



SERVICES CULTURE ÉDITIONS  
RESSOURCES POUR  
L'ÉDUCATION NATIONALE

**Ce document a été numérisé par le CRDP de Montpellier pour la  
Base Nationale des Sujets d'Examens de l'enseignement professionnel**

Ce fichier numérique ne peut être reproduit, représenté, adapté ou traduit sans autorisation.

**BACCALAURÉAT PROFESSIONNEL**  
**MICRO-INFORMATIQUE ET RÉSEAUX :**  
**INSTALLATION ET MAINTENANCE**

**ÉPREUVE E2**

Épreuve de technologie

Analyse fonctionnelle et structurelle d'un réseau ou  
d'un système de communication

**Ce dossier comprend 31 pages numérotées de 1/31 à 31/31, dont :**

**Page de garde : Page 1/31**  
**Barème : Page 2/31**  
**Sujet : Pages 3 à 13/31**  
**Annexes : Pages 14 à 27/31**  
**Documents réponses : Pages 28 à 30/31**  
**Schéma global du réseau : Page 31/31**

**À rendre obligatoirement avec votre copie**  
**les feuilles : 28/31, 29/31 et 30/31**

CODE ÉPREUVE : 0906-MIR T		EXAMEN : BCP	SPÉCIALITÉ : MICRO-INFORMATIQUE ET RÉSEAUX : INSTALLATION ET MAINTENANCE	
SESSION 2009	SUJET	ÉPREUVE : E2 Analyse fonctionnelle et structurelle d'un réseau ou d'un système de communication		Calculatrice autorisée
Durée : 4 HEURES		Coefficient : 3	Code sujet : 05-E2MRIM-08	Page : 1/31

## BARÈME :

A-ÉTUDE FONCTIONNELLE DU RÉSEAU V.O.A.	120pts
B-ÉTUDE DE LA MIGRATION DE L'ARCHITECTURE DU RÉSEAU	40pts
C-EXTENSION DU RÉSEAU V.O.A. : LIAISON WIFI	40pts

CRDP de l'académie de Montpellier

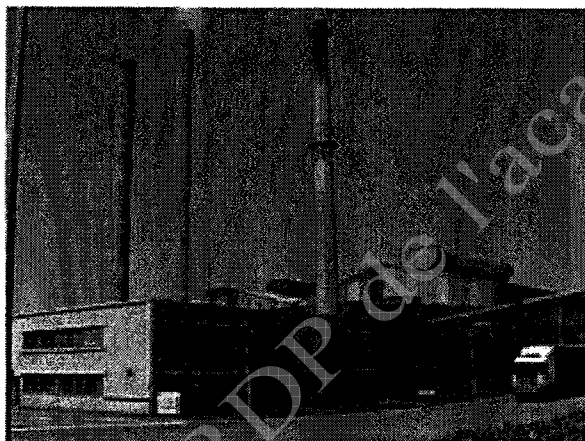
## PRÉSENTATION

Les fondements de la V.O.A. (Verrerie Ouvrière d'Albi) datent d'un conflit à la verrerie Sainte-Clothilde à Carmaux. Pour mémoire, le renvoi de deux ouvriers avait conduit à une grève ; le patron de l'époque, par mesure de rétorsion, avait fermé l'usine. Jean Jaurès alors employé avait mené les négociations de fond en comble et conseillé aux ouvriers de créer leur propre verrerie, leur propre entreprise. Ces derniers, en grande partie des employés albigeois, effectuaient 15 kilomètres quotidiens à pied d'Albi jusqu'à Carmaux.

La V.O.A. a finalement vu le jour en 1896 grâce à la générosité de Madame Dembourg, une riche bourgeoise qui donna son terrain pour la conception de cette future verrerie ouvrière.



La V.O.A. fut rebaptisée Verrerie d'Albi en 1991, lors de son rachat par le groupe Saint-Gobain, premier verrier national et perdit alors définitivement son titre de coopérative ouvrière.

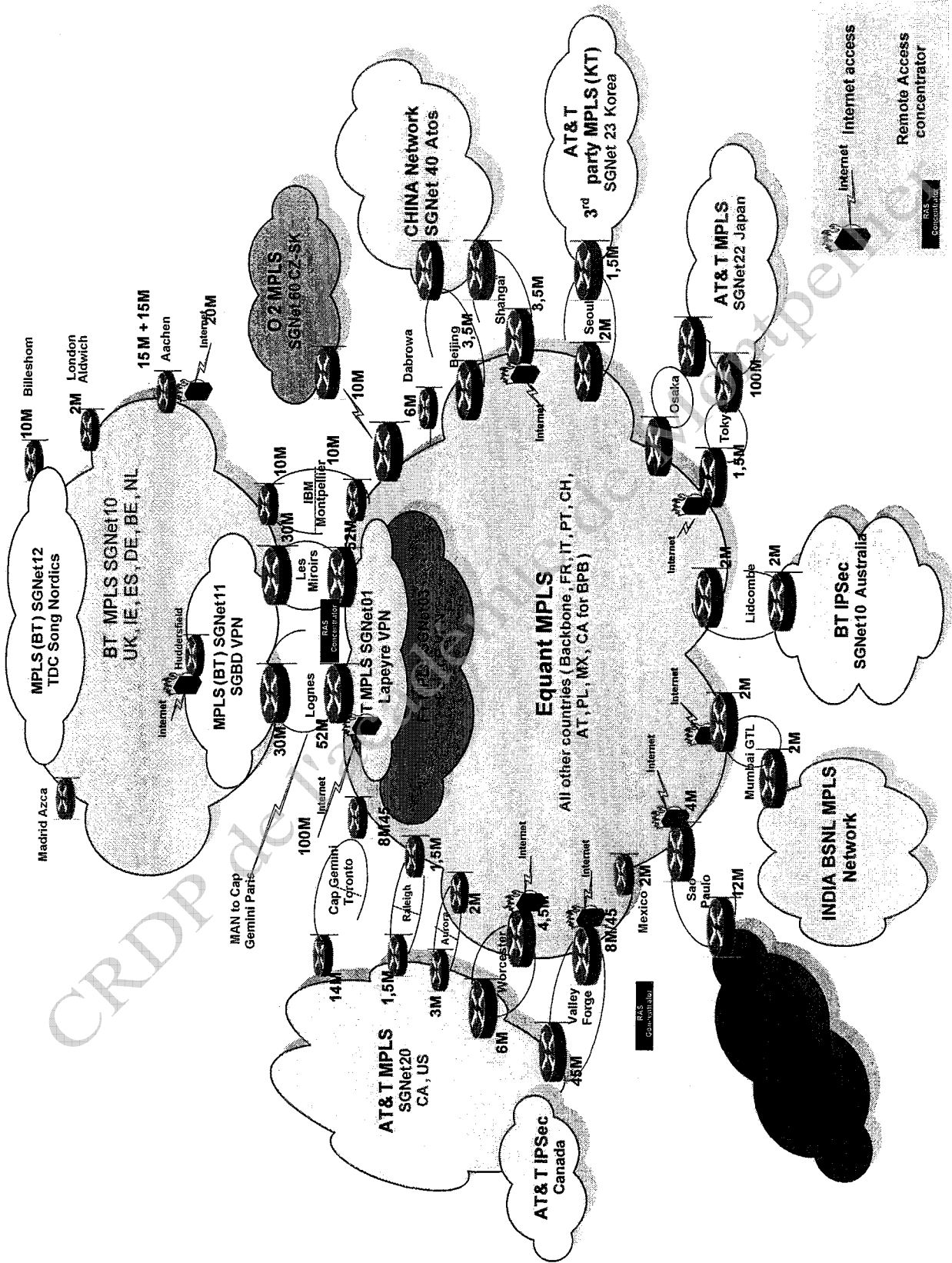


La V.O.A. emploie aujourd'hui 267 salariés sur les 23 hectares du site. Pour se donner un ordre d'idée, ils étaient 900 à l'époque de Jaurès en 1896 et plus de 350 ouvriers en 1995.

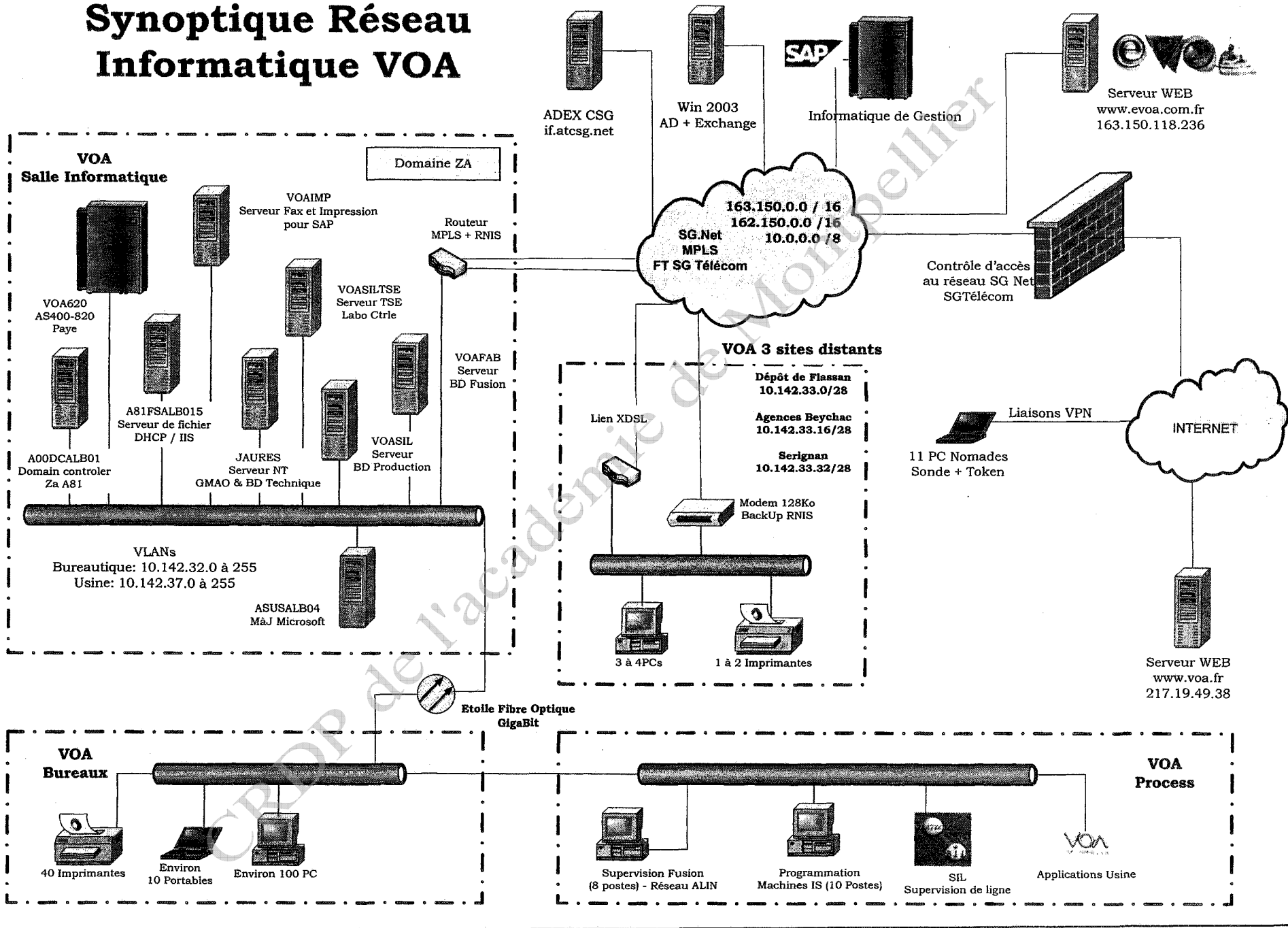
Avec près d'un million de bouteilles en verre produites par jour et plus de 1 800 clients, la V.O.A. occupe le troisième rang des 19 verreries françaises. Les chiffres clefs de la V.O.A. sont :

