BACCALAURÉAT 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 26 pages numérotées de 1/26 à 26/26, dont :

Page de garde	**:**	**Page 1/26**
Barème	**:**	**Page 2/26**
Sujet	**:**	**Pages 3/26 à 13/26**
Documents réponses	**:**	**Pages 14/26 à 16/26**
Annexes	**:**	**Pages 17/26 à 26/26**

Les feuilles DR1, DR2, DR3

sont à rendre obligatoirement avec votre copie

BAREME

PARTIE A ***12 POINTS***

ADSL

PARTIE B ***14 POINTS***

Etude et Paramétrage d'un routeur

PARTIE C ***13 POINTS***

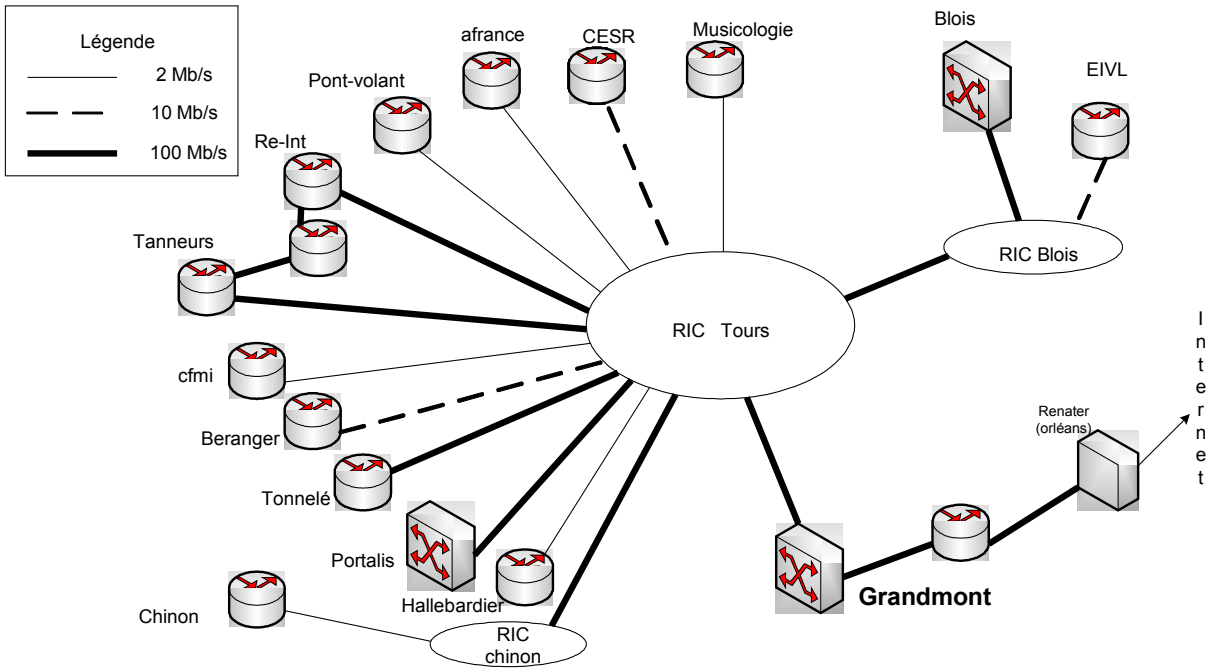
Messagerie

PARTIE D ***11 POINTS***

Etude du protocole ICMP

PRESENTATION DU RESEAU DE L' UNIVERSITE DE TOURS

Le réseau de l'Université de TOURS est composé de différents sites répartis de la manière suivante :

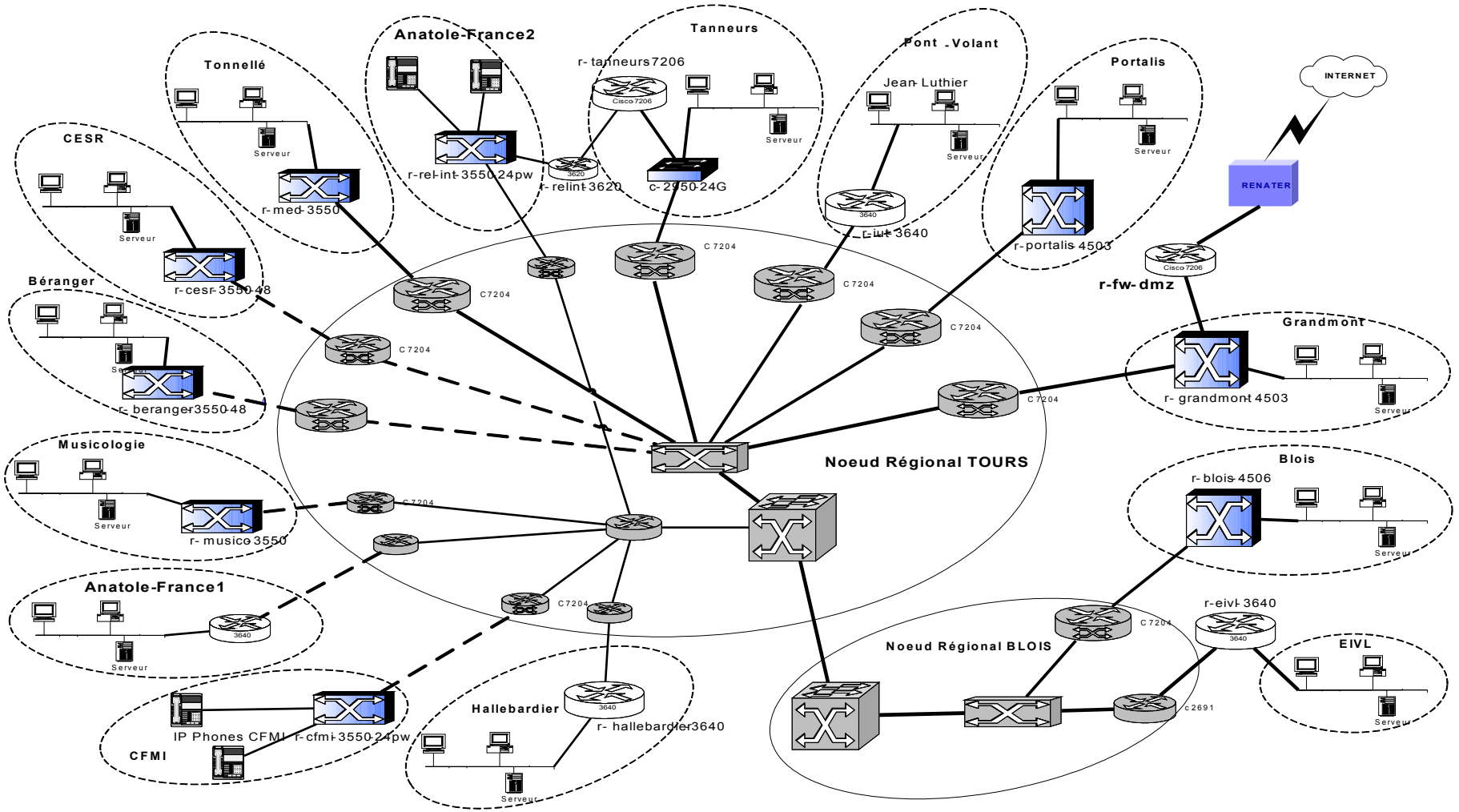


Le réseau de l'Université de TOURS est relié à un nœud RENATER situé à ORLEANS (RIC : **R**éseau **I**nter **C**ité).

