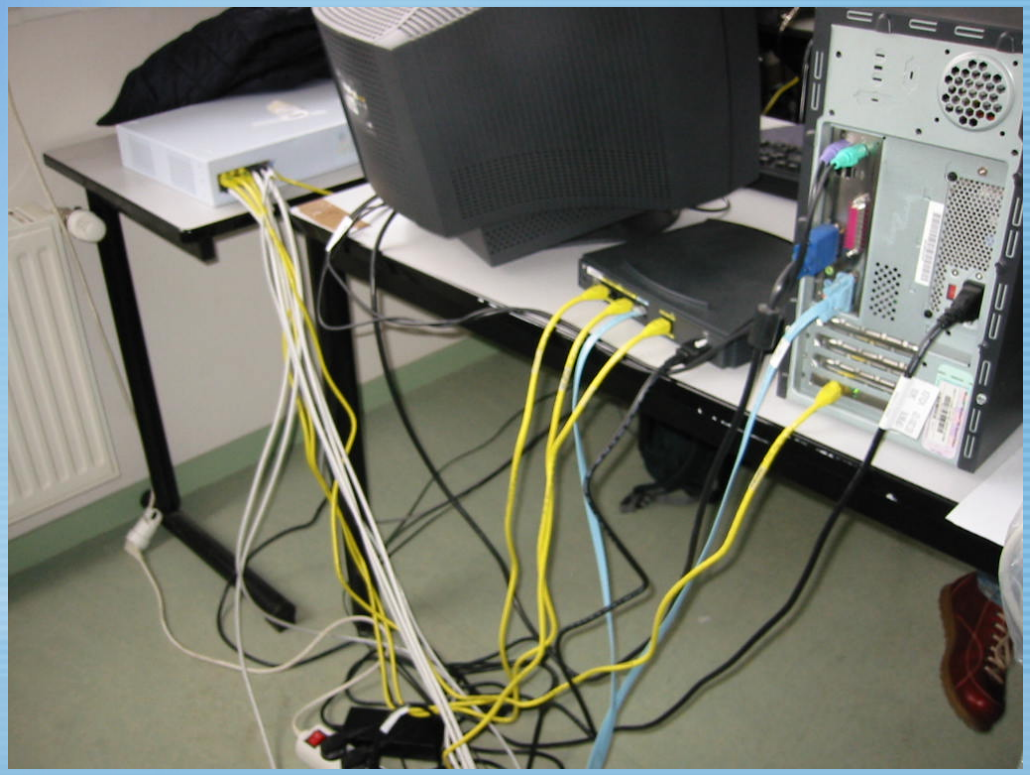
Architecture réseaux sécurisé



C. Gouinaud ISIMA

Chapitre I - Modélisation

Retour au modèle

- Problème d'architecture logique
  - Modélisation de flux
  - Modélisation de sécurité
- Problème d'architecture physique
  - Installation physique
  - Installation logiciel

L'art du cloisonnement

HTTP TCP IP 802.3 ATM 802.3 IP TCP HTPP

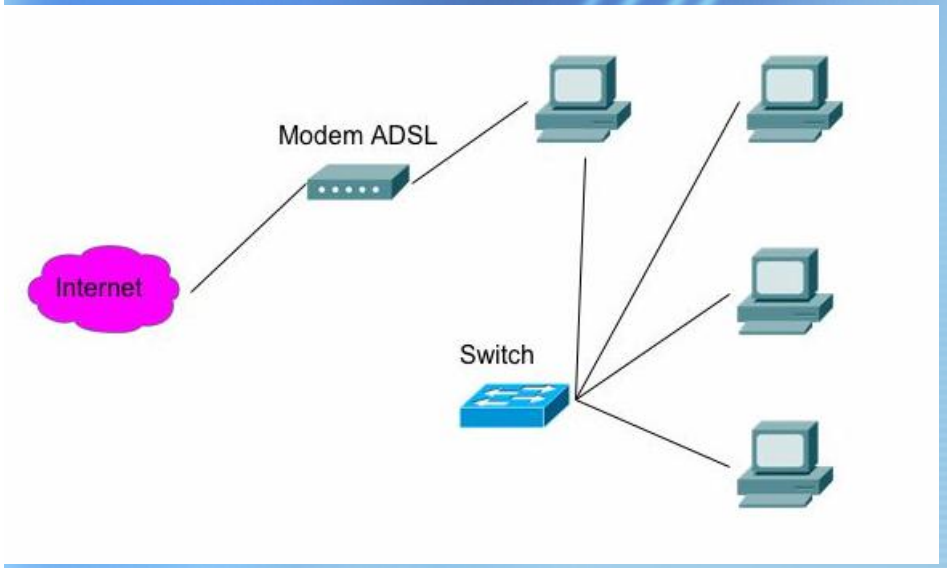
- Sécurisé : c'est limité l'extension géographique des protocoles
- Introduire une coupure dans la chaîne des protcoles.

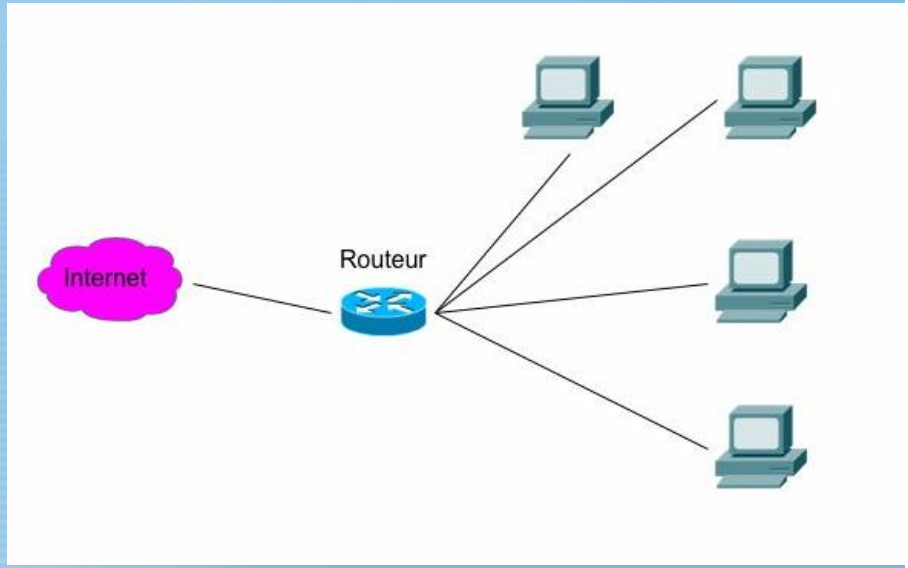
L'art de faire efficace

Architecturé un réseau c'est :