- 70 % de sa production de bouteilles concerne les vins
- 20 % les apéritifs et spiritueux
- 9% les huiles et les bouteilles d'eau minérale
- 1 % les boissons non alcoolisées
- en 2006, le chiffre d'affaires de la V.O.A. s'élevait à 19 millions d'euros.

L'entreprise V.O.A. fait donc partie maintenant du groupe Saint-Gobain et intègre ainsi le réseau mondial SG.Net présenté ci-dessous :



# Synoptique Réseau Informatique VOA



Examen : BCP Micro-informatique et Réseaux : Installation Épreuve : E2 Analyse fonctionnelle et structurelle d'un réseau ou d'un système de communication  
 N° Sujet : 05-E2MR/IM-08  
 Page 5/31

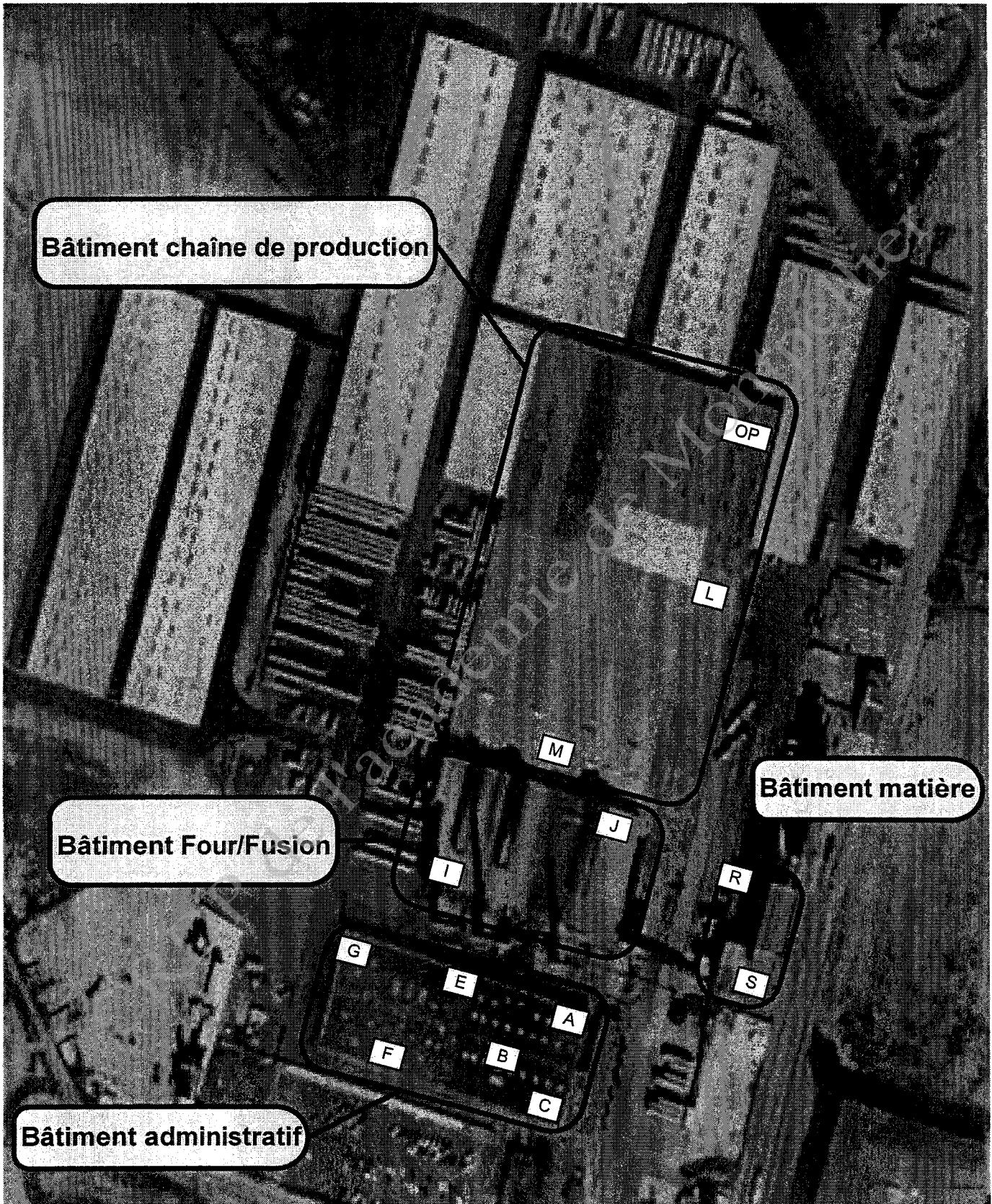
Le réseau de la V.O.A. répond au cahier des charges suivant :


- Il existe deux VLAN :
  - Bureautique 10.142.32.0/24
  - Usine 10.142.37.0/24
  
- Il existe 3 sites distants : Flassan, Beychac et Sérignan. On trouve sur chacun de ces sites :
  - un plan d'adressage IP différent
  - 3 à 4 stations
  - 1 ou 2 imprimantes
  - accès XDSL vers le réseau SG.Net
  - un lien de secours RNIS
  
- Dans le réseau bureautique on retrouve :
  - les serveurs du réseau (Jaures, V.O.A.SIL, V.O.A.IMP,...) entre 10.142.32.1/24 et 10.142.32.20/24
  - les éléments actifs du réseau (commutateurs, routeurs, point d'accès WiFi ...) entre 10.142.32.220/24 et 10.142.32.254/24
  - les imprimantes entre 10.142.32.170/24 et 10.142.32.219/24
  - les adresses libres pour les clients du réseau distribuées par un serveur DHCP
  
- Une étoile optique en fibre multimode 62,5/125µm qui relie les différentes baies de brassage. (voir sur la page suivante la répartition/localisation des baies de brassage sur le site).

**Voir Schéma global de l'architecture réseau à la page 31/31.**



Répartition/localisation des baies de brassage sur le site V.O.A.



Échelle   
70 m



# A-ÉTUDE FONCTIONNELLE DU RÉSEAU V.O.A.

## A-0 Étude du plan d'adressage IP (Cf. annexe 1)

Les administrateurs réseau de la V.O.A. ont à leur disposition une adresse IP de classe A pour effectuer leur plan d'adressage.

A-0-1 Justifier que l'adresse réseau 10.142.0.0 est une adresse de classe A. Préciser si cette adresse est une adresse privée ou publique.

L'usage des sous-réseaux a été décidé par les administrateurs réseau. Le masque de sous-réseau adopté limite le nombre de stations par sous-réseau.

A-0-2- Calculer pour le réseau de Sérignan le nombre d'hôtes possibles. Détailler votre calcul.

A-0-3- Compléter la colonne "Nb Adresses" dans le document réponse DR1.

## A-1 L'étoile optique :

Les différentes baies de brassage de la verrerie sont reliées entre elles par un ensemble de fibres optiques. Ainsi le câblage vertical est en fibre optique multimode alors que le câblage horizontal reste lui en paires torsadées Cat. 5e. Pour autant, un certain nombre de liaisons fibres restent sur des débits comparables à ceux des liaisons cuivre.

A-1-1 Définir ce que sont le câblage vertical et le câblage horizontal.

A-1-2 Sur l'étoile optique du réseau V.O.A., quelles sont les différentes technologies réseau sur fibre ainsi que leur débit respectif ?

A-1-3 Justifier alors le choix de la fibre optique par rapport à la paire torsadée, par exemple pour la liaison baie I vers Baie L entre les commutateurs RESFD1 et RESFBC1. (voir notamment le plan répartition/localisation des baies de brassage sur le site).

## A-2 Étude des VLAN :

Le réseau de la verrerie est divisé en réseaux virtuels de la manière suivante :

- Le réseau bureautique et gestion (SAP) : VLAN32 : 10.142.32.0/24 : c'est le seul réseau autorisé nativement à utiliser la liaison MPLS SG.Net.
- Le réseau usine indépendant : VLAN37 : 10.142.37.0/24 : réseau avec un contrôle d'accès vers la liaison MPLS SG.Net, pour certaines stations défini par le service informatique.