RENATER est le **RE**seau **NA**tional de télécommunication pour la **T**echnologie, l'**E**nseignement et la **R**echerche. Plus de 600 sites sont raccordés au réseau RENATER. Ce réseau leur permet de communiquer entre eux, de développer des échanges et d'accéder aux centres de recherche publics et privés, aux établissements d'enseignement du monde entier et à l'Internet.

A ce jour, l'Université de TOURS dispose de 12 adresses publiques de classe C, dont une réservée pour RENATER.

Plan de l'interconnexion des différents sites



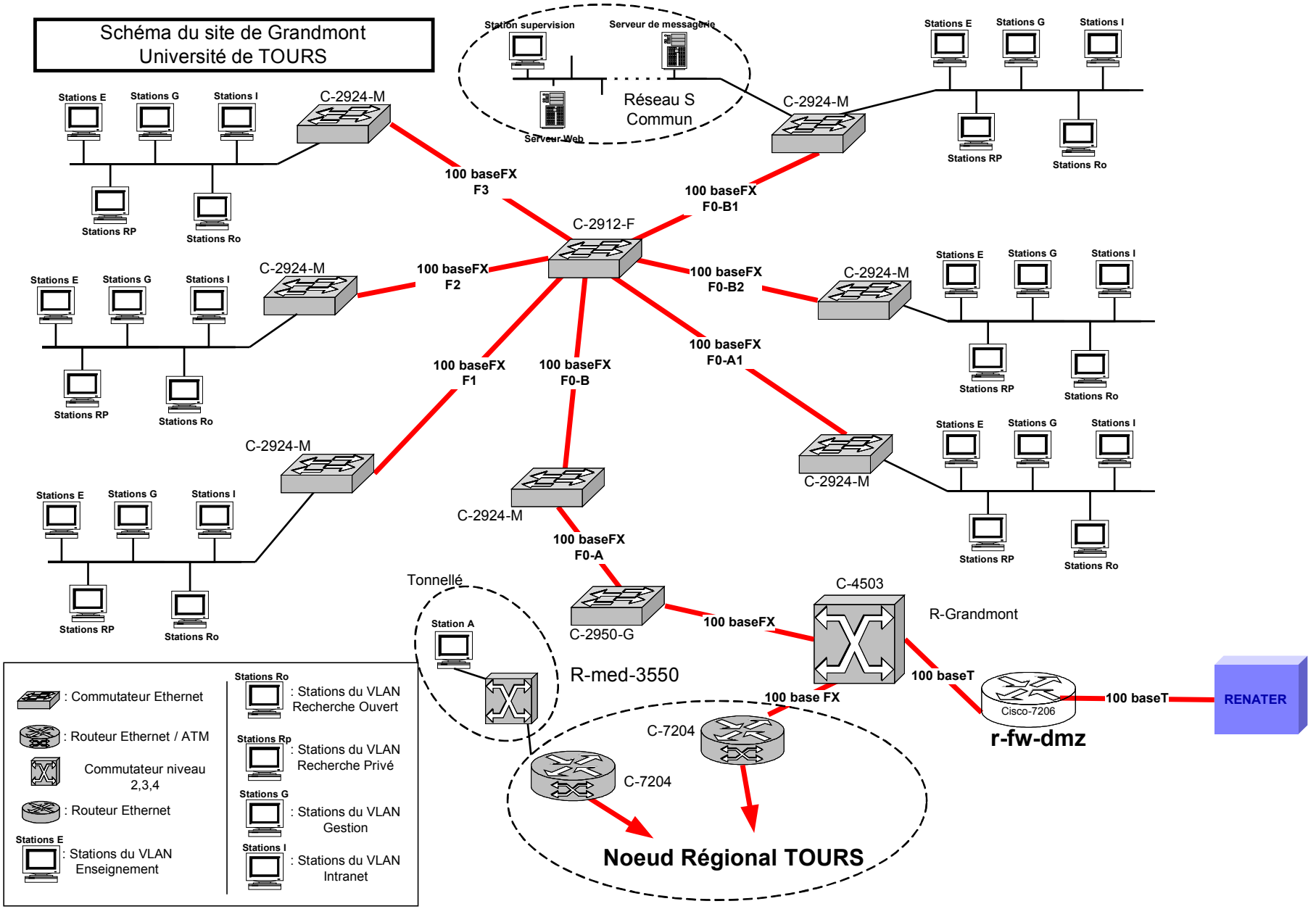


Schéma du site de Grandmont
Université de TOURS
Station supervision
Serveur de messagerie
Réseau S
Commun
Serveur Web
C-2924-M
C-2912-F
C-2950-G
C-4503
R-Grandmont
R-med-3550
Tonnellé
Station A
C-7204
Noeud Régional TOURS
Cisco-7206
r-fw-dmz
RENATER
100 baseFX
F3
100 baseFX
F0-B1
100 baseFX
F2
100 baseFX
F0-B2
100 baseFX
F1
100 baseFX
F0-B
100 baseFX
F0-A1
100 baseFX
F0-A
100 baseFX
100 base FX
100 baseT
100 baseT
Stations E
Stations G
Stations I
Stations RP
Stations Ro
: Commutateur Ethernet
: Routeur Ethernet / ATM
Commutateur niveau 2,3,4
: Routeur Ethernet
: Stations du VLAN Enseignement
: Stations du VLAN Recherche Ouvert
: Stations du VLAN Recherche Privé
: Stations du VLAN Gestion
: Stations du VLAN Intranet

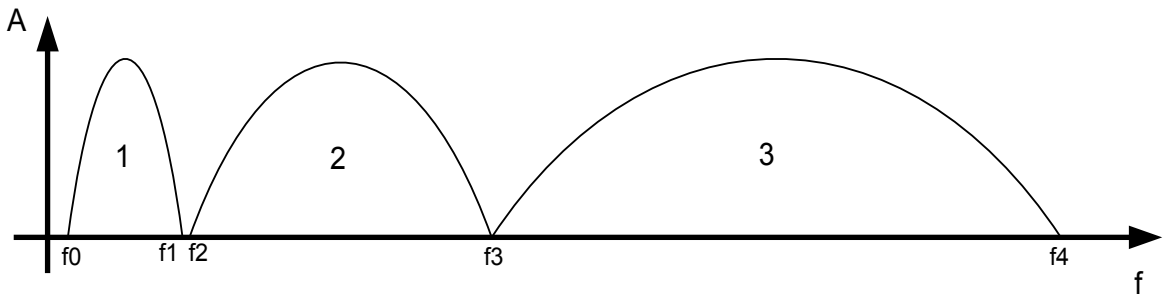
A-ADSL

Le BackBone inter-sites se fait sur des liens ATM . L'utilisateur dispose d'un accès ADSL.

A-1 L'ADSL

ADSL signifie **A**symetrical **D**igital **S**ubscriber **L**ine (Ligne d'abonné numérique asymétrique).
Pour transmettre les flux de données, la technologie ADSL s'appuie sur des paires cuivrées, ces mêmes fils qui transportent actuellement la voix dans notre téléphone traditionnel.
La liaison ADSL achemine les données de l'abonné sur la boucle locale jusqu'au réseau ATM du prestataire. **Seuls les abonnés situés à une distance telle que l'affaiblissement de la ligne ne dépasse pas 60 dB peuvent être raccordés au réseau ADSL**.

