C :00 :1C:5F |
| 128.156.5.1 | 02 :60 :8C :01 :51 |
| 128.156.5.2 | 02 :60 :8C :02 :62 |

# ANNEXE 6 : RFC 1918

RFC 1918 Address Allocation for Private Internets February 1996 3.
Private Address Space The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:
10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

# ANNEXE 7 : CLASSE D'ADRESSES IPV4

| Classe | Adresse IP | Identificateur de réseau | Identificateur d'hôte |
|---|---|---|---|
| A | W.X.Y.z | w | x.y.z |
| B | W.X.V.z | W.X | y-z |
| c | w.x.y.z | w.x.y | z |



# ANNEXE 8 : NAT

## 1- NAT Statique

### a- Principe de fonctionnement

Le NAT statique consiste à associer une adresse IP privé à une adresse IP publique. Dans ce cas, la seule action qui sera effectuée par le routeur, sera de remplacer l'adresse source (sortante) par l'adresse de l'interface publique du routeur. En effet cette opération doit être effectuée puisqu'il est impossible de se connecter à Internet avec une adresse IP privé.

### b- Avantages et inconvénients

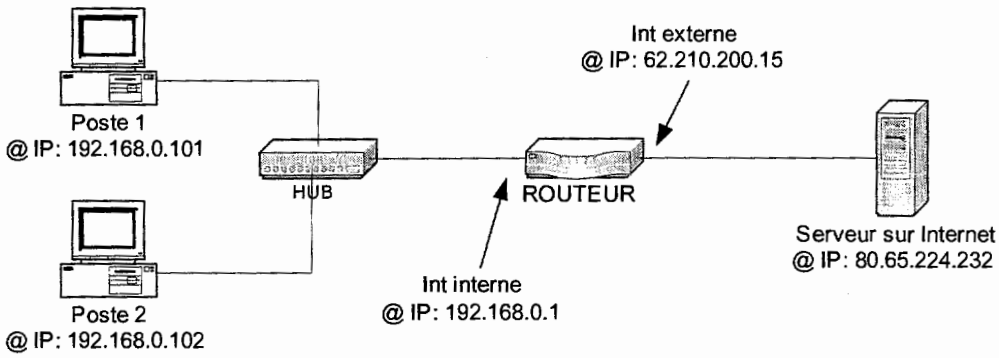
Le NAT statique permet à une machine possédant une adresse IP privée d'être vue sur Internet. Ceci est intéressant si l'on souhaite héberger des services vus de l'extérieur. Il permet également à un poste d'accéder à Internet.
En revanche, on s'aperçoit qu'il faut autant d'adresse publique que l'on souhaite avoir de poste relié à Internet. Cette méthode ne règle pas le problème posé, à savoir, la pénurie d'adresse publique. De plus, si l'on souhaite donner une adresse publique par machine, nous pourrions très bien lui donner cette adresse directement plutôt que de lui affecter une adresse privée et de passer par un routeur.

## 2- NAT Dynamique

### a- Principe de fonctionnement

Le NAT dynamique est aussi appelé **IP masquerading**. Il consiste à associer une adresse IP publique à plusieurs adresses IP privées. On dit que l'on masque les adresses privées.

Prenons le schéma suivant :




Lorsque le poste 1 appartenant au réseau local souhaite accéder sur le site WEB 80.65.224.232, il envoie une requête au socket 80.65.224.232:80. En fait, la requête est envoyée à la passerelle (puisque c'est le dispositif qui permet de sortir de notre réseau). Le routeur translate l'adresse IP privé du poste par l'adresse publique du routeur. Le serveur reçoit la requête et peut répondre, puisque l'adresse figurant dans le datagramme IP est une adresse IP publique (celle du routeur). La réponse arrive au routeur mais il n'est pas capable à ce stade là de réexpédier les données du poste 1. C'est grâce au port TCP (ou UDP) que le routeur va pouvoir remettre le paquet à l'initiateur de la requête. En effet, si une machine fait une requête avec comme port source 2345, le routeur saura que lorsqu'il recevra un paquet venant de l'extérieur avec ce port destination il faudra le réexpédier à cette machine.