- Facilité les communications
- Fiabilisé les communications
- Accélérer les communications
- Limiter les coût d'installation
- Limiter les coût de maintenance

Exemple simple





Constat :

Du fait de leur conception :

- Protocoles peu sécurisé
- La couche session est absente
- Tout cela est très anciens (1975)
- On ne peut pas espérer d'évolution rapide

Il faut se débrouillé !

Principales attaques

- Denial of service = blocage de service
- Inondation (flooding) SYN
- Spoofing = usurpation d'adresse
- Détournement de service (ex :SMTP)
- Vol de session
- Rebond par vol de mots de passe
- Les chevaux de trois
- Les vers
- Le vol de données
- L'usurpation téléphonique

Architecture de sécurité

Plusieurs buts :

- Empêcher l'écoute
- Empêcher la corruption
- Empêcher l'utilisation abusive
- Rendre robuste au incident

Sécurité générique

- Rendre étanche ou rendre incompréhensible
- Sauvegardé et rendre inaccessible
- Diffusé partiellement
- Cloisonné suivant les besoins
- Avoir une politique de sécurité

Politique de sécurité

Liste de recette et procédure visant à ce :

- Que tout les employé soit conscient du problème et accepte les régles
- Que tout le monde connaisse les régles
- Que chacun sache ce qu'il doit faire
- Qu'il existe des procédure pour :
  - Eviter les perte ou coruption de données
  - Limiter les indisponibilité dues aux malveillance
  - Faciliter les reprise en cas de problème

Sécurité consentie

- Pour être efficace une politique de sécurité doit être :
- Acceptable et justifié
- Raisonnable
- Le moins contraignante possible
- Tenable dans le temps

Enquête de sécurité

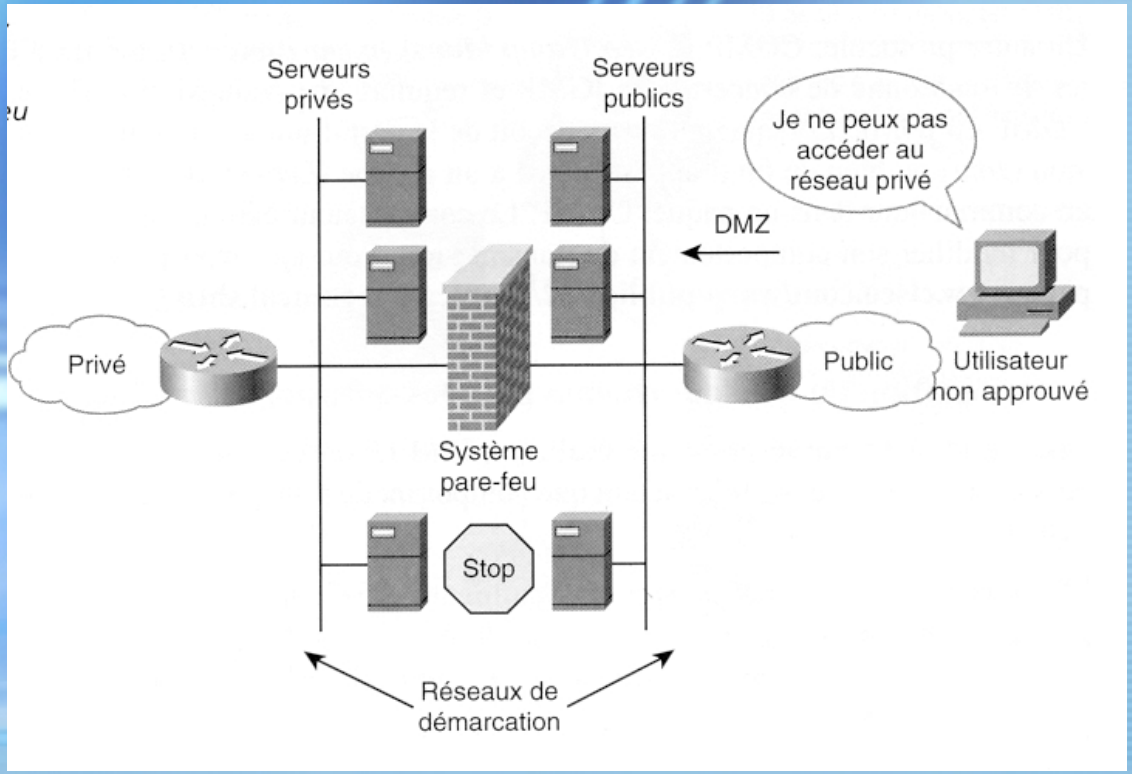
- Fondamentale pour l'acceptation
- Comporte au moins :
  - Efficacité perçus des procédures
  - Difficultés introduites
  - Problèmes rencontrés
  - Améliorations possibles

Niveau de coupure

Il faut choisir le niveau :