L'ensemble de ces VLAN est défini sur tous les commutateurs et routeurs de l'architecture. L'affectation des stations dans ces deux VLAN se fait de manière statique en fonction du port de brassage. Les liens nécessitant le transport de plusieurs VLAN répondent à la norme 802.1Q.

A-2-1 Expliquer la notion de réseaux virtuels. Que signifie l'acronyme VLAN ?

A-2-2 Le routeur d'accès à la liaison MPLS SG.Net a pour adresse logique 10.142.32.254/24. Quelle fonction est donc nécessaire pour permettre aux stations du VLAN37 d'accéder au réseau SG.Net ?

A-2-3 Indiquer les adresses IP des éléments actifs qui se chargent de cette tâche.

A-3 Étude des listes d'accès:

Comme dit précédemment, il existe des listes d'accès (voir annexe 2) vers le réseau SG.Net depuis le VLAN37.

**Extrait du fichier de configuration de la pile StackWise HSRP de la baie A :**

```
.....  
.....  
interface VLAN32  
  ip address 10.142.32.250 255.255.255.0  
.....  
interface VLAN37  
  ip address 10.142.37.250 255.255.255.0  
  ip access-group 37 in  
.....  
ip classless  
ip route 10.0.0.0 255.0.0.0 10.142.32.254  
ip route 10.0.0.0 255.255.0.0 10.142.32.254  
ip route 10.142.33.0 255.255.255.0 10.142.32.254  
ip route 163.150.0.0 255.255.0.0 10.142.32.254  
ip route 162.150.0.0 255.255.0.0 10.142.32.254  
ip route 194.51.14.0 255.255.255.0 10.142.32.254  
ip route 212.234.0.0 255.255.0.0 10.142.32.254  
no ip http server  
.....  
ip access-list 37 permit 10.142.37.0 0.0.0.31  
.....
```

Filtrage des trames en entrée

Définition de la plage d'adresses autorisées

A-3-1 Définir le type de liste d'accès. Justifier votre réponse.

A-3-2 Déterminer la plage d'adresses IP autorisée à sortir du VLAN37 vers le réseau SG.Net.

A-3-3 Quelle règle implicite permet de cantonner le reste du trafic au sein du VLAN37 ?

A-3-4 Quelle est l'adresse IP de la passerelle permettant aux paquets autorisés du VLAN37 de sortir sur le réseau SG.Net ?

#### A-4 Étude de l'architecture DNS (Cf. annexe 3)

Le réseau de la V.O.A. utilise un annuaire Active Directory. L'utilisation d'un serveur DNS est nécessaire pour la résolution des noms des différents domaines de St Gobain.

On admet qu'un serveur DNS principal est présent dans chacun des domaines locaux et que ce serveur effectue une redirection d'adresse pour la résolution des noms qui ne font pas partie du domaine concerné.

A-4-1 Quel est le rôle rempli par un serveur DNS ?

A-4-2 Quel est l'intérêt d'utiliser un serveur DNS par zone de recherche ?

A-4-3 Qu'appelle-t-on un nom FQDN ?

A-4-4 Sur le document réponse DR1, flécher et numérotant chronologiquement les échanges DNS qui se font suite à une demande de résolution de la part de la station 1 de la zone locale 1.

#### A-5 Étude du réseau V.O.A. liaison intersite

Les sites V.O.A. ont une infrastructure basée sur la redondance de lien. Les liaisons intersite sont généralement de type fibre et adaptées aux possibilités locales de communication.

A-5-1 Lister les différents types de lien utilisés pour la communication entre sites V.O.A. .

A-5-2 La V.O.A. utilise une liaison RNIS comme lien de secours. Pourquoi utilise-t-on cette technologie ?

A-5-3 Que regroupe le sigle xDSL ?

A-5-4 Rappeler la signification de VPN. Que doit-on mettre en œuvre pour assurer son déploiement ?

A-5-5 Quels peuvent être les besoins du site V.O.A. pour avoir décidé de mettre en œuvre un VPN ?

## B-ÉTUDE DE LA MIGRATION DE L'ARCHITECTURE DU RÉSEAU

Le réseau V.O.A. connaît depuis quelques années une restructuration profonde, mais pour des raisons de coût, celle-ci se fait par étapes. C'est ainsi que cohabitent sur le réseau des gammes d'éléments actifs très disparates. Les commutateurs de la société sont en effet variés, pour preuve :

- Catalyst 2924
- Catalyst 2950
- Catalyst 2948
- Catalyst 2960
- Catalyst 3550
- Catalyst 3750

Les technologies de liens fibre et cuivre ne sont pas en reste, un rapide coup d'œil au schéma réseau et on aperçoit :

- FO 1000base SX
- FO 100base FX
- Gigabit-ethernet cuivre
- Gigastack Cisco
- Ethernet et Fast-Ethernet cuivre

La migration engagée poursuit son cours et voici venu le moment de migrer les éléments actifs de la Baie Op et de la baie A.

### B-1 Migration baie OP

B-1-1 Quelle est la norme Ethernet de la fibre optique raccordée sur le matériel RESFBF présent dans la baie OP ?

B-1-2 Réaliser le choix des commutateurs de la gamme 2950 ainsi que des modules Gigabit Ethernet que vous devez installer en lieu et place des commutateurs 2924 présents.

Consulter pour ce faire le schéma global de l'architecture réseau et le contenu de l'annexe 4.

Compléter le document réponse DR2.

B-1-3 Les 24 ports 10/100 de ces commutateurs permettent d'obtenir, d'après la documentation constructeur, des débits de 200 Mbit/s. Quel mode de communication permet d'obtenir ce débit ?

B-1-4 Qu'entend-t-on par « agrégation de lien » ?

B-1-5 L'ensemble de l'architecture possède une forte redondance de lien. Quel problème cela peut-il poser ?

B-1-6 Citer le protocole réseau permettant de résoudre le problème évoqué précédemment et expliquer son fonctionnement.

## B-2 Migration baie A

B-2-1 Réaliser le choix du commutateur de la gamme 3750 ainsi que des modules que vous devez installer en lieu et place du commutateur 3550 présent.

Consulter pour ce faire le schéma global de l'architecture réseau et le contenu de l'annexe 4.

Compléter le document réponse DR2.

B-2-2 Combien de ports sont libres sur ce commutateur ? Expliquer comment vous pouvez vous en servir pour supprimer certains tranciever externes 100b FX. Par exemple, quelle modification pouvez-vous envisager dans la baie E ?

B-2-3 Rappeler la structure du modèle OSI et situer le commutateur Catalyst 3750 sur ce modèle. Justifier votre réponse.

## B-3 Sauvegarde des configurations

L'outil DOS wrnet.exe (voir annexe 5) permet de sauvegarder, via un serveur TFTP présent sur le réseau à l'adresse IP 10.142.32.101, les configurations des éléments actifs du réseau. C'est la solution choisie par l'administrateur du système pour sauvegarder les configurations de ces éléments actifs (commutateurs/routeurs).

B-3-1 Sur quels protocoles applicatifs, la commande wrnet s'appuie-t-elle pour fonctionner ?

B-3-2 Proposer sur le document réponse DR2 une commande permettant de sauvegarder sur le serveur TFTP de la V.O.A., la configuration du commutateur RSBF1 dans un fichier texte save\_RESBF1.txt.

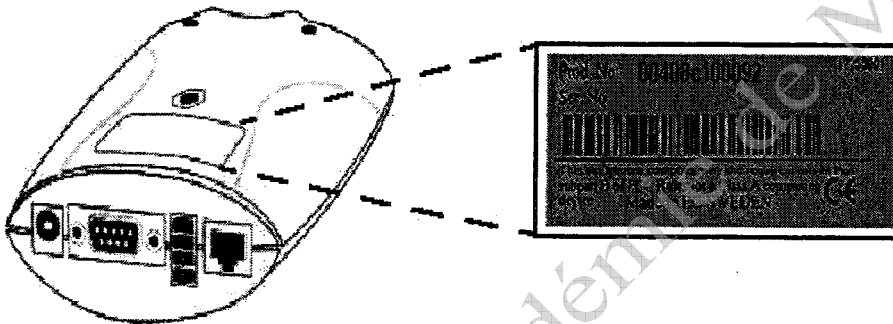
## C- EXTENSION DU RÉSEAU V.O.A. : LIAISON WIFI

Afin de prévenir tout risque d'accident au niveau de cette unité de production, l'entreprise cherche à étendre un système de vidéosurveillance vers le hangar de déchargement de matière première. Afin de pouvoir interconnecter la caméra IP au réseau IP de la V.O.A., il est nécessaire de réaliser une liaison informatique vers le bâtiment qui abritera la caméra.

L'équipe informatique a choisi de mettre en œuvre une liaison par pont WiFi et d'effectuer un filtrage par adresses MAC du trafic sur cette liaison. En effet, il n'existe sur le réseau actuel qu'une station susceptible de visionner ce flux vidéo : (10.142.33.139/24 : 00 02 3F 72 89 25).

### Mise en œuvre de la caméra IP AXIX 2100 :

La caméra IP AXIX 2100 est connectée directement au point d'accès OUTDOOR ROUTER II via sa connectique Ethernet. Son adresse physique est donnée par son numéro de produit présent sur l'étiquette en face arrière de la caméra. De plus, l'équipe informatique a décidé de considérer cette caméra comme un élément actif du réseau et ainsi de fixer son adresse logique en conséquence. La station dédiée à l'administration des éléments actifs du réseau de la V.O.A. devra donc accéder à la console d'administration de cette caméra. Cette station spécifique a pour adresse physique : 00 02 3F 71 B9 46



C-1 Vous venez de prendre possession du matériel nécessaire à la mise en œuvre du pont WiFi, deux OUTDOOR ROUTER II. En vous aidant de l'annexe 6, lister les étapes permettant la configuration des deux ponts WiFi.