Que se passe-t-il si deux postes du réseau local ouvrent en même temps un numéro de port identique ?
Le NAT dynamique prévoie ce genre de situation en translatant aussi le port du client (en plus de son adresse). Cette opération est appelée le **PAT** (Translation de port). En réalité, il remplace le port du client par un port qu'il choisit lui-même et étant donné que c'est lui qui choisi le nouveau port, il n'en prend jamais 2 identiques. Il garde ces informations de correspondance dans la table NAT. Ainsi, il pourra reconnaître les données qui arrive de l'extérieur par le port unique qu'il aura ouvert et qui correspond au port du client.

Le NAT dynamique permet de partager l'accès Internet à un grand nombre de machines (contrairement au NAT statique). Ceci permet de répondre au problème de la pénurie d'adresse publique.

En revanche il ne permet pas de rendre accessible un poste depuis l'extérieur. En effet, si cela fonctionne c'est parce que le routeur reçoit les informations depuis l'intérieur vers l'extérieur et le retour peut s'effectuer grâce à l'entrée (de correspondance) présente dans la table NAT. Il n'y aura aucune information dans cette table si la connexion est initiée depuis l'extérieur. Ceci n'est pas un inconvénient car il est possible de palier à ce problème et de plus cela permet d'améliorer la sécurité.

# ANNEXE 9 : PROTOCOLE DE ROUTAGE RIP

Routage Dynamique :

Un routeur configuré avec des routes dynamiques utilise un ou plusieurs protocoles de routage, qui ajustent automatiquement les routes en fonction des modifications de topologie ou de trafic.

| Propriété | Rip v1 | Rip v2 |
|---|---|---|
| Diffusion | Broadcast | Multicast 224.0.0.9 |
| Authentification | Non | Oui |
| Masque de Sous réseau | Non | Oui |
| Domaine de routage | Non | Oui |
| ID S.A. | Non | Oui |
| Next Hop | Non | Oui |
| Limitation | 15 sauts | 15 sauts |
| Nb d'entrées dans un message | 25 | 25 |

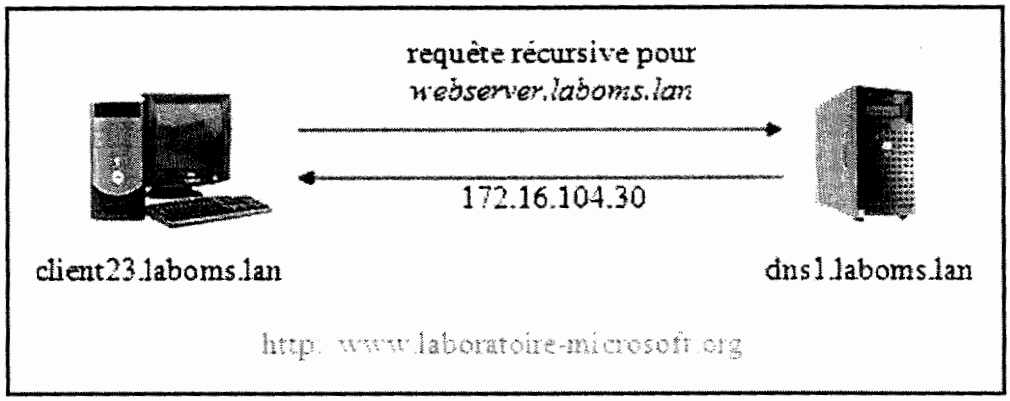
# ANNEXE 10 : DIFFERENTS TYPE DE REQUETTES DNS

Un serveur DNS peut recevoir deux types de requêtes DNS :

- **une requête récursive :** Lorsqu'un serveur DNS reçoit une requête récursive, il doit donner **la réponse la plus complète possible**. C'est pourquoi le serveur DNS est souvent amené à joindre d'autres serveurs de noms dans le but de trouver la réponse exacte.

- **une requête itérative :** Lorsqu'un serveur reçoit une requête itérative, il renvoie **la meilleure réponse qu'il peut donner sans contacter d'autres serveurs DNS** (c'est-à-dire en consultant uniquement sa propre base de données).