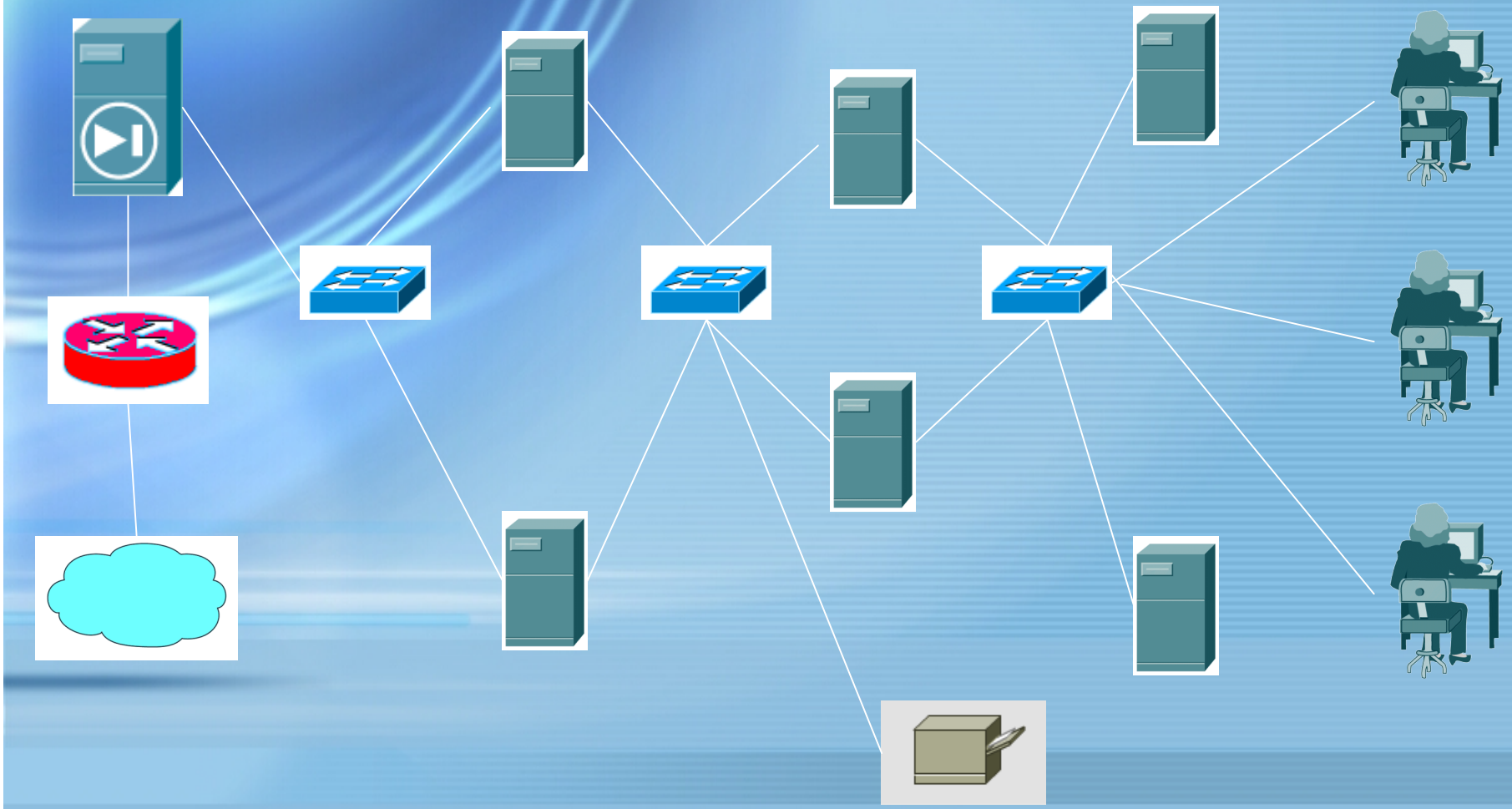
- Suivant le type de réseau physique
- Suivant le type de protocole
- Suivant le risque financier
- Suivant les possibilités technique
- Suivant le type de trafic