C-2 Compléter les 2 fiches de suivi matériels (Document réponse DR3) nécessaires à la mise en œuvre du pont WiFi. Certains paramètres sont libres de votre choix, d'autres sont imposés par la structure du réseau V.O.A..

C-3 Dans le cadre d'une optimisation de la liaison WiFi entre les bâtiments, il est demandé de mettre en œuvre un filtrage par adresse MAC. Expliquer ce choix.

C-4 Définir la table de filtrage MAC à initier dans chacun des ponts WiFi.

C-5 Que représente le terme SNR ? (aidez-vous du document page 27).

C-6 Une valeur SNR élevée indique-t-elle une bonne qualité de liaison ? Pourquoi ?

# ANNEXE 1

Machine	Commentaire	Nouvelle Adresse IP
Routeur MPLS + RNIS	SGT/France télécom	10.142.32.254/24
Routeur 3550	Réseau LAN V.O.A.	VLAN32 : 10.142.32.253/24
		VLAN37: 10.142.37.253/24
Routeur 3750	Réseau LAN V.O.A.	VLAN32 : 10.142.32.250/24
Pile StackWise HSRP	Réseau LAN V.O.A.	VLAN32 : 10.142.32.252/24
Commutateur 29XX	Réseau LAN V.O.A.	VLAN32 : 10.142.32.220-237/24 10.142.32.251/24
Relais de messagerie FT	@Transpac: 194.51.14.x/y	N/A
Relais de messagerie SG		idem
V.O.A.MSG	Serveur NT4 de messagerie Exchange 5.5 BDC	10.142.32.2
V.O.A.SV1	Serveur NT4 de fichier PDC DNS DHCP	10.142.32.1
V.O.A.IMP	Serveur d'impression et de Fax SAP	10.142.32.3
V.O.A.SUS	Serveur MàJ Microsoft Update Service	10.142.32.4
JAURES	Serveur NT4 BD Technique BDC	10.142.32.5
V.O.A.620	Serveur AS400	10.142.32.6
V.O.A.SIL	Serveur W2000 Base de donnée SIL	10.142.32.7

Site	Adresse IP	Masque	Nb Adresses	Passerelle	Id XT	PC principal
Albi	10.142.32.0	255.255.255.0		10.142.32.254	FR0702	XXXXXXXX
Usine	10.142.37.0	255.255.255.0		10.142.32.254	FR0702	XXXXXXXX
Beychac	10.142.33.16	255.255.255.240		10.142.33.14	FR0764	XXXXXXXX
Sérignan	10.142.33.32	255.255.255.240		10.142.33.30	FR1733	XXXXXXXX
Flassans	10.142.33.0	255.255.255.240		10.142.33.46	FR1842	XXXXXXXX
Sète	10.142.33.48	255.255.255.248		10.142.33.49	FR2523	A81DTDEP050
Valence	10.142.33.56	255.255.255.248		10.142.33.57	FR2524	A81DTDEP058



## Les ACL ou Listes de contrôle d'accès

Les ACL (Access Control List) permettent de filtrer des paquets suivant des critères définis par l'utilisateur. Sur des paquets IP, il est ainsi possible de filtrer les paquets entrants ou sortants d'un routeur en fonction :

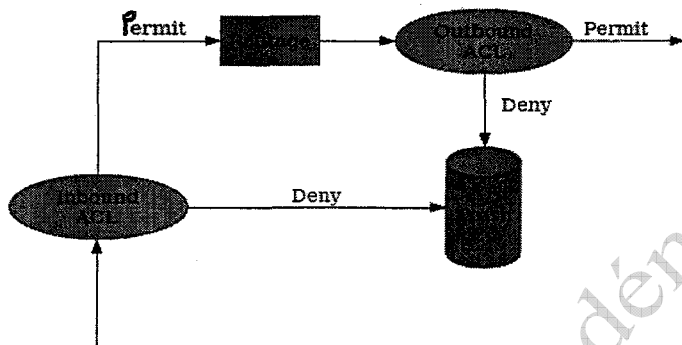
- de l'adresse logique de destination ou source
- du type de protocole (TCP, UDP, ICMP, IGRP, IGMP, ...)
- port source ou port destination
- ...

Il existe essentiellement 2 types d'ACL :

Protocole	Plage
IP standard	1-99, 1300-1999
IP étendu	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX étendu	900-999
Protocole IPX Service Advertising	1000-1099

- Les listes standards : uniquement sur les IP sources
- Les listes étendues : sur l'ensemble des champs des en-têtes IP, TCP et UDP.

Il est possible de résumer le fonctionnement des ACL de la façon suivante :



le paquet est vérifié par rapport au 1er critère défini  
 s'il vérifie le critère, l'action définie est appliquée  
 sinon le paquet est comparé successivement par rapport aux ACL suivantes  
 s'il ne satisfait aucun critère, l'action Deny est appliquée par défaut

Les critères sont définis à partir des informations contenues dans les en-têtes IP, TCP ou UDP. Des masques sont définis pour pouvoir identifier une ou plusieurs adresses IP en une seule définition. Ces masques définissent la portion de l'adresse IP qui doit être examinée ; ainsi 0.0.255.255 signifie que seuls les 2 premiers octets doivent être examinés.

Ces ACL peuvent filtrer, soit le trafic entrant sur l'interface d'un routeur, soit le trafic sortant de l'interface du même routeur, voir filtrer les deux trafics.

La syntaxe générale de création d'une liste d'accès standard est :

access list {1-99} {permit | deny} [source address] [source mask]

La syntaxe générale de création d'une liste d'accès étendue est :

access-list {100-199} {permit | deny} [protocol] [source address] [source mask] [destination address] [destination mask] [operator operand]

### Exemple:

```
#autorise les trames du poste 172.16.3.10 à sortir du routeur par l'interface Eth0 et bloque toutes les autres #
interface Eth0
  ip address 172.16.1.1 255.255.255.0
  ip access-group 1 out
access-list 1 permit 172.16.3.10 0.0.0.0
```

## Saint-Gobain Telecom SGnet corporate DNS architecture NOTES

**Many domains :** There are many heterogeneous domains and subdomains

**Many DNS servers :** There are many DNS servers running; not all of them are known from SGnet, and we have to take care of DNS traffic between them.

**Several parallel update procedures :** DNS information should be updated only once on one DNS only, not manually in each DNS server, modification available for everybody.

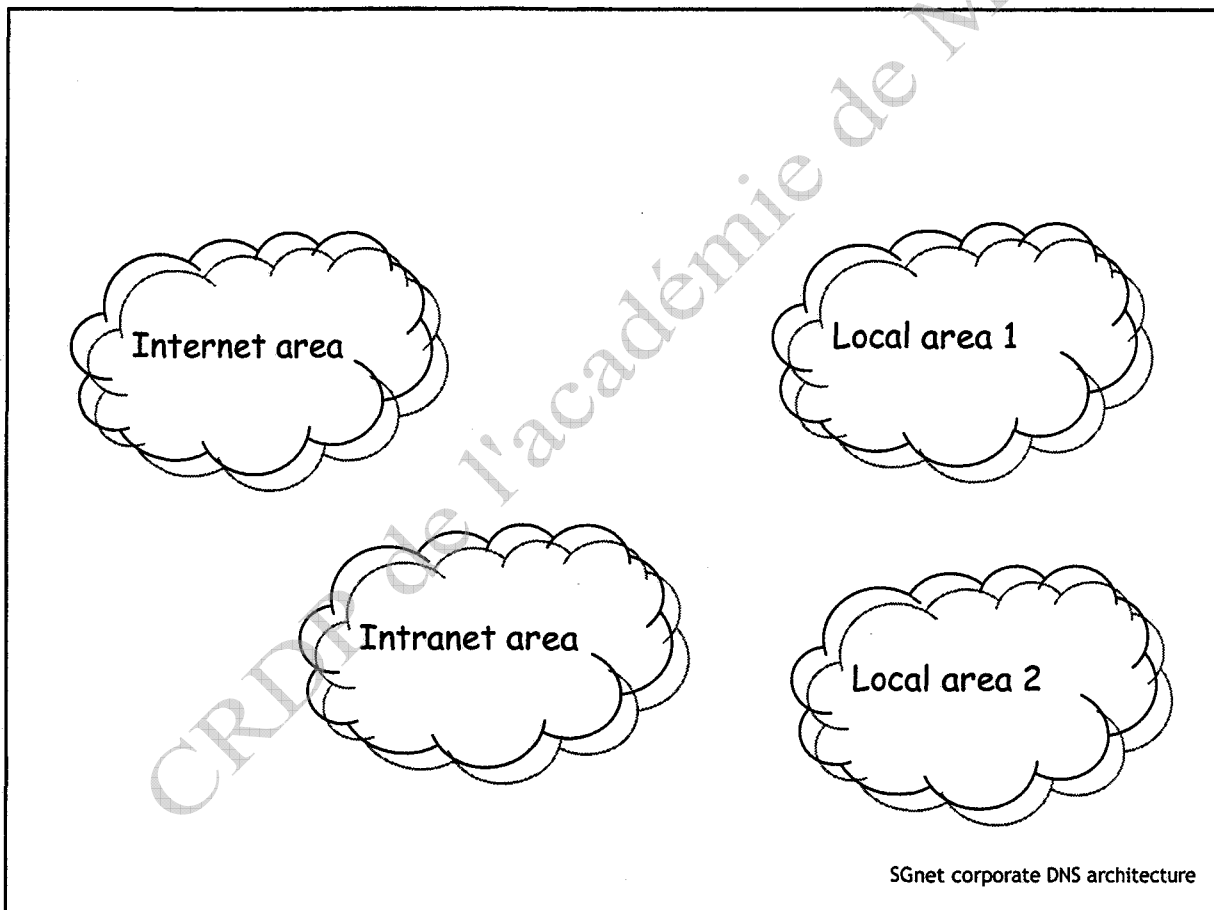
**Several internet access :** There are more and more internet access in the Group, and everybody should use the closest gate for internet access.