La technologie ADSL utilise 3 bandes de fréquence comme illustré ci-dessous:



A-1-1- Indiquer à quoi correspond la bande de fréquence [f0,f1] puis préciser la valeur de ces deux fréquences.

A-1-2- Indiquer à quoi correspondent les bandes de fréquence 2 et 3 en précisant comment elles sont utilisées par l'ADSL.

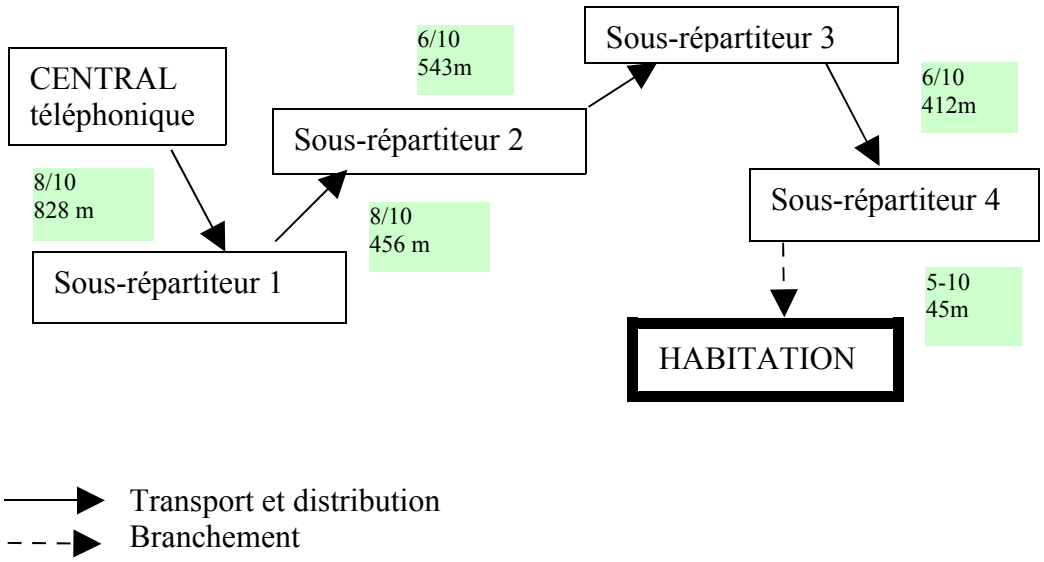
A-1-3- Combien de couches du modèle OSI utilise l'architecture ATM ? Citer leurs noms.

A-1-4- Quel élément matériel trouve-t-on entre la boucle locale et le réseau ATM ?

A-2 L'affaiblissement

L'affaiblissement est un paramètre important pour disposer ou non de l'ADSL.
La qualité de la ligne et la distance séparant le central de l'abonné, sont également à prendre en compte.

A-2-1- Déterminer l'affaiblissement chez l'abonné pour le cas suivant en vous aidant du tableau ci-dessous :



Affaiblissement linéique à 300 KHz				
Transport et distribution				
calibre des câbles	*4/10*	*5/10*	*6/10*	*8/10*
dB / Km à 300 kHz	*15*	*12,4*	*10,3*	*7,9*
Branchement				
type des câbles	5-9	5-10	série 278	série 92
dB / Km à 300 kHz	*7*	*10*	*15*	*15*

A-2-2- En déduire si l'abonné peut-être raccordé au réseau.

A-3 Vitesse de connexion

rappel : le débit est aussi appelé "capacité C de la connexion". On peut donner sa valeur théorique à l'aide du théorème de Nyquist :

$$C = \omega . \log_2 (1 + \frac{Ps}{Pb})$$

avec :

- **C** : capacité de la connexion (en b/s).
- **ω** : Bande Passante de la ligne (en Hz)
- **Ps / Pb** : Rapport de Puissance signal sur bruit
- **$\log_2$ (x)** = log(x) / log (2) (logarithme décimal)

Le rapport signal sur bruit (S/B) est mesuré en décibels. Il faut donc calculer le rapport de puissance (Ps/Pb) pour pouvoir appliquer le théorème de Nyquist.

S/B = 10 log (Ps / Pb)

A-3-1- Sachant que le rapport signal sur bruit **S/B = 20,4 dB, calculer le rapport Ps/Pb.**

A-3-2- Pour une bande passante de 75 KHz, calculer le débit sur un lien ADSL selon le théorème de Nyquist.

A-3-3- Comparer ce débit à une liaison RTC classique de 56 Kbits/s.

A-3-4- Combien de temps prendra alors la transmission de l'image suivante ?

Remarque : pour le calcul vous prendrez le débit normalisé de **512 Kbits/s**.

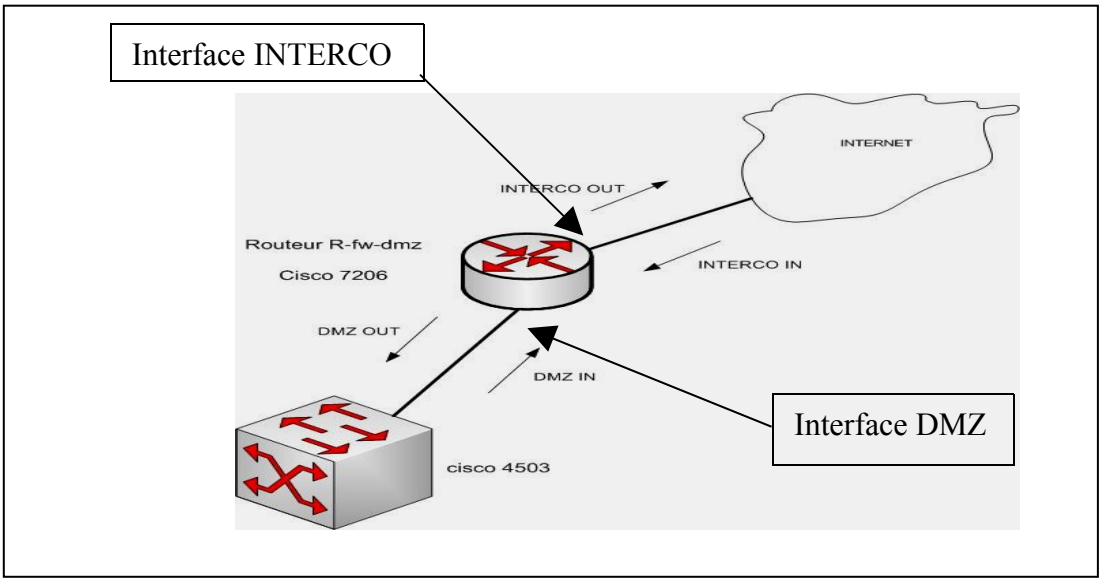
Taille = 31,3Ko

B - ETUDE ET PARAMÉTRAGE D'UN ROUTEUR

B-1 Etude du routeur du site de Grandmont

Le routeur qui nous intéresse (R-fw-dmz) se situe sur le site de Grandmont et joue le rôle de passerelle filtrante vers Internet pour tous les sites en utilisant la translation d'adresses et les listes d'accès (access-list).

Zoom sur le routeur et ses interfaces :



Voir également les schémas pages 4 et 5

L'intitulé du routeur R-fw-dmz fait penser à Firewall et DMZ.