Modèle classique DMZ

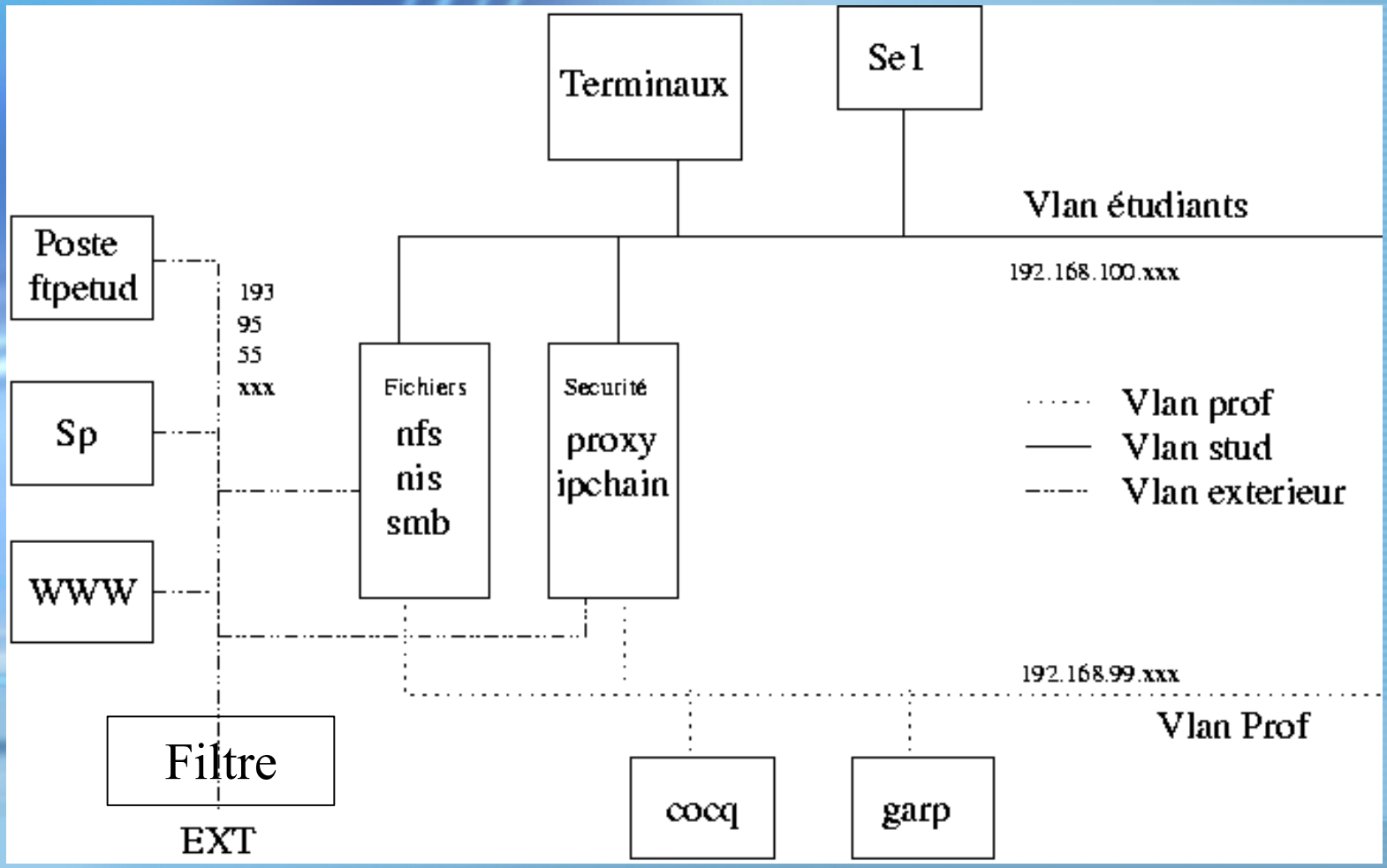


- Zone de confiance
- Zone de démarcation
- Repose sur un firewall

Conception à base de proxy



Modèle ISIMALIN



Architecture réseaux et modèles

- Retour au but = type d'utilisation
- Niveaux de décisions
- Modèle classique

Types de trafic

- Trafic système
- Trafic interactif
- Trafic de communication

Besoin différent en :

- Débit
- Délais/gigue
- Connexion

3 Niveaux différents

- Physique Câble et câblage média …
- Appareillage actif choix et disposition
- Configuration des serveurs et des services

Les trois obéissent à des règles différentes

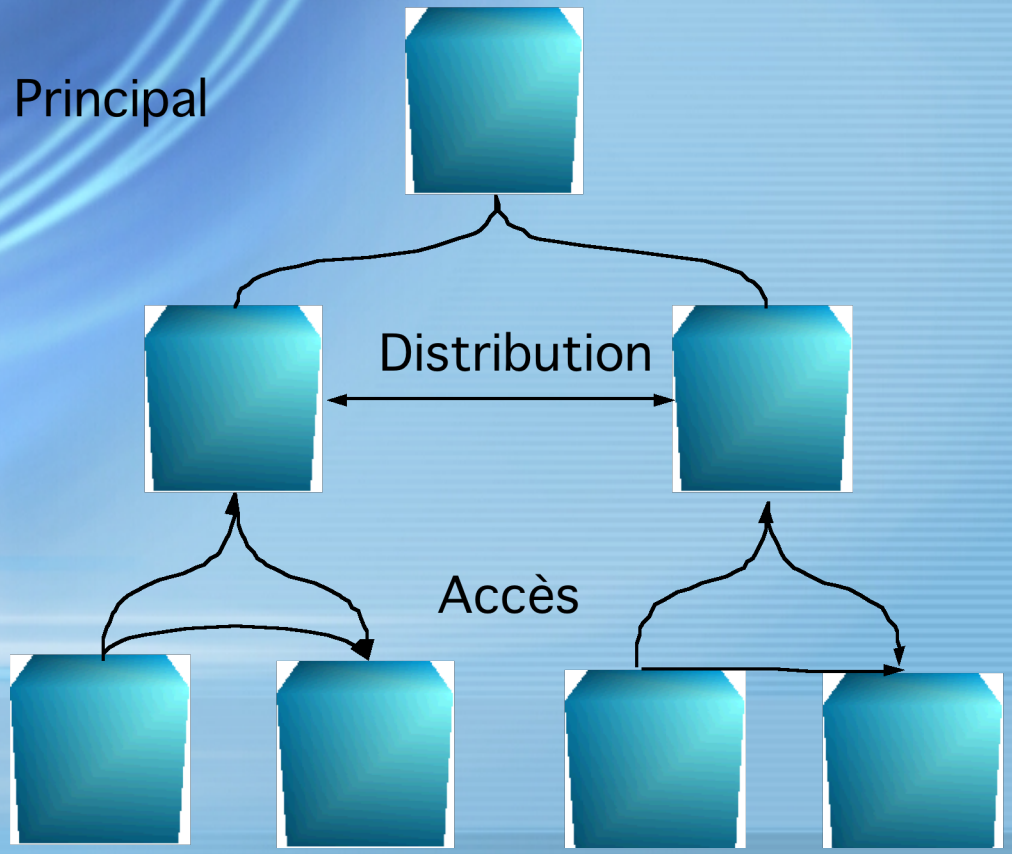
Modèle 3 tiers

- Répondre au besoin de cloisonnement
- Répondre au besoin de communication inter-service
- Accélérer le fonctionnement des intra-services
- Faciliter le diagnostic des pannes
- Limiter l'étendu des pannes
- Refléter une organisation logique

Modèle 3 tiers (suite)

- Un tiers d'accès
  - Communication locales
- Un tiers de distribution
  - Flux de données d'entreprise
- Un tiers principal
  - Transport entre les sites distants

Modèle 3 tiers (suite)



Tiers principal

- Commutation a haute vitesse
- Ni nommage, ni routage
- Protocole HIS, ATM, Frame relay
- Chemin redondant
- Pas forcément le plus rapide

Tiers de distribution

- Convention de nommage et de numérotation
- Sécurité et accès au service
- Routage
- Gestion des profils de trafic (qos)
- Cloisonnement niveaux MAC