**Intranet AND internet resolution :** DNS must be able to solve intranet and internet queries, without any restriction.

**NAT translation :** Zone transfer mechanism doesn't work if NAT function (Network Address Translation) is enabled in one of the routers between 2 DNS servers.

From a DNS point of view, there are 3 kinds of areas :

- local areas,
- one Intranet area,
- one Internet area

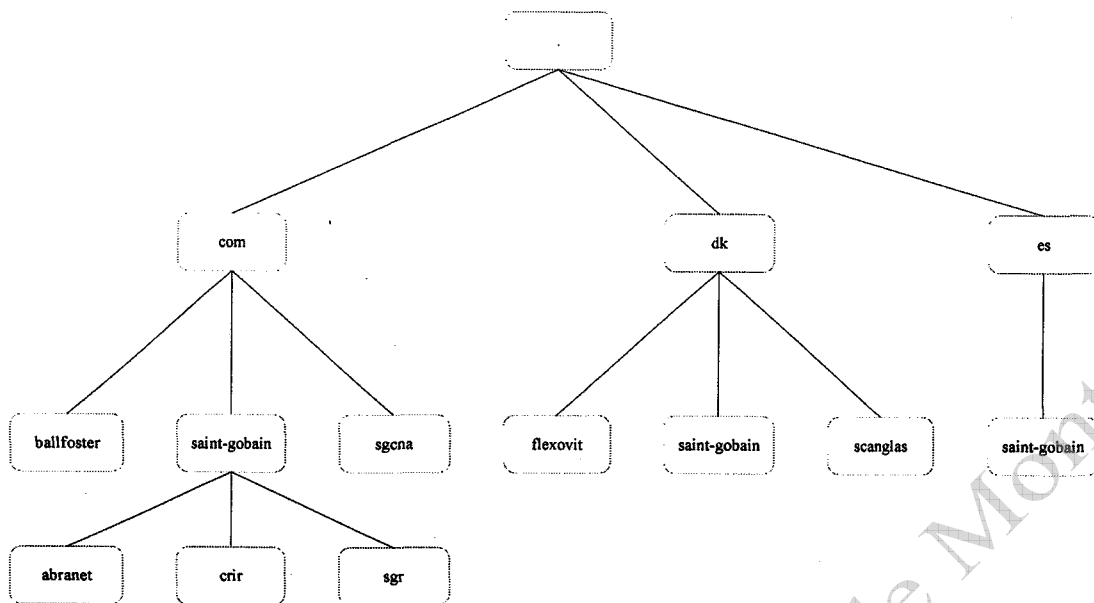


Each local area has its own local DNS. This DNS defines all resources related to the domain, shared and unshared: application servers, web servers, mail routing records, as well as domain controllers, printers, ...

To connect a local DNS to the intranet DNS, i.e. to make a local DNS able to solve non-local addresses (intranet or internet), just a forward to the intranet DNS has to be coded.

There is one primary DNS server managing the intranet area.

This intranet DNS is primary for all intranet domains. It contains records related to intranet resources (i.e. every resource shared by different sites in the group: web servers, application servers, routing mail records, ...). If a same domain is defined in both the intranet DNS and a local DNS, intranet level definitions are a subset of local level definitions.



This illustration shows the zones defined in this DNS; see the forward that reroutes internet DNS queries to an internet DNS.

Primary zone for ballfoster.com
Primary zone for saint-gobain.com
Primary zone for abranet.saint-gobain.com
Primary zone for crir.saint-gobain.com
Primary zone for sgr.saint-gobain.com
Primary zone for sgna.com
Primary zone for flexovit.dk
Primary zone for saint-gobain.dk
Primary zone for scanglas.dk
Primary zone for saint-gobain.es
Forward to internet

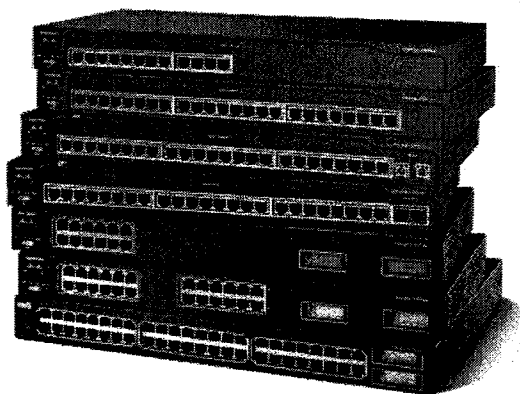
To provide performance and reliability, several copies of the intranet DNS can be installed. They are « secondary DNS » for the intranet zone.

Each of them has its own forward to the local internet access.

**Gamme Cisco Catalyst 2950. Commutateurs d'étage Catalyst 10/100/1000**

Cette gamme de commutateurs 10/100/1000 à détection automatique offre de nombreuses fonctionnalités avancées de qualité de service (QoS) et de traitement des flux multicast.

La gamme de commutateurs Catalyst 2950 est composée de 9 modèles différents permettant de combiner tous les besoins en nombre de ports 10/100 de 12 à 48 ports, les besoins en ports 100FX, ceux en Gigabit cuivre et Gigabit fibre.



Avec une matrice de commutation de 13,6 Gigabits par seconde (Gb/s) et une bande passante maximale de transfert de 10,1 millions de paquets par seconde, le Catalyst 2950 délivre sur tous les ports un débit à la vitesse du médium. Le commutateur Catalyst 2950 supporte des fonctions augmentant les performances tel que le Fast EtherChannel®, le Gigabit EtherChannel et le 802.3ad, offrant jusqu'à 4Gb/s de bande passante entre commutateurs, routeurs et serveurs en agrégeant les liens Ethernet, Fast Ethernet et Gigabit Ethernet entre eux et en répartissant la charge par sessions entre les équipements.

Dénomination commerciale	Nb de port	Ports additionnels
WS-C2950-12	12 10/100 ports	-
WS-C2950-24	24 10/100 ports	-
WS-C2950T-24	24 10/100 ports	2 10/100/1000BaseT ports
WS-C2950C-24	24 10/100 ports	2 100BaseFX ports
WS-C2950SX-24	24 10/100 ports	2 1000BaseSX intégrés
WS-C2950G-12-EI	12 10/100 ports	2 1000BaseX (Gbic)
WS-C2950G-24-EI	24 10/100 ports	2 1000BaseX (Gbic)
WS-C2950G-48-EI	48 10/100 ports	2 1000BaseX (Gbic)

Les entreprises de taille moyenne qui ont une infrastructure de câblage réseau existante en cuivre (Categorie 5, UTP) ont maintenant la possibilité de migrer leurs LAN en Gigabit Ethernet.

Le Catalyst 2950T-24 est doté de deux ports fixes haut débit 10/100/1000BaseT (Gigabit sur cuivre) en plus des 24 ports 10/100 pour connecter les postes de travail.

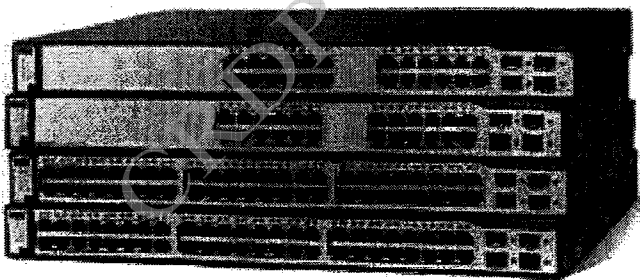
Le Catalyst 2950T-24 offre une solution Gigabit sur cuivre intégrée pour les entreprises de petite et moyenne taille qui veulent faire évoluer leur coeur de réseau en Fast Ethernet vers le Gigabit, et qui veulent pousser le Fast Ethernet jusqu'au poste de travail.

Pour de plus longues distances, la remontée vers le coeur de réseau en fibre est toujours la meilleure des solutions.

### **Caractéristiques techniques Série Catalyst 2950 :**

- Matrice de commutation de 8,8 Gbits/s pour les commutateurs en versions de logiciel SI uniquement et 13,6Gbits/s pour les commutateurs en version de Cisco IOS EI
- 12, 24 ou 48 ports 10Base-T/100Base-TX à détection automatique, chacun fournissant jusqu'à 200 Mbits/s aux utilisateurs individuels, aux serveurs et aux groupes de travail.
- Les Catalyst 2950 (sauf les versions 2950-12, 2950-24, et 2950C-24) possèdent 2 ports Gigabit Ethernet (1000BaseX) intégrés, fournissant une bande passante totale de 4 Gbits/s aux fédérateurs Gigabit Ethernet, aux serveurs Gigabit Ethernet ou entre les commutateurs, sur une infrastructure cuivre (UTP Catégorie 5E et supérieure), fibre (SX, LX, ZX, CWDM), ou propriétaire pour chaîner en Gigabit jusqu'à 9 équipements (GigaStack).
- Le Catalyst 2950C-24 possède, lui, 2 liaisons ascendantes en fibre multimode (100BaseFX) fournissant chacune jusqu'à 200 Mbits/s de bande passante sur une distance de 2 kilomètres maximum.
- Mémoires DRAM 16 Mo et flash 8 Mo embarquées, autorisant les mises à jour logicielles et optimiser l'investissement.
- Agrégation de bande passante via les technologies Fast EtherChannel, Gigabit EtherChannel et 802.3ad, améliorant la tolérance de panne et permettant d'obtenir une bande passante de 400 Mbits/s à 4 Gbits/s entre commutateurs, routeurs et serveurs individuels.

### **Commutateurs Cisco Catalyst 3750**



La gamme Cisco Catalyst 3750 est optimisée pour les déploiements Gigabit Ethernet de forte densité et comprend un large éventail de commutateurs qui répondent aux besoins de connectivités à l'accès, en agrégation ou pour la constitution de petits réseaux fédérateurs.