B-1-1- Expliquer le rôle d'un firewall.

B-1-2- Expliquer ce qu'est une DMZ.

B-1-3- Citer 2 protocoles routables et 2 protocoles de routage.

B-1-4- Hormis celles filtrées, **citer 2 types de trames qui ne sont pas routées par le routeur R-fw-dmz.**

B-2 Paramétrage du routeur du site de Grandmont :

B-2-1- En vous aidant des annexes 1, 2, 3 et 4 **compléter le document réponse DR1 qui concerne une partie de la configuration du routeur R-fw-dmz .**

B-2-2- Pour les règles des lignes **4** et **6** du document réponse 1 (DR1), **calculer les plages d'adresses des réseaux concernés.**

B-2-3- Pourquoi toutes les access-lists présentes dans la configuration du routeur se terminent par "*permit ip any any*" ?

B-2-4- Si l'on souhaite interdire le service TFTP, **quelle ligne faut-il ajouter à la configuration du routeur dans l'access-list "dmz_in".**

C – Messagerie

C-1- Citer 3 protocoles permettant d'envoyer des E-mails et/ou d'en recevoir ?

C-2- Dans la messagerie électronique, on utilise des adresses du type **david.vincent@univ-tours.fr**. **Que représente la deuxième partie de cette adresse ?**

Un analyseur de protocole situé dans "**le réseau S**" a permis de faire un relevé entre une station A du réseau de "**Tonnellé**" et un serveur de l'université de TOURS situé dans le "**réseau S**" au cours d'un échange initié par l'utilisateur. (Voir schéma page 5)

Voici une des trames ETHERNET II récupérées :

00 04 75 CE 24 CF 00 0D 29 D4 69 7F 08 00 45 00
00 31 EE 6D 40 00 80 06 6C 02 0A 53 04 21 C3 34
D1 0E 0D 68 00 8F DE 08 55 7A 79 36 D4 8F 50 18
F8 4D A0 7A 00 00 34 37 20 6E 6F 6F 70 0D 0A

A l'aide des annexes 4, 5 et 6 :

C-3- Analyse des couches liaison, réseau et transport :

C-3-1 Faire un schéma représentant la station A et le serveur en indiquant les sockets utilisés par le client et le serveur.

Remarque : un socket est la combinaison de trois éléments : l'adresse IP de la machine, le protocole au niveau transport et le numéro du port.

C-3-2 Indiquer la signification des numéros de port source et destination.

C-3-3 Quelles sont les principales caractéristiques du protocole de niveau TRANSPORT utilisés ?

C-3-4 En vous basant sur le schéma du réseau de Grandmont (page 5), **indiquer à quels éléments actifs correspondent les adresses MAC source et destinataire (préciser leurs valeurs).**

C-3-5 Déterminer la longueur totale du datagramme IP puis en déduire si cette trame contient des bits de bourrage.

C-4- Conclusion : Quel est l'objectif de la demande initiée par l'utilisateur ?

D – Etude du protocole ICMP

Les trames ci-dessous ont été capturées sur une station du réseau local d'un lycée lors d'un échange avec le serveur WEB de l'université de TOURS. Pour éviter une surcharge, on n'a retenu que les trames non identiques et on a supprimé les champs non significatifs.

Frame 1 (106 bytes on wire, 106 bytes captured)
Ethernet II, Src: 00:50:fc:6f:c5:d6, Dst: 00:02:b3:e7:92:e1
Internet Protocol, Src Addr: 192.168.228.228 , Dst Addr: 195.52.209.10
  Time to live: 1
  Protocol: ICMP
Internet Control Message Protocol
  Type: 8
  Code: 0

Frame 2 (134 bytes on wire, 134 bytes captured)
Ethernet II, Src: 00:02:b3:e7:92:e1, Dst: 00:50:fc:6f:c5:d6
Internet Protocol, Src Addr: 192.168.231.254, Dst Addr: 192.168.228.228
  Time to live: 64
  Protocol: ICMP
Internet Control Message Protocol
  Type: 11
  Code: 0
  Internet Protocol, Src Addr: 192.168.228.228, Dst Addr: 195.52.209.10
    Time to live: 1
    Protocol: ICMP
   Internet Control Message Protocol
    Type: 8
    Code: 0

Frame 7 (106 bytes on wire, 106 bytes captured)
Ethernet II, Src: 00:50:fc:6f:c5:d6, Dst: 00:02:b3:e7:92:e1
Internet Protocol, Src Addr: 192.168.228.228, Dst Addr: 195.52.209.10
  Time to live: 2
  Protocol: ICMP
Internet Control Message Protocol
  Type: 8
  Code: 0

Frame 8 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: 00:02:b3:e7:92:e1, Dst: 00:50:fc:6f:c5:d6
Internet Protocol, Src Addr: 172.21.107.17, Dst Addr: 192.168.228.228
  Time to live: 63
  Protocol: ICMP
Internet Control Message Protocol
  Type: 11
  Code: 0
  Internet Protocol, Src Addr: 192.168.228.228, Dst Addr: 195.52.209.10
    Time to live: 1
    Protocol: ICMP
   Internet Control Message Protocol
    Type: 8
    Code: 0

Frame 13 (106 bytes on wire, 106 bytes captured)
Ethernet II, Src: 00:50:fc:6f:c5:d6, Dst: 00:02:b3:e7:92:e1
Internet Protocol, Src Addr: 192.168.228.228, Dst Addr: 195.52.209.10
  Time to live: 3
  Protocol: ICMP
Internet Control Message Protocol
  Type: 8
  Code: 0

Frame 14 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: 00:02:b3:e7:92:e1, Dst: 00:50:fc:6f:c5:d6
Internet Protocol, Src Addr: 195.55.207.10, Dst Addr: 192.168.228.228
  Time to live: 252
  Protocol: ICMP
Internet Control Message Protocol
  Type: 11
  Code: 0
  Internet Protocol, Src Addr: 192.168.228.228, Dst Addr: 195.52.209.10
    Time to live: 1
    Protocol: ICMP
  Internet Control Message Protocol
    Type: 8
    Code: 0

Frame 19 (106 bytes on wire, 106 bytes captured)
Ethernet II, Src: 00:50:fc:6f:c5:d6, Dst: 00:02:b3:e7:92:e1
Internet Protocol, Src Addr: 192.168.228.228, Dst Addr: 195.52.209.10
  Time to live: 4
  Protocol: ICMP
Internet Control Message Protocol
  Type: 8
  Code: 0

Frame 20 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: 00:02:b3:e7:92:e1, Dst: 00:50:fc:6f:c5:d6
Internet Protocol, Src Addr: 195.52.211.18, Dst Addr: 192.168.228.228
  Time to live: 251
  Protocol: ICMP
Internet Control Message Protocol
  Type: 11
  Code: 0
  Internet Protocol, Src Addr: 192.168.228.228, Dst Addr: 195.52.209.10
    Time to live: 1
    Protocol: ICMP
  Internet Control Message Protocol
    Type: 8
    Code: 0

Frame 29 (106 bytes on wire, 106 bytes captured)
Ethernet II, Src: 00:50:fc:6f:c5:d6, Dst: 00:02:b3:e7:92:e1
Internet Protocol, Src Addr: 192.168.228.228, Dst Addr: 195.52.209.10
  Time to live: 5
  Protocol: ICMP
Internet Control Message Protocol
  Type: 8
  Code: 0