Tiers d'accès

- Segmentation logique
- Isolation des LAN
  - Limitation du Broadcast
  - Optimisation de bande passante
- Distribution des services
  - Accès serveur départementaux

Avantage de la conception hiérarchique

- Évolutivité
- Facilité d'implémentation
- Facilité de dépannage
- Prévisibilité
- Support de protocoles
- Facilité de gestion

Modèle d'architecture

- Ce sont des guides de conception
- Ils ont des vocations différentes
  - Performance
  - Fiabilité
  - Sécurité
- Il faut inventer son modèle

Un peu de bon sens

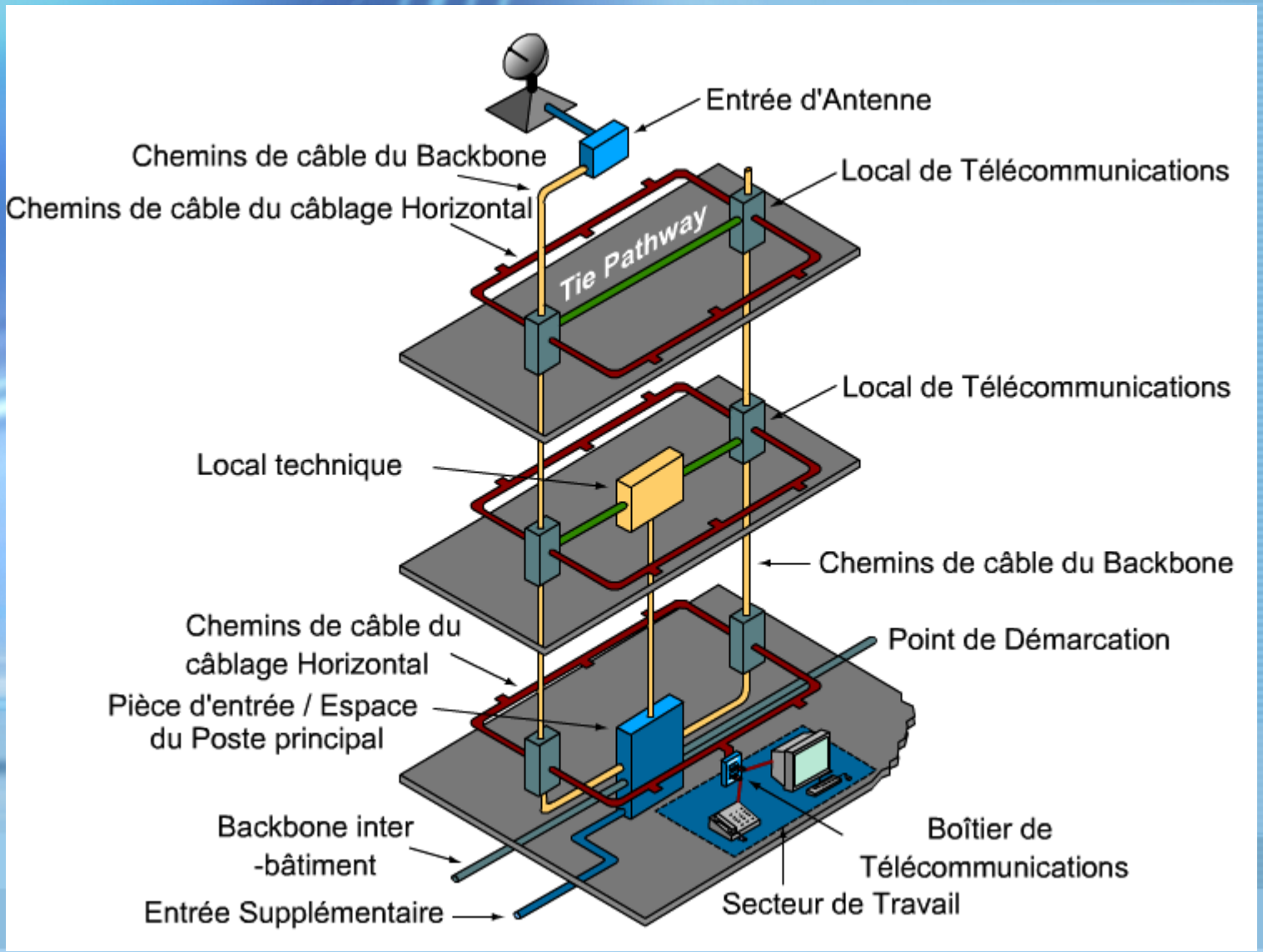
- Centralisation des fichiers
- Sauvegarde
- authentification
- Surveillance
- Rigueur