Lorsqu'une machine cliente envoie une requête à un serveur DNS (étape 3 de la résolution de nom d'hôte), elle est **toujours de type récursif.** Dans l'exemple ci-dessous, l'ordinateur client nommé *client23.laboms.lan* cherche l'adresse IP correspondant au nom d'hôte *webserver.laboms.lan.* C'est pourquoi il envoie une requête récursive au serveur DNS nommé *dns1.laboms.lan.* A partir de cet instant *dns1.laboms.lan* a pour obligation renvoyer une réponse au client. Pour cela il va chercher dans sa mémoire cache, puis la base de données qu'il héberge et va éventuellement contacter d'autres serveurs DNS. Une fois qu'il a obtenu la réponse (la réponse peut être négative), il la renvoie au client. Dans notre exemple, le serveur DNS a trouvé l'adresse IP recherchée qui est : *172.16.104.30.* L'ordinateur client peut ensuite contacter le serveur web nommé *webserver.laboms.lan.*




Lorsqu'un serveur DNS ne peut pas répondre à la requête récursive d'un client, **il va d'abord essayer de contacter ses redirecteurs**. Si le serveur DNS est paramétré pour utiliser des redirecteurs alors il envoie une requête récursive au premier serveur DNS défini dans sa liste de redirecteurs. Par contre, si le serveur DNS n'a pas de redirecteurs, il va envoyer une requête itérative au premier serveur DNS situé dans sa liste de serveur DNS racine. **Le serveurs DNS n'envoie donc des requêtes itératives que si il n'a pas de redirecteurs.**

Configuration des indications de racine :Lorsque le serveur DNS n'est pas configuré pour utiliser des redirecteurs, il se sert des indications de racine pour résoudre les noms d'hôtes ou les adresses IP appartenant à des zones qu'il n'héberge pas. Les indications de racine sont un ensemble de serveurs hébergeant la zone contenant les enregistrements du domaine racine ou domaine ".".

Les "serveurs DNS racines" sont au nombre de 13 à travers le monde. Il appartiennent tous à un même domaine nommé *root-servers.net.* Par défaut, le serveur DNS de Windows 2003 Server est configuré pour utiliser ces treize serveurs DNS. Cela signifie que si le serveur DNS reçoit une requête DNS dont il ignore la réponse, il va contacter un de ces serveurs racine pour l'obtenir.

Si l'on ne souhaite pas que les clients puissent résoudre les noms de domaines utilisés sur Internet, il suffit de ne mettre aucun serveur DNS dans la liste des serveurs racine ou bien de spécifier le nom d'hôte d'un serveur DNS local. On peut configurer les "serveurs DNS racine" dans l'onglet *Indication de racine* ( *clic droit / propriétés* sur le nom du serveur DNS dans la console MMC).