Frame 30 (106 bytes on wire, 106 bytes captured)
Ethernet II, Src: 00:02:b3:e7:92:e1, Dst: 00:50:fc:6f:c5:d6
Internet Protocol, Src Addr: 195.52.209.10, Dst Addr: 192.168.228.228
  Time to live: 124
  Protocol: ICMP
Internet Control Message Protocol
  Type: 0
  Code: 0

L'échange entre le lycée et l'université s'est arrêté lors de la réception de la trame N°30, les trames suivantes ont été capturées lors de tests effectués sur le réseau interne du lycée :

Frame 33 (58 bytes on wire, 58 bytes captured)
Ethernet II, Src: 00:c0:a8:fe:b4:1b, Dst: 00:10:a7:0b:4a:2a
Internet Protocol, Src Addr: 192.168.228.35, Dst Addr: : 192.168.225.12
  Time to live: 100
  Protocol: ICMP
Internet Control Message Protocol
  Type: 12
  Code: 2
  Internet Protocol, Src Addr: 99.111.109.32
    Total Length: 30510
    Time to live: 101
    Protocol: SCPS

Frame 36 (58 bytes on wire, 58 bytes captured)
Ethernet II, Src: 00:c0:a8:fe:b4:1b, Dst: 00:10:a7:0b:4a:2a
Internet Protocol, Src Addr: 192.168.228.35, Dst Addr: 192.168.225.12
  Time to live: 100
  Protocol: ICMP
Internet Control Message Protocol
  Type: 3
  Code: 1
  Internet Protocol, Src Addr: 99.111.109.32
    Time to live: 101
    Protocol: SCPS

Frame 40 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: 00:02:b3:e7:92:e1, Dst: 00:c0:a8:fe:b4:1b
Internet Protocol, Src Addr: 192.168.231.254, Dst Addr: 192.168.228.35
  Time to live: 128
  Protocol: ICMP
Internet Control Message Protocol
  Type: 3
  Code: 3
  Internet Protocol, Src Addr: 192.168.228.35, Dst Addr: 192.168.231.254
    Time to live: 100
    Protocol: UDP
  User Datagram Protocol, Src Port: 5000 Dst Port: 53

D-1- Compléter les documents réponses DR2 (diagramme d'échange) et DR3 (tableau).

D-2- En déduire la commande qui a engendré les trames de 1 à 30 ? Quel est son rôle ?

D-3- Quelles sont les tâches réalisées par les équipements intermédiaires dans le cadre de l'échange avec l'université ?

D-4- Analyse de la trame N°40 :

D-4-1 Indiquer et expliquer la fonction réalisée par l'équipement d'adresse 192.168.231.254. Justifier votre réponse.

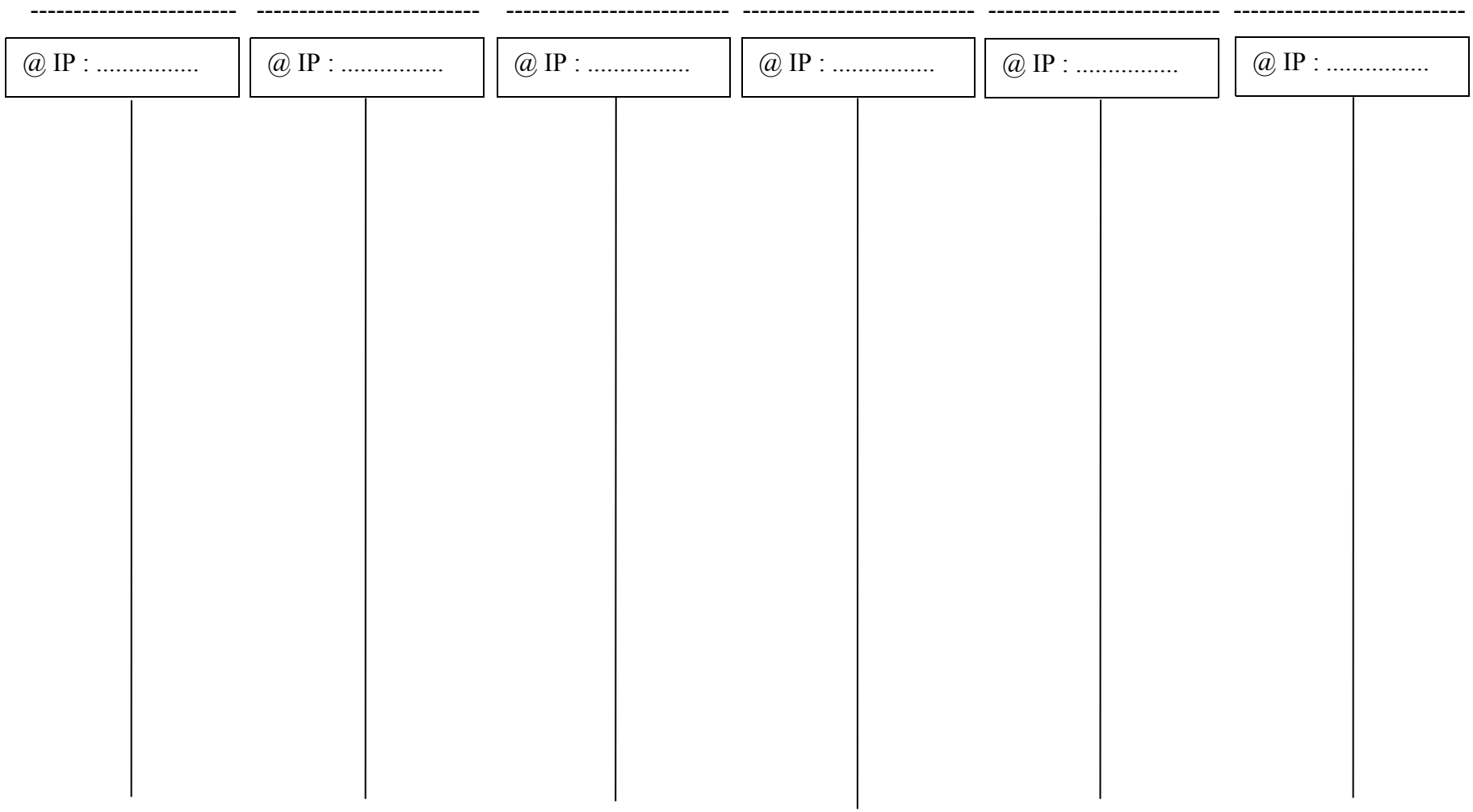
D-4-2 Cette trame signale un dysfonctionnement, **préciser lequel en justifiant votre réponse.**

DOCUMENT REPONSE 1 (DR1)

Ligne	***Extrait de la configuration du routeur***	***Explications***
1	*deny udp any any range 6881 6889*	
2	*deny tcp any any range 135 139*	
3	*deny udp any any eq 445*	
4	*deny tcp 10.0.0.0 0.255.255.255 any eq smtp log*	
5	*deny ip any 172.16.0.0 0.15.255.255*	
6	*deny ip 195.52.208.0 0.0.7.255 any*	
7	*permit ip any any*	

DOCUMENT REPONSE (DR2)

Indiquer la nature des équipements :



DOCUMENT REPONSE (DR3)