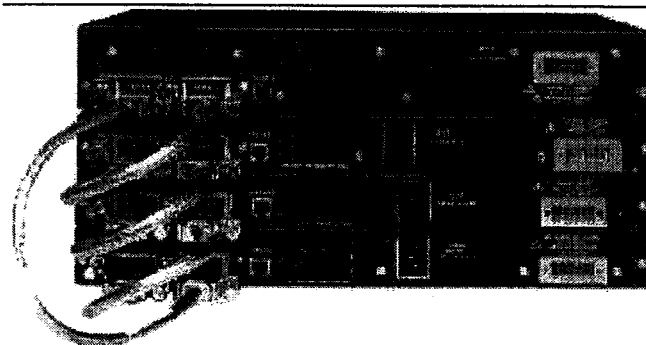
Modèle	Description
Cisco Catalyst 3750-24TS	24 ports Ethernet 10/100 et 2 ports Gigabit Ethernet SFP
Cisco Catalyst 3750-48TS	48 ports Ethernet 10/100 et 2 ports Gigabit Ethernet SFP
Cisco Catalyst 3750-24PS	24 ports Ethernet 10/100 PoE et 2 ports Gigabit Ethernet SFP
Cisco Catalyst 3750-48PS	48 ports Ethernet 10/100 PoE et 4 ports Gigabit Ethernet SFP
Cisco Catalyst 3575G-24T	24 ports Ethernet 10/100/1000
Cisco Catalyst 3750G-24TS	24 ports Ethernet 10/100/1000 et 4 ports Gigabit Ethernet SFP ; 1,5U
Cisco Catalyst 3750G-24TS-1U	24 ports Ethernet 10/100/1000 et 4 ports Gigabit Ethernet SFP ; 1U
Cisco Catalyst 3750G-48TS	48 ports Ethernet 10/100/1000 et 4 ports Gigabit Ethernet SFP
Cisco Catalyst 3750G-16TD	16 ports Ethernet 10/100/1000 et 1 port 10GE Xenpak
Cisco Catalyst 3560G-48PS	48 ports Ethernet 10/100/1000 PoE et 4 ports Gigabit Ethernet SFP
Cisco Catalyst 3750G-24PS	24 ports Ethernet 10/100/1000 PoE et 4 ports Gigabit Ethernet SFP
Cisco Catalyst 3750G-48PS	48 ports Ethernet 10/100/1000 PoE et 4 ports Gigabit Ethernet SFP
Cisco Catalyst 3750-24FS	24 ports Ethernet 100BASE-FX et 2 ports Gigabit Ethernet SFP
Cisco Catalyst 3750G-12S	12 ports Gigabit Ethernet SFP
Cisco Catalyst 3750G-24WS	24 ports Ethernet 10/100/1000 PoE et 2 ports Gigabit Ethernet SFP ; Contrôleur WLAN intégré ; 2U

### Caractéristiques techniques :

Les interfaces physiques 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, 1000BASE-T, compatibles IEEE 802.3z, et les interfaces physiques CWDM sont supportées via des modules SFP remplaçables à chaud qui apportent une grande flexibilité lors du déploiement des commutateurs.

Le protocole Cisco HSRP (Hot Standby Router Protocol) permet la répartition de charge dynamique et la redondance des liens routés. Jusqu'à 32 groupes HSRP sont supportés par unité ou par pile. Le protocole Cisco HSRP permet la création de topologies de routage redondantes à tolérance de pannes.

Ports StackWise d'empilement : câblage cuivre spécifique Cisco StackWise compatible également avec la technologie StackWise Plus des commutateurs de la gamme Cisco Catalyst 3750-E.



## Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix (Gbic/SFP)

Model Number	Description
WS-G5482	= 1000BASE-T GBIC transceiver module for Category 5 copper wire
WS-G5483	= 1000BASE-T GBIC transceiver module for Category 5 copper wire
GLC-T	= 1000BASE-T SFP transceiver module for Category 5
WS-G5484	= 1000BASE-SX GBIC transceiver module for Multi mode Fiber (MMF), 850-nanometer (nm) wavelength
GLC-SX-MM	= 1000BASE-SX SFP transceiver module for MMF, 850-nm wavelength
WS-G5486	= 1000BASE-LX/LH GBIC transceiver module for MMF and SMF, 1300-nm wavelength
GLC-LH-SM	= 1000BASE-LX/LH SFP transceiver module for MMF and SMF, 1300-nm wavelength
WS-G5487	= 1000BASE-ZX GBIC transceiver module for Single Mode Fiber (SMF), 1550-nm wavelength
GLC-ZX-SM	= 1000BASE-ZX SFP transceiver module for SMF, 1550-nm wavelength
GLC-BX-D	= 1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength
SFP-GE-T	= 1000BASE-T SFP transceiver module for Category 5 copper wire, extended operating temperature range and DOM support
WS-X3500-XL	WS-X3500-XL (Cisco GigaStack GBIC and 50 centimeter cable for GigaStack GBIC)

Platform	Switch or Module	Transceiver Module	Minimum Software Release Required	
			Catalyst Operating System	Cisco IOS Release
Catalyst 2950 series	WS-C2950G-12-EI	WS-G5483	Not supported	12.1(6)EA2b
		WS-G5484, G5486, G5487	1	1
	WS-C2950G-24-EI	WS-G5483	Not supported	12.1(6)EA2b
		WS-G5484, G5486, G5487	1	1
	WS-C2950G-24-EI-DC	WS-G5483	Not supported	12.1(6)EA2b
		WS-G5484, G5486, G5487	1	1
	WS-C2950G-48-EI	WS-G5483	Not supported	12.1(6)EA2b
		WS-G5484, G5486, G5487	1	1
	WS-C2950ST-8 LRE	GLC-T (1000BASE-T)	Not supported	12.1(19)EA1c
		GLC-SX-MM, -LH-SM, -ZX-SM	1	1
	WS-C2950ST-24 LRE	GLC-T (1000BASE-T)	Not supported	12.1(19)EA1c
		GLC-SX-MM, -LH-SM, -ZX-SM	1	1
WS-C2950ST-24 LRE997	GLC-T (1000BASE-T)	Not supported	12.1(19)EA1c	
	GLC-SX-MM, -LH-SM, -ZX-SM	1	1	

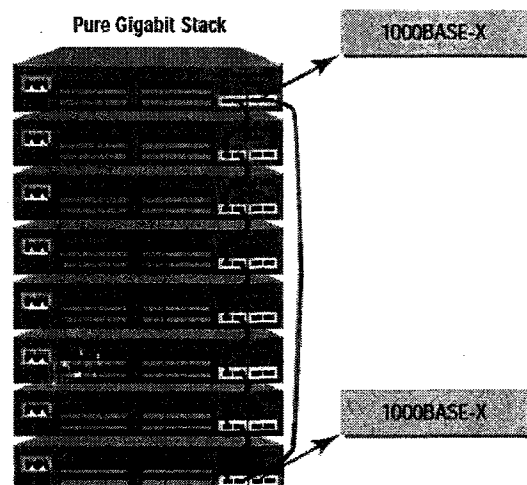
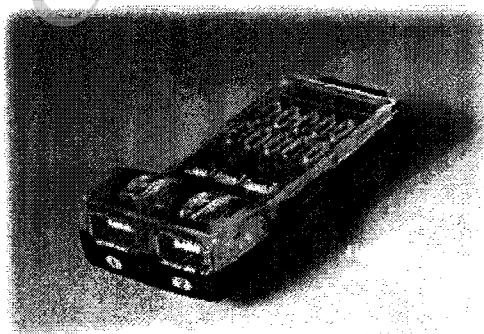


Platform	Switch or Module	Transceiver Module	Minimum Software Release Required	
			Catalyst Operating System	Cisco IOS Release
Catalyst 3750 series (Continued)	WS-C3750G-48TS	GLC-T (10/100/1000)	Not supported	12.1(14)EA1
		GLC-SX-MM, -LH-SM, -ZX-SM	1	1
		GLC-BX-D, GLC-BX-U	Not supported	12.2(25)SEB
	WS-C3750G-24PS	GLC-T (10/100/1000)	Not supported	12.1(14)EA1
		GLC-SX-MM, -LH-SM, -ZX-SM	1	1
		GLC-BX-D, GLC-BX-U	Not supported	12.2(25)SEB
	WS-C3750G-48PS	GLC-T (10/100/1000)	Not supported	12.1(14)EA1
		GLC-SX-MM, -LH-SM, -ZX-SM	1	1
		GLC-BX-D, GLC-BX-U	Not supported	12.2(25)SEB
	WS-C3750G-12S	GLC-T (10/100/1000)	Not supported	12.1(14)EA1
		GLC-SX-MM, -LH-SM, -ZX-SM	1	1
		GLC-BX-D, GLC-BX-U	Not supported	12.2(25)SEB
	ME-C3750-24TE-MA and ME-C3750-24TE-DA	GLC-T (10/100/1000)	Not supported	12.1(14)AX
		GLC-SX-MM, -LH-SM, -ZX-SM	1	1
		GLC-BX, -D, -U		12.2(25)EY2
WS-C3750-24FS-S	GLC-T (10/100/1000)	Not supported	12.2(25)SEB	
	GLC-SX-MM, -LH-SM, -ZX-SM			
	GLC-BX, -D, -U			

### Cisco Systems GigaStack Gigabit Interface Converter WS-X3500-XL

The Cisco Systems GigaStack® Gigabit Interface Converter (GBIC) is a versatile, low-cost, Gigabit Ethernet stacking GBIC that offers high-speed interconnectivity between Catalyst® 3550, 2950G, 3500 XL and modular Catalyst 2900 XL Switches.

The GigaStack GBIC is implemented in a standard GBIC form, which offers customers the highest level of deployment flexibility and scalability—using available Gigabit Ethernet GBIC ports for high-performance stacking today while preserving the option to migrate to standard Gigabit Ethernet uplinks tomorrow.



Microsoft Windows XP [version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.

A:\>wrnet /?

WrNet v1.2 Copyright 2001 www.NetLatency.com

A program to use SNMP to instruct a Cisco router to copy its RunningConfig to a TFTP server.

To make sure this program runs correctly, add "snmp-server community WORD rw" to your Cisco router configuration. Replace "WORD" with the SNMP community name of your choice.