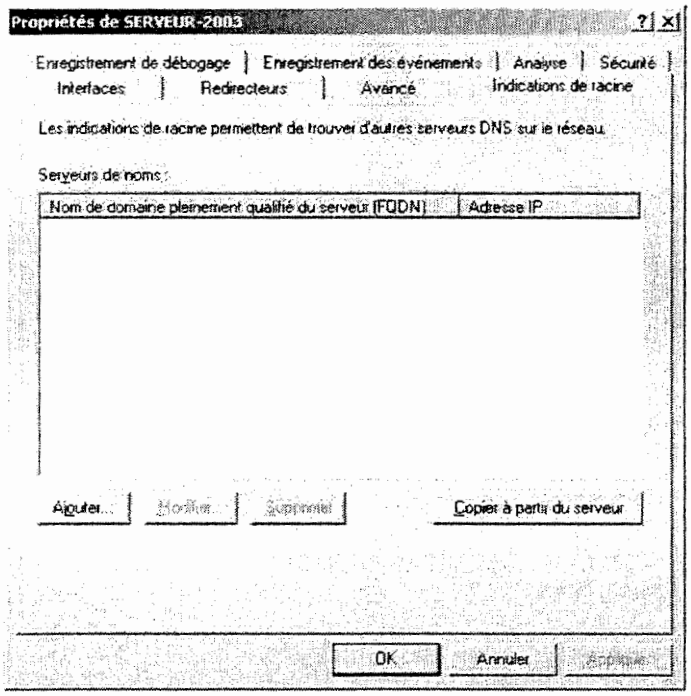
# ANNEXE 11 : CONFIGURATION DU SERVEUR DNS D'UNE AGENCE D'UN CLIENT

## Copie d'écran de la configuration de la station de travail d'une agence:

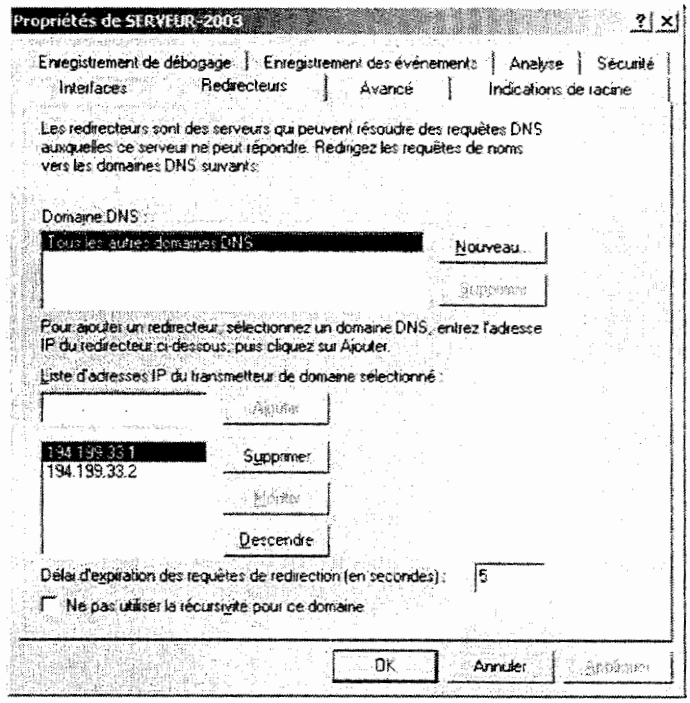
```
Carte Ethernet Connexion au réseau local:

        Description . . . . . . . . . . . : Carte Fast Ethernet compatible VIA
        Adresse physique . . . . . . . . . : 00-C0-9F-1D-47-FF
        DHCP activé. . . . . . . . . . . . : Oui
        Configuration automatique activée . . . . : Oui
        Adresse IP. . . . . . . . . . . . . : 192.168.33.121
        Masque de sous-réseau . . . . . . . : 255.255.255.0
        Passerelle par défaut . . . . . . . : 192.168.33.254
        Serveur DHCP. . . . . . . . . . . . : 192.168.33.253
        Serveurs DNS . . . . . . . . . . . . : 192.168.33.253
        Serveur WINS principal. . . . . . . : 192.168.33.253
        Serveur WINS secondaire . . . . . . : 192.168.33.252
        Bail obtenu . . . . . . . . . . . . : vendredi 1 octobre 2004 10:49:27
        Bail expirant . . . . . . . . . . . : vendredi 1 octobre 2004 14:49:27
```

## Copies d'écran des propriétés du serveur DNS d'une agence

### Configuration des indications de racine




### Configuration des redirecteurs



## DOCUMENT RÉPONSE 1 : QUESTION A.5.2

| Numéro du fil (extrémité 1) | couleur | | Numéro du fil |
|---|---|---|---|
| 1 | Blanc/orange | | 1 |
| 2 | | | 2 |
| 3 | | | 3 |
| 4 | | | 4 |
| 5 | | | 5 |
| 6 | | | 6 |
| 7 | | | 7 |
| 8 | | | 8 |