N° de trame	@ IP source	@ IP destination	TTL	Type	Code	Description en fonction du type
1						
2						
19						
20						
30						
33						
36						
40						

Annexe 1

Extrait de la configuration du routeur R-fw-dmz

```
!
!
version 12.2
service timestamps debug uptime
service timestamps log datetime localtime
service password-encryption
!
hostname r-fw-dmz
!
enable secret 5 "encryped password"
enable password 7 "encryped password"
!
interface FastEthernet2/0
 description *** Renater ****
 ip address 195.55.207.10 255.255.255.252
 ip access-group interco_in in
 ip access-group interco_out out
 ip nat outside
 ip route-cache flow
 duplex full
 speed auto
!
interface FastEthernet2/1
 description *** site Grandmont ***
 ip address 195.52.211.17 255.255.255.252
 ip access-group dmz_out out
 ip nat inside
 ip route-cache flow
 duplex full
 speed auto
!
ip nat pool net-222 195.52.222.1 195.52.222.220 netmask 255.255.255.0
ip nat pool net-221 195.52.221.1 195.52.221.254 netmask 255.255.255.0
ip nat pool net-iut 195.52.208.248 195.52.208.251 netmask 255.255.255.252
ip nat pool net-223 195.52.223.1 195.52.223.240 netmask 255.255.255.0
ip nat pool gestion 195.52.208.240 195.52.208.243 netmask 255.255.255.252
ip nat pool BUmed 195.52.208.244 195.52.208.247 netmask 255.255.255.252
ip nat inside source list 1 pool net-222
ip nat inside source list 2 pool net-223
ip nat inside source list 3 pool net-221
!
```

```
ip access-list extended dmz_in
 deny   tcp any eq 412 any
 deny   tcp any any eq 412
 deny   udp any eq 412 any
 deny   udp any any eq 412
 deny   tcp any range 4662 4665 any
 deny   tcp any any range 4662 4665
 deny   udp any range 4662 4665 any
 deny   udp any any range 4662 4665
 deny   tcp any range 6346 6347 any
 deny   tcp any any range 6346 6347
 deny   udp any range 6346 6347 any
 deny   udp any any range 6346 6347
 deny   tcp any eq 6699 any
 deny   tcp any any eq 6699
 deny   udp any eq 6699 any
 deny   udp any any eq 6699
 deny   tcp any range 6881 6889 any
 deny   tcp any any range 6881 6889
 deny   udp any range 6881 6889 any
 deny   udp any any range 6881 6889
 deny   tcp any any range 135 139
 deny   tcp any any eq 445
 deny   udp any any range 135 netbios-ss
 deny   udp any any eq 445
 deny   tcp 10.0.0.0 0.255.255.255 any eq smtp log
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip any any
!
logging facility local4
logging 192.168.1.10
access-list 1 deny   10.145.2.16 0.0.0.15
access-list 1 permit 10.128.0.0 0.31.255.255
access-list 2 permit 10.81.0.0 0.0.255.255
access-list 2 deny   10.0.192.0 0.127.63.255
……….
end
```

Annexe 2

Les routeurs sont des équipements de niveau 3 (réseau) et sont chargés de l'acheminement des datagrammes IP entre les réseaux.
En terme de sécurité, ils sont chargés plus précisément :

- de la recherche de chemins de secours
- du filtrage des broadcasts
- du filtrage des datagrammes IP (ACL)
- du contrôle des correspondances entre ports et adresses IP, et entre adresses MAC et adresses IP. (contrôle d'usurpation)

Les ACL (Access Control Lists)

Les ACL sont des filtres appliqués à chaque datagramme IP transitant à travers le routeur et qui ont pour paramètres :

- l'adresse IP de la source
- l'adresse IP de la destination
- le type du paquet (tcp, udp, icmp, ip)
- le port de destination du paquet

Pour un datagramme donné, l'ACL prend deux valeurs :

- **deny** : le paquet est rejeté.
- **permit** : le paquet peut transiter par le routeur.

Syntaxe

Les routeurs Cisco acceptent deux types d'ACL :

- l'access-list simple :

  access-list access-list-number {deny|permit} protocole ip-source source-masque

- l'access-list étendue (extended) :

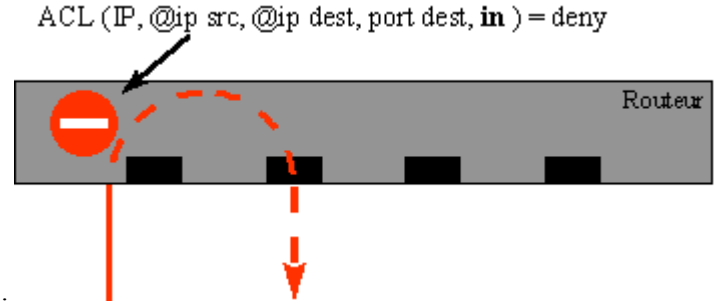
  access-list access-list-number {deny|permit} protocole ip-source source-masque ip destination destination-masque port-destination

access-list-number	numéro d'access-list : • entre 1 et 99 (simples) • entre 100 et 199 (étendus)
• **deny**	interdit l'accès lorsque les conditions sont vérifiées
• **permit**	autorise l'accès lorsque les conditions sont vérifiées
• **protocole**	nom ou numéro d'un protocole IP, comme **icmp**, **tcp**, **udp** ou **ip** pour préciser tous les protocoles ip

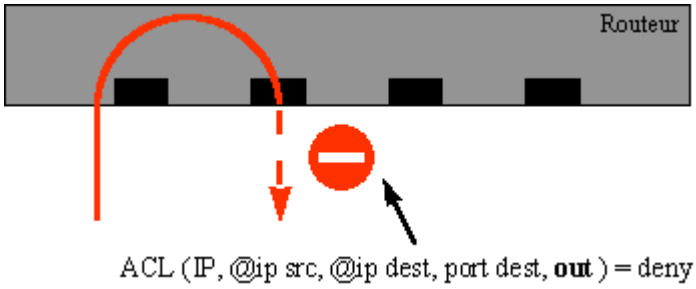
ip-source	adresse ip d'un réseau ou d'une station. Ce peut être : • l'adresse précisée sur 32 bits, • **any** pour toutes les stations (équivaut à 0.0.0.0 255.255.255.255) • **host** source pour une station particulière (équivaut à source 0.0.0.0)
masque-source	permet d'ignorer certains bits de l'adresse source. Les bits ignorés sont positionnés à 1 dans le masque.
ip-destination	adresse ip d'un réseau ou d'une station. Ce peut être : • l'adresse précisée sur 32 bits, • **any** pour toutes les stations (équivaut à 0.0.0.0 255.255.255.255) • **host** destination pour une station particulière (équivaut à source 0.0.0.0)
masque-destination	permet d'ignorer certains bits de l'adresse destination. Les bits ignorés sont positionnés à 1 dans le masque.
port-destination	uniquement pour tcp et udp, expresion de type : • **eq** numéro de port : identique (égale) à ... • **gt** numéro de port : plus grand que... • **lt** numéro de port : plus petit que • **ne** numéro de port : différent de ... • **established** : dans le cas d'une connexion tcp établie. • **Range N° port début N° port fin** : Défini une plage de N° de port.
log	Créer un fichier journal (log) pour consigner l'événement.