Usage:        **WRNET**        **ipAddress**    **community**    **TFTPserver**    **filename**    **[-l]**

Arguments:

- ipAddress = IP address of device (or DNS name)
- community = SNMP read/write community name on router
- TFTPserver = IP address of TFTP server (or DNS name as resolved by the server)
- filename = directory and filename to save config
- [-l] = Output success/failure information in logfile format

Extrait de la configuration du commutateur RESBF1 :

.....  
ip address 10.142.32.230 255.255.255.0  
.....

ip default-gateway 10.142.32.252  
ip http server  
ip http authentication local  
.....

snmp-server engineID local 000000090200003080C8F580  
snmp-server community public RO  
snmp-server community private RW  
snmp-server location Baie M  
snmp-server contact Service Informatique  
snmp-server chassis-id 0x10  
radius-server source-ports 1645-1646  
.....

## Outdoor Router

### Basic Configuration Steps

This section will describe a 5-step installation approach to configure your Outdoor Router-II devices to service an Avaya Wireless Outdoor Router Network.

To install and configure the Outdoor Router-II proceed as follows:

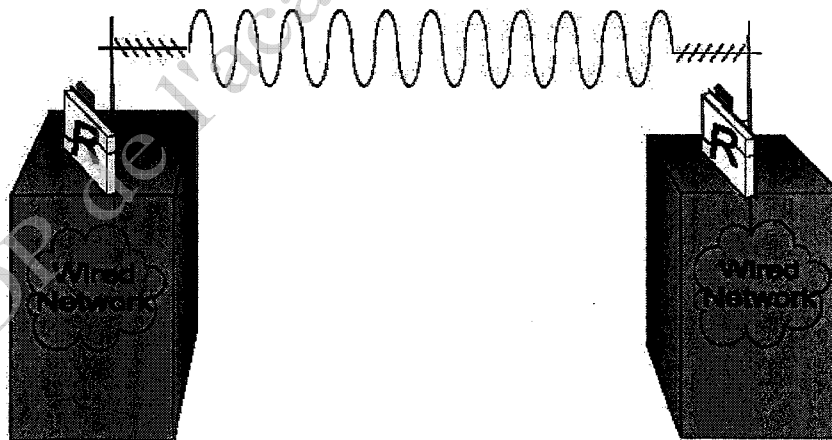
1. Install the Outdoor Router-II devices .
2. Use the OR Manager program to connect to the Outdoor Router (and change the factory-set IP address).
3. Modify the factory-set default parameters (optional).
4. Save the configuration parameters to a back-up file.
5. Upload the configuration to the Outdoor Router-II device.

Repeat steps 2 to 5 for each of the Outdoor Router-II devices that you wish to install.

To connect to a Outdoor Router-II, you need to address each device via its IP address. Each new Outdoor Router-II device comes with a factory-set default IP address (153.69.254.254), that you must change upon first configuration. You can either use:

- A unique IP address value that falls within the range of IP addresses allocated to your organization.
- A user-defined IP address value if your organization does not use IP addressing (please consult the section "Creating a Template File" on page 5-36).

**Figure 0-1 Basic Point-to-Point Topology**



To set up a Point-to-Point link you will need two Outdoor Router-II devices that will be connected to an outdoor antenna installation. One device will be setup as Point-to-Point Master and the other as the Point-to-Point Slave (see Table 0-1).

**Table 0-1 Basic Point-to-Point Topology Settings**

Outdoor Router	Slot A	Slot B
A	Point-to-Point Master	varies
B	Point-to-Point Slave	varies

## **Bridge Setup**

The Bridge Setup screen can be used to optimize the performance of your wireless network. The factory-set configuration of your Outdoor Router-II device is a "transparent" bridge mode, that is, all Ethernet traffic will be bridged without filtering.

One of the ways to optimize the performance of your wireless networks is to prevent "redundant" traffic from being transmitted over the wireless network. Redundant traffic may include:

- Specific network protocols exchanged by networking devices such as servers that are not relevant to the wireless clients.
- Broadcast and/or multicast messages exchanged by specific networking devices such as servers that are not specifically addressed to the wireless clients.
- "Junk traffic" such as error messages that are generated by malfunctioning devices, or as the result of incorrect network configurations that could have been avoided (e.g. closed network loops).

Filtering redundant traffic will save the bandwidth of the wireless medium for the wireless stations, optimizing throughput efficiency for these stations.

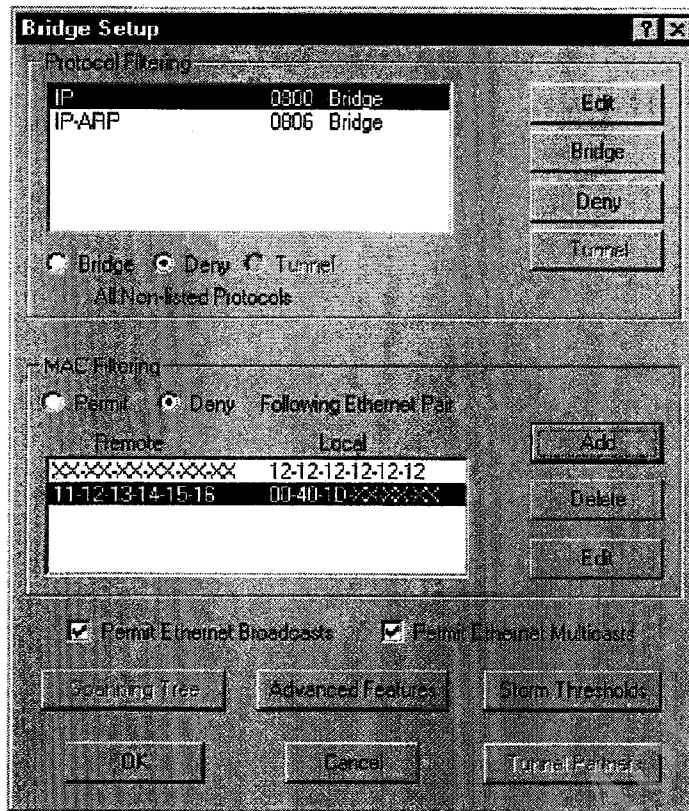
## **Eliminating Redundant Traffic**

Data transmitted via your network can be divided in two major types of data:

- **True Data** - is data communicated between network stations, such as file-transfer or e-mail. This "True Data", usually referred to as "payload", also includes messages that were retransmitted one or multiple times as a result of a collision, malfunctioning cable connection or poor radio link.
- **Network Overhead Data** - is data exchanged between network services to control the dataflow. This overhead data that usually referred to as "traffic load", includes protocol and broadcast messages and/or error messages that result from a configuration mismatch.

The ratio of network overhead in relation to "True Data" differs from one networking service to another. However when the ratio of network overhead is more than actually required, this may affect the performance of your wireless network, because your "True Data" has to share the bandwidth capacity with the network overhead.

In general, in order to optimizing performance of the wireless network, you should limit the protocols bridged by the Outdoor Router systems only to those protocols that are necessary for your network. In many cases, bridging only IP and IP-ARP packets will allow your wireless systems to connect without excessive overhead from the IPX/SPX systems on your network.



Optimizing wireless performance via the Bridge Setup menu can be achieved in the following ways:

- Protocol Filtering to permit or deny specific networking protocols from being bridged to the wireless interface (see page 5-5).

#### Static MAC Address Filter

To filter out traffic exchanged between stations that is not required to be sent or received via the wireless medium, you can set the "MAC Filtering" in the bottom section of the Bridge Setup window. The default value, "<All Address Pairs Permitted>" will be acceptable for most networking environments.

You can use this option to filter broadcast or multicast messages exchanged between wired servers that can receive each others' messages via the wired network. You can also use this feature to prevent traffic from a wireless customer's private servers from being bridged onto the wireless network.

To explicitly filter out traffic between such devices:

1. Add the MAC Addresses of both devices as a pair in the Static MAC Address filter list
2. Select the 'Deny' Following Ethernet Pair radio button.

When 'Deny' Following Ethernet Pair is selected, messages will be forwarded over the wireless link unless they are between stations listed. All traffic that one of the stations wishes to send to any other (non-paired) MAC Address will be either permitted.

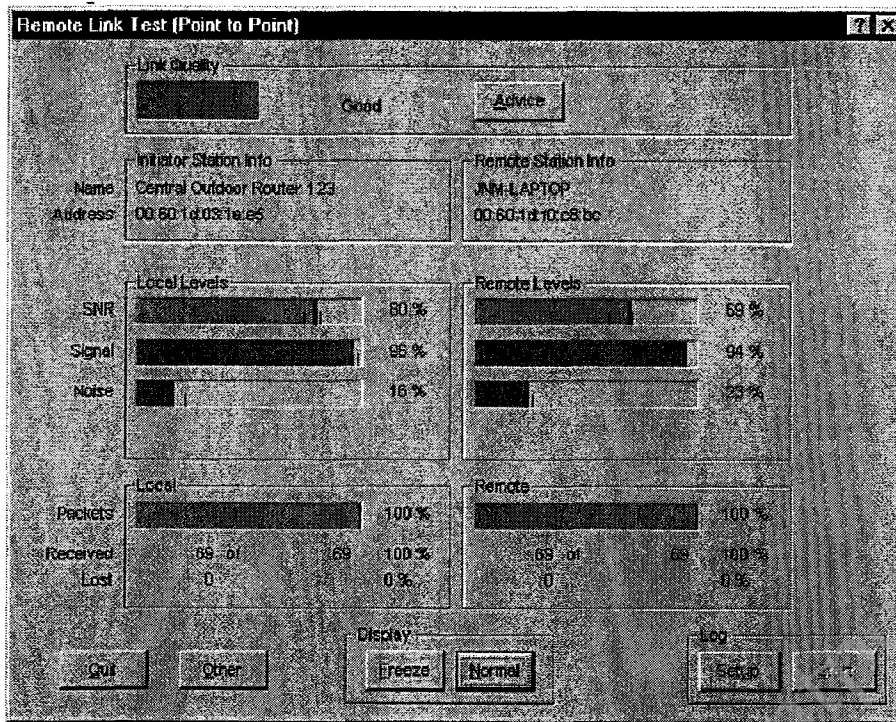


Table A-1 Factory-Set Configuration

<b>Outdoor Router Identifiers</b>	
IP Address: 153.69.254.254 <sup>1</sup>	Subnet Mask: 255.255.255.0
Read Password: public	Read/Write Password: public
<b>ORINOCO PC Card Interface Settings</b>	
RF-Channel: 2.462 MHz—France 2.484 MHz—Japan 2.422 GHz—All other countries	
<b>IEEE 802.11b Access Point Settings</b>	
WaveLAN Network Name: WaveLAN Network <sup>2</sup>	
Wireless Cell ID: MAC Address of the IEEE 802.11 PC Card.	
Medium Reservation: Disabled	
Transmit Rate: High (11 Mbps)	
<b>Outdoor Router Settings</b>	for Central Outdoor Router      Outdoor Router type: Central Outdoor Router
	for Remote Outdoor Router      Outdoor Router type: Remote Outdoor Router (Point-to-Point Slave)
	Transmit Rate: Low (1 Mbps)

- 1 When using IP networks, change this IP address to a unique address in the range assigned to your organization.
- 2 When your network includes MS-DOS stations using the IEEE 802.11 WaveLAN DOS ODI driver, you are advised to change the value to a name that consists of "UPPER CASE" characters only.