## DOCUMENT RÉPONSE 2 : QUESTIONA.6

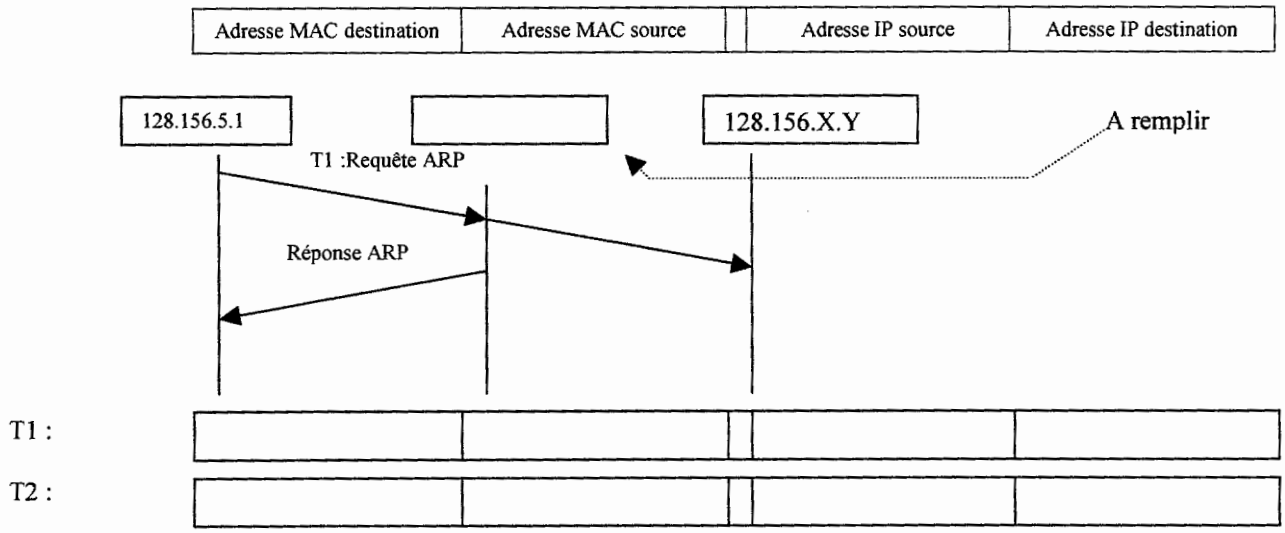
| Numéro du fil (extrémité 1) | couleur | | Numéro du fil |
|---|---|---|---|
| 1 | Blanc/orange | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |

## DOCUMENT RÉPONSE 3 : QUESTION A7

| Trames | Adresses apprises par le SWITCH A | Port du SWITCH A |
|---|---|---|
| T1 | | |
| T2 | | |
| T3 | | |
| T4 | | |
| T5 | | |

# DOCUMENT RÉPONSE 4 : QUESTION B4.3

Forme de la trame à remplir :




# DOCUMENT RÉPONSE 5 : QUESTION B6.4

| Adresse IP du sous-réseau | Première adresse | Dernière adresse | Adresse de diffusion du sous-réseau |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## DOCUMENT RÉPONSE 6 : TABLE DE ROUTAGE PARTIELLE DU ROUTEUR XFW

| Adresse destination | Masque | Interface de sortie | Prochain saut (Next hop ou passerelle) | Commentaire |
|---|---|---|---|---|
| | | | | Cette route permet aux stations des agences d'accéder au réseau du serveur de fichiers |
| | | | | Cette route permet aux stations des agences d'accéder à XMESS |
| | | | | Cette route permet aux stations des agences d'accéder au réseau des serveurs PICTA |
| | | | | Cette route permet l'accès à Internet |

## DOCUMENT RÉPONSE 7 : QUESTION D1

Complétez les champs manquants et complétez le diagramme temporel d'échanges en précisant la nature du protocole :

| Equipement : **Station de travail** | Equipement : **DNS local** | Equipement : **Interface interne pare-feu** | Equipement : **Interface externe pare-feu** | Equipement : **ROUTEUR** | Equipement : ---------- | **Serveur web** |
|---|---|---|---|---|---|---|
| Adresse IP : ---------- | Adresse IP : ---------- | Adresse IP : ---------- | Adresse IP : ---------- | Adresse IP : **10.133.128.254** | Adresse IP : ---------- | Adresse IP : ---------- |

**Trame n°....**

**Trame n°....**

**Trame n°....**

**Trame n°....**

**Trame n°....**

**Trame n°....**

**Trame n°....**