Activation de l'access-list

On associe à chaque interface du routeur une ACL.
Une ACL de type in, associée à une interface, contrôle le trafic qui entre dans le routeur par cette interface



Une ACL de type out associée à une interface contrôle le trafic qui quitte le routeur par cette interface.



Attention :

- les ACL ne s'appliquent qu'au **trafic en transit** et pas au trafic généré par le routeur lui-même. Par exemple, le trafic résultant d'une connexion telnet vers le routeur n'est pas soumis aux ACL.

- Implicitement la règle : **deny ip any any** est toujours appliquée à la fin de l'access-list, il n'est donc pas nécessaire de rajouter cette commande pour bloquer le reste du trafic.

L'activation d'une access-list sur une interface se fait par la commande :

ip access-group access-list-number {in|out}

access-list-number	numéro de l'access-list
in	filtre les paquets en entrée
out	filtre les paquets en sortie

Recommandations pour la configuration des routeurs :

Access-list contre le spoofing

L'access-list suivante interdit l'accès au réseau pour tous les datagrammes en provenance de l'extérieur, dont :

- l'adresse source est locale (127.0.0.0, 0.0.0.0)
- l'adresse source est privée (10.0.0.0, 172.16.0.0 et 192.168.0.0) (RFC 1918),
- l'adresse source est une adresse multicast (224.0.0.0) ou broadcast (255.255.255.255)
- l'adresse source est sur le réseau interne

access-list 100 deny ip 127.0.0.0 0.255.255.255 any

interdire paquet ip de réseau 127.0.0.0 vers tout(toute station)

access-list 100 deny ip 10.0.0.0 0.255.255.255 any

access-list 100 deny ip 192.168.0.0 0.0.255.255 any

access-list 100 deny ip 172.16.0.0 0.0.255.255 any

access-list 100 deny ip 224.0.0.0 31.255.255.255 any

access-list 100 deny ip host 255.255.255.255 any

access-list 100 deny ip host 0.0.0.0 any

access-list 100 permit ip any any

Cette access-list doit être appliquée sur toutes les interfaces externes :

ip access-group 100 in

Adresse IP et masque générique

Les ACL définissent des familles d'adresses IP à l'aide d'une **adresse IP** et d'un **masque générique**.

Pour vérifier si une adresse IP appartient à une famille :

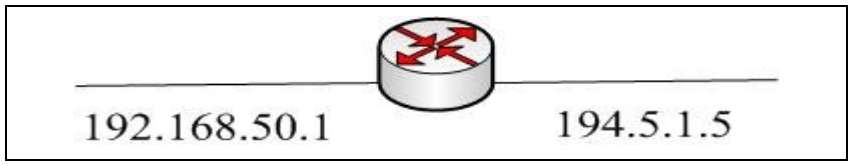
- prendre l'adresse IP
- appliquer le masque générique, c'est-à-dire mettre à 0 dans l'adresse IP tous les bits qui sont à 1 dans le masque classique.
- comparer le résultat obtenu à l'adresse générique de la famille.

Exemples d'adresses génériques et de masques :

- 192.9.200.0 0.0.0.255 Toutes les adresses IP du réseau 192.9.200.0
- 192.9.200.1 0.0.0.0 L'adresse IP 192.9.200.1
- 0.0.0.0 255.255.255.255 Toute adresse IP.
- 192.9.200.0 0.0.0.63 Toutes les adresses IP comprises entre 192.9.200.0 et 192.9.200.63
- 147.210.0.254 0.0.255.0 Toutes les adresses IP de la forme 147.210.x.254

Annexe 3

Exemple de configuration partielle d'un routeur



interface ethernet 0	*va configurer l'interface eth0*
description interface interne	
ip address 192.168.50.1 255.255.255.0	*configuration de l'interface*
ip access-group 102 in	*l'accesslist 102/inbound s'applique à cette interface*
!	
interface ethernet 1	*va configurer l'interface eth1*
description interface externe	
ip address 194.5.1.5 255.255.255.0	*configuration de l'interface*
ip access-group 120 in	*l'accesslist 120/inbound s'applique à cette interface*
!	
ip route 0.0.0.0 0.0.0.0 ethernet 1	*route par défaut*
ip route 192.168.50.0 255.255.255.255 ethernet 0	*route interne*
!	
access-list 102 permit tcp 192.168.50.0 0.0.0.255 any	*les machines du réseau 192.168.50 vers tout*
access-list 102 permit icmp any any	*tout en icmp*
access-list 102 permit tcp any any established	*toutes les connexions établies*
access-list 102 permit tcp any gt 1023 any 80	*tout (port > 1023) vers tout (port 80)*
access-list 102 permit tcp any host 1.2.3.4 53	*tout vers 1.2.3.4 (port 53)*
access-list 102 permit tcp any ne 53 host 2.3.4.5	*tout (port différent de = 53) vers 2.3.4.5*
access-list 102 permit tcp any host 3.4.5.6 range 1 45	*tout vers 3.4.5.6 (port 1 à 45)*
access-list 102 deny tcp any any range 6000 6003	*tout vers tout (port entre 6000 et 6003)*
access-list 102 permit tcp host 192.168.10.7 20 any gt 1024	*machine 192.168.10.7(port 20) vers tout (>1024)*
access-list 102 deny ip any any	*Tout interdire le reste*
!	
access-list 120 deny ip 192.168.50.0 any	*anti-spoofing interdiction*
access-list 120 permit tcp any 192.168.50.5 eq 53	*peut se connecter sur le serveur de noms de fichiers*
end	

Annexe 4

Assignation de certains ports associés aux processus serveurs en fonction des protocoles de transport TCP et UDP.

Processus	Port	Protocole Description
ftp-data	20	File Transfer [Default Data]
ftp	21	File Transfer [Control]
ssh	22	SSH Remote Login Protocol
telnet	23	Telnet
smtp	25	Simple Mail Transfer
domain	53	Domain Name Server
bootpc	68	Bootstrap Protocol Client
tftp	69	Trivial File Transfer
http	80	World Wide Web HTTP
pop2	109	Post Office Protocol - Version 2
pop3	110	Post Office Protocol - Version 3
sftp	115	Simple File Transfer Protocol
nntp	119	Network News Transfer Protocol
statsrv	133	Statistics Service
netbios-ns	137	NETBIOS Name Service
netbios-dgm	138	NETBIOS Datagram Service
netbios-ssn	139	NETBIOS Session Service
Imap2	143	Interim Mail Access Proto v2
snmp	161	Simple Net Mgmt Proto
https	443	MComhttps
Microsoft-DS	445	NETBIOS Datagram Service(Win2000)
P2P	6881 to 6889	client P2P