Chapitre II – conception physique

Rappel appareillage

- Media
- Commutateur
- Routeur
- Relais
- Filtre
- Serveur

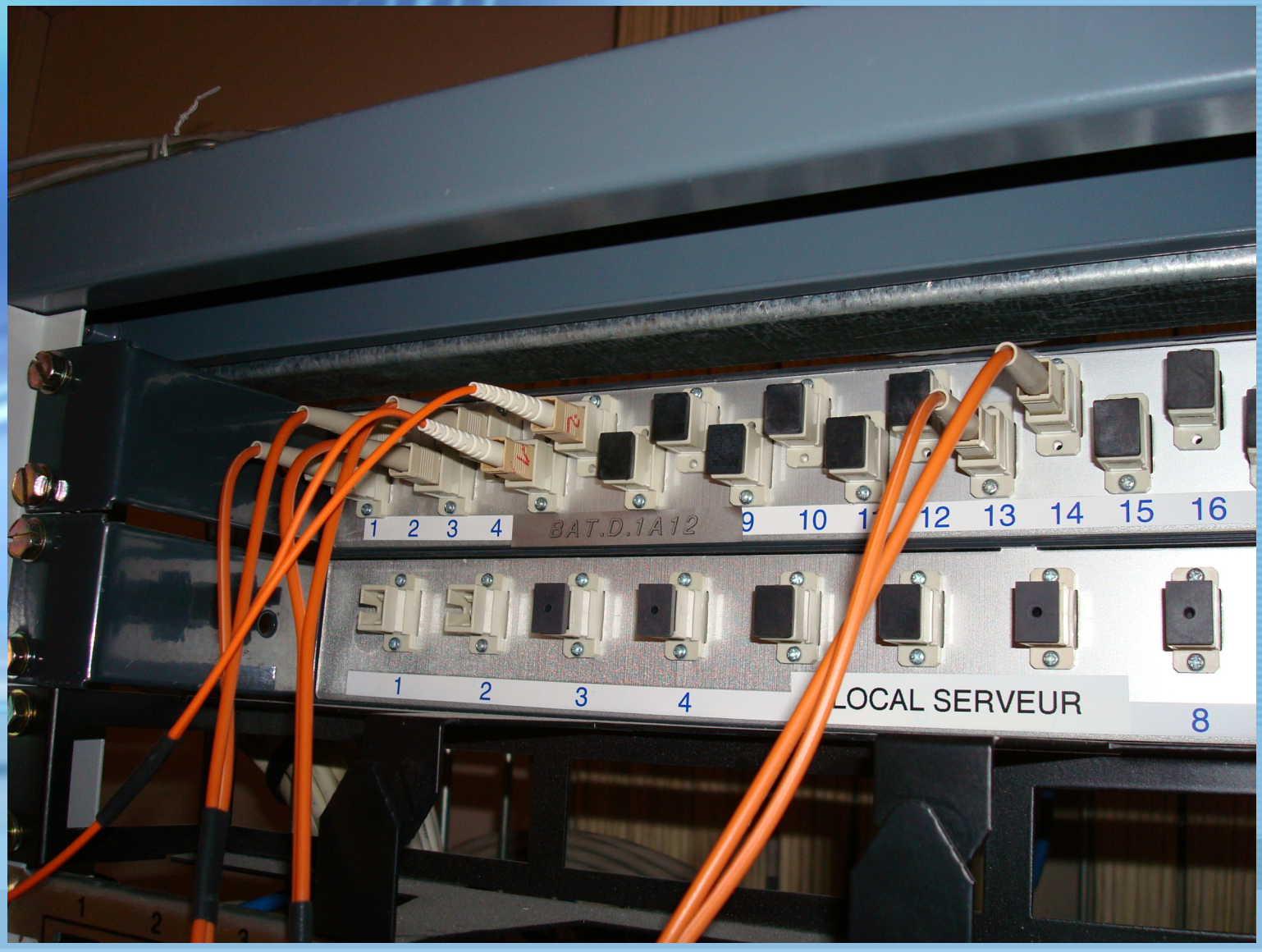
Câble et câblage



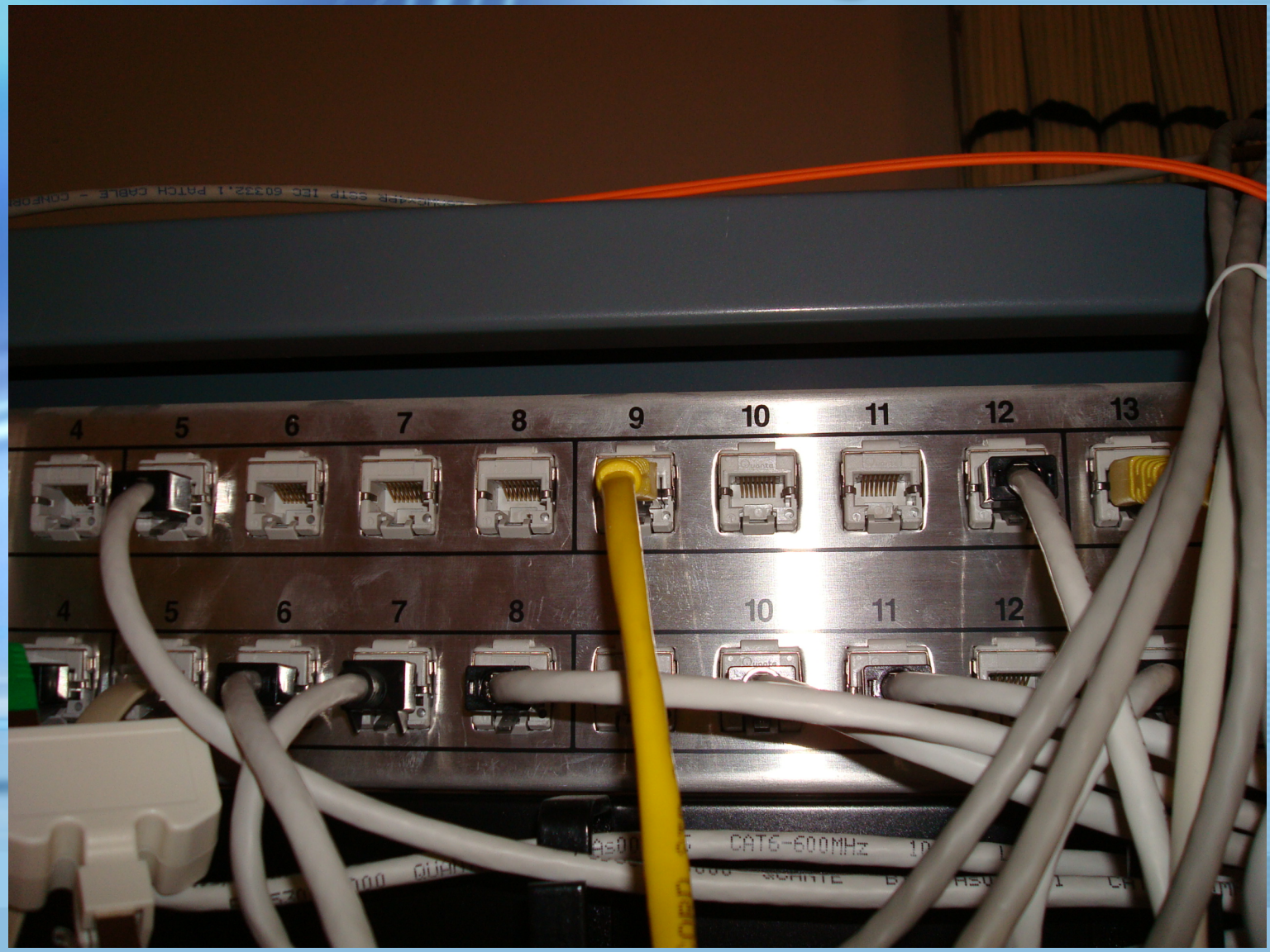
Type de câble

- Cuivre
  - Câble coaxial
  - Paire torsade catégorie 6 STP
- Fibre optique
  - Multimode (10 gb/s)
  - Monomode (100 Mb/s)