Plan de fréquence

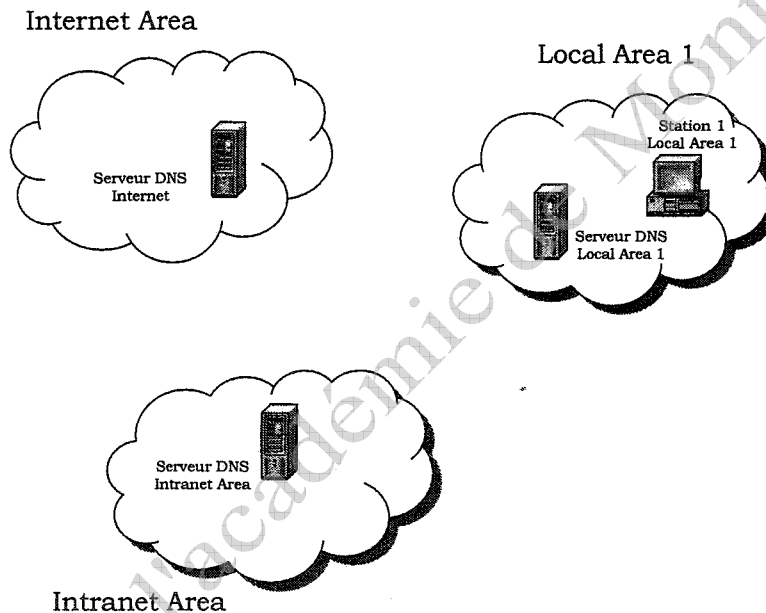
Numéro du canal	Fréquence Américaine (FCC) (GHz)	Fréquence Européenne (CEPT) (GHz)	Fréquence JAPON (GHz)
1	2,412	2,412	2,412
2	2,417	2,417	2,417
3	2,422	2,422	2,422
4	2,427	2,427	2,427
5	2,432	2,432	2,432
6	2,437	2,437	2,437
7	2,442	2,442	2,442
8	2,447	2,447	2,447
9	2,452	2,452	2,452
10	2,457	2,457	2,457
11	2,462	2,462	2,462
12	Interdit	2,467	2,467
13	Interdit	2,472	2,472
14	Interdit	Interdit	2,484

**A-0-3 :**

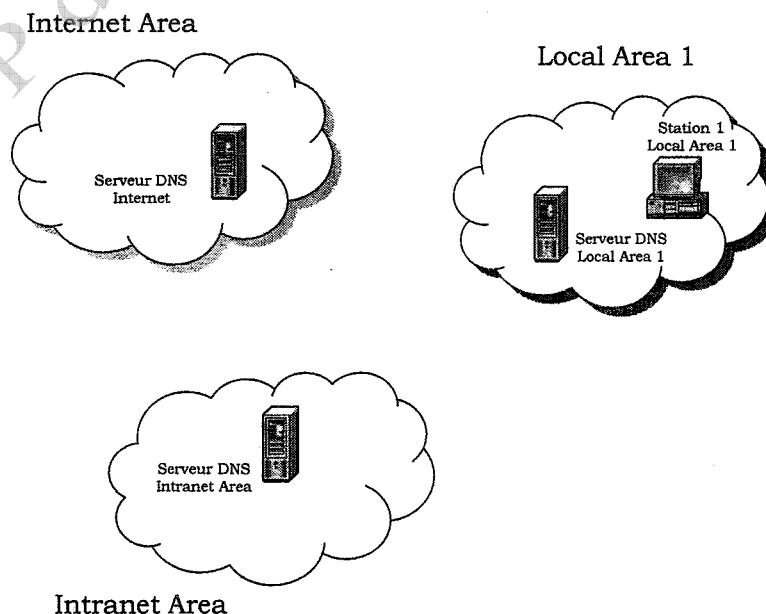
Site	Adresse IP	Masque	Nb Adresses	Passerelle	Id XT	PC principal
Albi	10.142.32.0	255.255.255.0	.....	10.142.32.254	FR0702	XXXXXXXX
Usine	10.142.37.0	255.255.255.0	.....	10.142.32.254	FR0702	XXXXXXXX
Beychac	10.142.33.16	255.255.255.240	.....	10.142.33.14	FR0764	XXXXXXXX
Sérignan	10.142.33.32	255.255.255.240	.....	10.142.33.30	FR1733	XXXXXXXX
Flassans	10.142.33.0	255.255.255.240	.....	10.142.33.46	FR1842	XXXXXXXX
Sète	10.142.33.48	255.255.255.248	.....	10.142.33.49	FR2523	A81DTDEP050
Valence	10.142.33.56	255.255.255.248	.....	10.142.33.57	FR2524	A81DTDEP058

**A-4-4 :**

**Cas n°1 : La résolution DNS demandée ne peut être faite que par le serveur DNS de la zone Intranet**



**Cas n°2 : La résolution DNS demandée ne peut être faite que par le serveur DNS de la zone Internet**



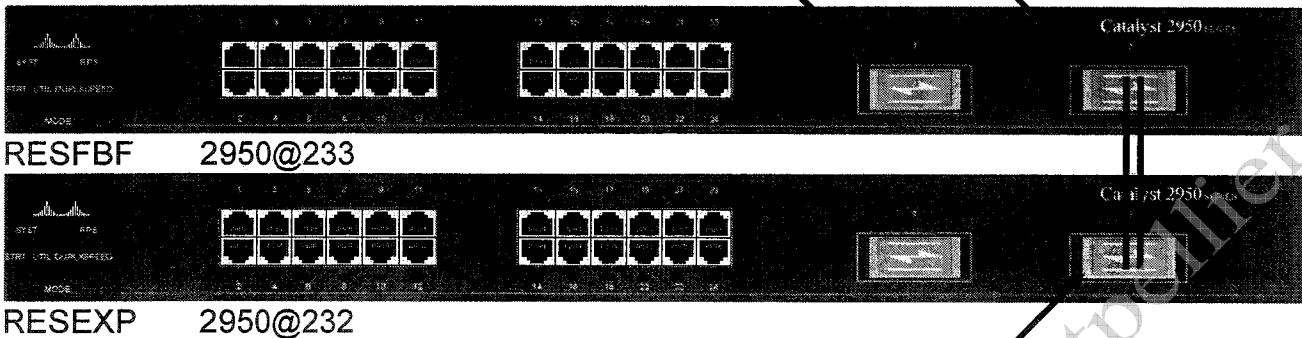


B-1-2 :

Dénomination commerciale commutateurs : .....

Module 1 : .....

Module 2 : .....



Module 3 : .....

B-2-1 :

Dénomination commerciale du commutateur : .....

Description : .....

Nombre et dénomination commerciale des modules Fibre :

Nombre : ..... Dénomination : .....

Nombre et dénomination commerciale des modules GEth :

Nombre : ..... Dénomination : .....

B-3-2 :

Nom de la communauté lecture/écriture : .....

Nom du fichier de sauvegarde : .....

Adresse IP du serveur TFTP : .....

Adresse IP du commutateur : .....

Commande proposée : .....

**Document réponse : DR3**

**C-2 :**

<b>Type de matériel</b>	Point d'accès WiFi
<b>N° immatriculation V.O.A.</b>	WIFI BRI 1
<b>Emplacement géographique</b>	Bâtiment matière
<b>Référence matériel</b>	OUTDOOR ROUTER II
<b>Configuration</b>	
<b>Date de dernière configuration</b>	11/02/05
<b>Paramétrage du périphérique</b>	
Adresse MAC	00 40 1D 30 22 14
Adresse IP	
Login administrateur	
Mot de passe	
SSID	WIFIV.O.A.
Taux de transfert d'information en Mb/s	11Mb/s
Topologie du matériel	Point to Point Master
Canal de transmission	
Opération effectuée le ___ / ___ / _____ par LE CANDIDAT	

<b>Type de matériel</b>	Point d'accès WiFi
<b>N° immatriculation V.O.A.</b>	WIFI BRI 2
<b>Emplacement géographique</b>	Bâtiment hangar déchargement
<b>Référence matériel</b>	OUTDOOR ROUTER II
<b>Configuration</b>	
<b>Date de dernière configuration</b>	11/02/05
<b>Paramétrage du périphérique</b>	
Adresse MAC	00 40 1D 30 22 12
Adresse IP	
Login administrateur	
Mot de passe	
SSID	WIFIV.O.A.
Taux de transfert d'information en Mb/s	
Topologie du matériel	
Canal de transmission	
Opération effectuée le ___ / ___ / _____ par LE CANDIDAT	

# Schéma global de l'architecture réseau informatique V.O.A.