Annexe 5

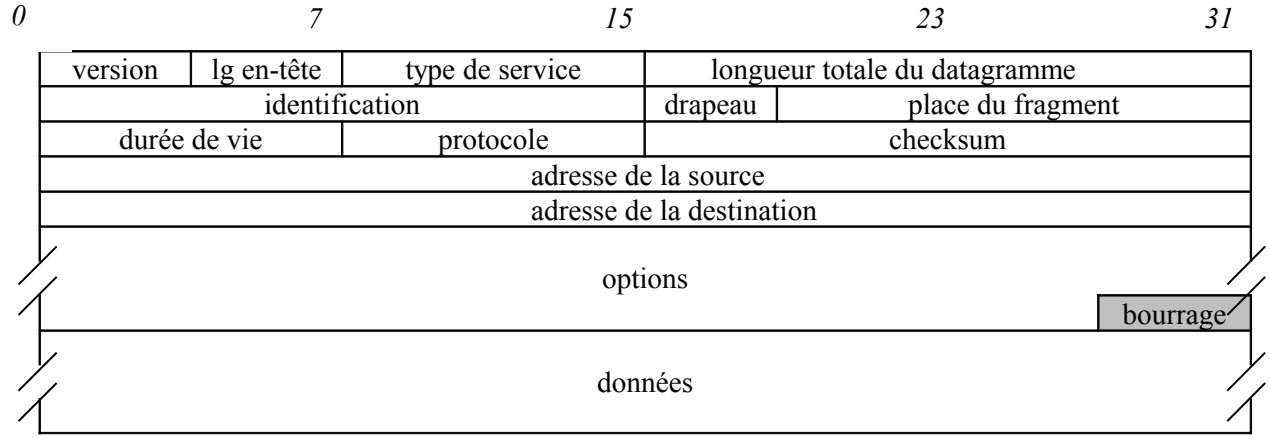
FORMAT D'UNE TRAME ETHERNET_II

Adresse MAC Destination 6 octets	Adresse MAC Source 6 octets	Protocole Niveau 3 2 octets	Données niveau 3 + bourrage éventuellement 46 octets minimum, 1 500 octets maximum	CRC 4 octets

Exemples de valeurs du champ protocole d'une trame ETHERNET_II

Champ protocole (hexadécimal)	Protocole
0x0800	DOD IP (Internet)
0x0806	ARP
0x80D5	IBM SNA Service on Ether
0x8035	RARP
0x86DD	IPv6

FORMAT D'UN DATAGRAMME IP



Les champs spécifiques d'un paquet IP sont:

- **version** est codé sur 4 bits. Actuellement ce champ a une valeur égale à 4 (IPv4).
- **longueur de l'en-tête** ou IHL (Internet Header Length) sur 4 bits spécifie le nombre de mots de 32 bits qui composent l'en-tête. Si le champ option est vide, l'IHL vaut 5.
- **type de service** ou ToS (Type of Service) est codé sur 8 bits. Spécifie à la passerelle intermédiaire le type d'acheminement attendu.
- **identification** codé sur 16 bits permet de sécuriser le réassemblage des paquets après fragmentation.
- **drapeau** codé sur 3 bits a le 1er bit toujours nul, le 2ème bit à 0 indique que le paquet peut être fragmenté et à 1 s'il ne peut pas l'être, le 3ème bit à 0 indique s'il s'agit du dernier fragment et à 1 que d'autres fragments suivent.
- **place du fragment** codé sur 13 bits indique la position du 1er octet dans le datagramme total non fragmenté. Il s'agit d'un nombre multiple de 8 octets.
- **durée de vie** détermine en seconde, la durée de vie d'un datagramme. Cette valeur est décrémentée toutes les secondes ou à chaque passage à travers une passerelle.
- **protocole** codé sur 8 bits indique le protocole de la couche supérieure (liste donnée par le rfc 1700, ex: "1"=ICMP, "2"=IGMP, "6"=TCP, "17"=UDP).
- **checksum** est la somme de contrôle portant sur l'en-tête.
- **adresses** de la source et de la destination sont codées sur 32 bits.

- **option** est de longueur variable et peut être nul.

Annexe 6

FORMAT DES MESSAGES TCP

Bit 0 7	**8** 15	**16** 23	**24** 31
Port source		Port destination	
Numéro de séquence			
Acquittement			
Lg entête	6 bits réservés	6 drapeaux	Fenêtre
Checksum		Pointeur message urgent	
Options (bourrage)			
Data			

Port source et Port destination : Ils identifient les programmes d'application.

N° de séquence : Il indique le n° du 1er octet transmis dans le segment.

Acquittement : indique le n° du prochain octet attendu par l'émetteur de ce message

Lg entête : sur 4 bits, elle indique la taille en mots de 32 bits de l'entête

Drapeaux : bit URG : Validation de la valeur du champ "pointeur message urgent"
bit ACK : la valeur du champ "acquittement" peut être prise en compte
bit PSH : le données doivent être immédiatement transmises à la couche supérieure
bit RST : fermeture de la connexion à cause d'une erreur irrécupérable
bit SYN : ouverture de la connexion
bit FIN : fin de connexion (plus de data à émettre)

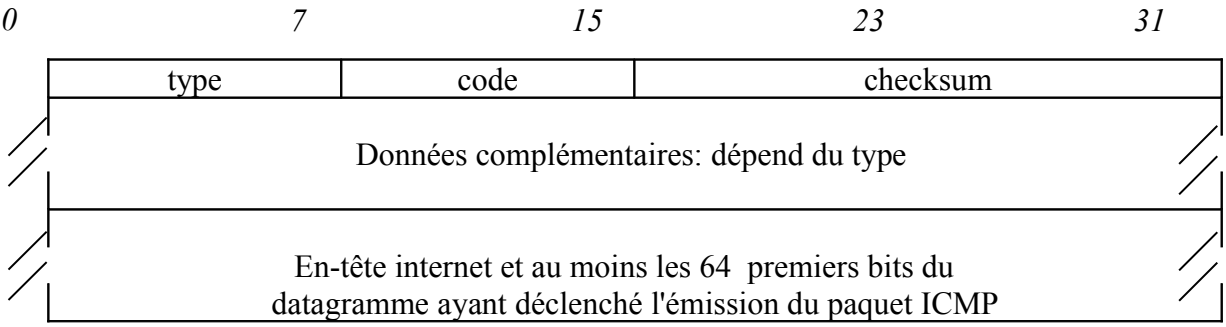
Fenêtre : Nombre d'octets que le récepteur peut accepter sans ACR.

Pointeur de message urgent : Si le drapeau URG est positionné, les données passent avant le flot de données normales. Ce champ indique alors la position de l'octet de la fin des données urgentes.

Le champ option peut-être utilisé si deux machines doivent se mettre d'accord sur une taille maximale de segment appelé MSS (Maximum Segment Size).

Annexe 7

FORMAT D'UN PAQUET ICMP



Types et codes des paquets ICMP:

Type	Code	description
0	0	Réponse à une demande d'écho
3		Destination inaccessible
	0	Le réseau ne peut être atteint
	1	La station ne peut être atteinte
	2	Le protocole n'est pas disponible bien que la station soit accessible
	3	Le port est inaccessible et le niveau 4 ne sait pas délivrer les données
	4	La fragmentation est nécessaire car le paquet est trop grand
	5	La route proposée en option n'est pas valable
4	0	Message de contrôle de flux
5		Redirection
	0	Pour un réseau ou un sous-réseau
	1	Pour une station
	2	Pour un réseau ou un sous-réseau avec un type de service
	3	Pour une station avec un type de service
8	0	Demande d'écho
9	0	Information sur les routeurs
10	0	Sélection d'un routeur
11		Durée de vie écoulée (=0)
	0	La durée de vie est écoulée avant l'arrivée à destination
	1	Le temps limite de réassemblage de fragment est dépassé
12		Message d'erreur de paramètre
	0	Le pointeur indique l'erreur
	1	Il manque une option
	2	Mauvaise longueur
13	0	Estampille temporelle (timestamp)
14	0	Réponse à l'estampille temporelle