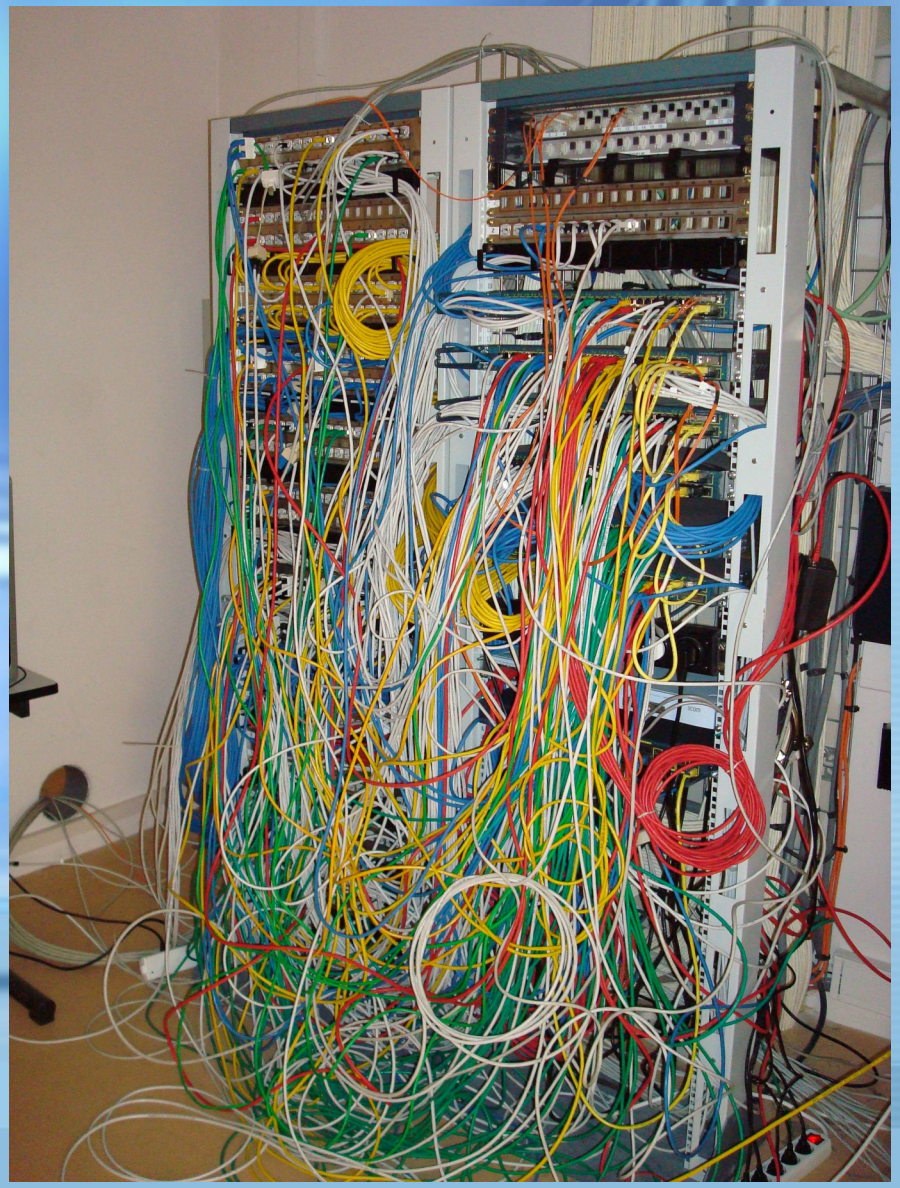
Panneau de brassage optique

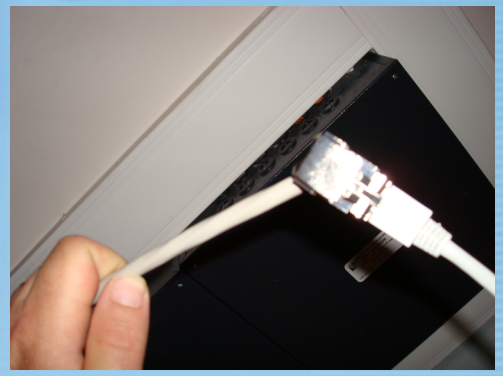


Panneau de brassage cuivre



Baie de brassage





Cuivre/optique

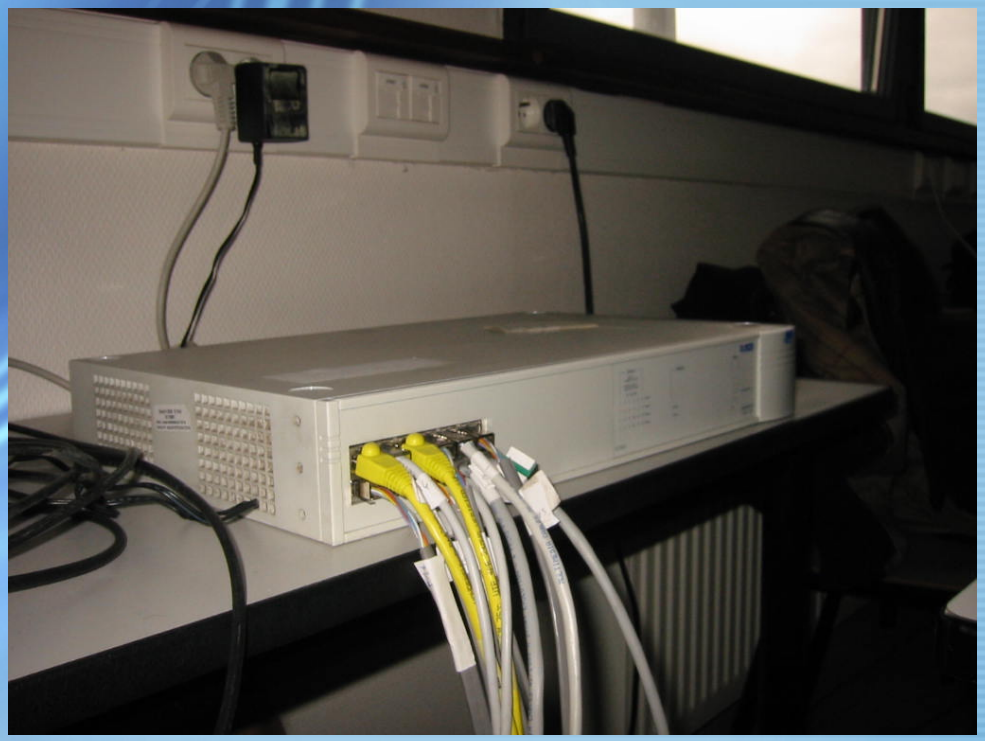
Cuivre :

- Coût cable+actif
- Facilité d'installation
- Interface répandue

Fibre optique:

- Débits
- Isolation++
- Atténuation++
- Sécurité++
- Connecteurs chers
- Appareillage cher

HUB/Switch

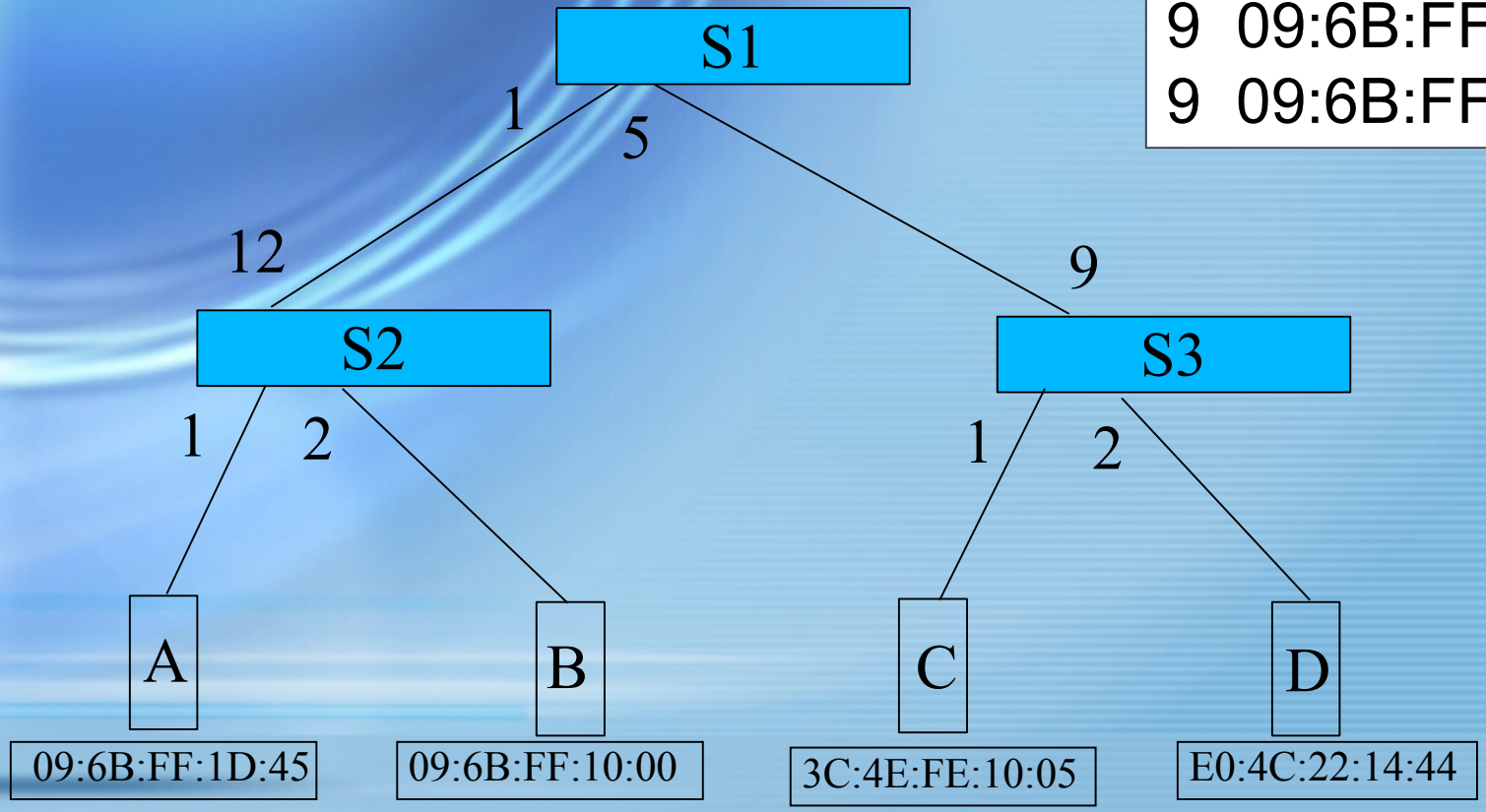


- Switch = Commutateur niveau MAC
- Administrable

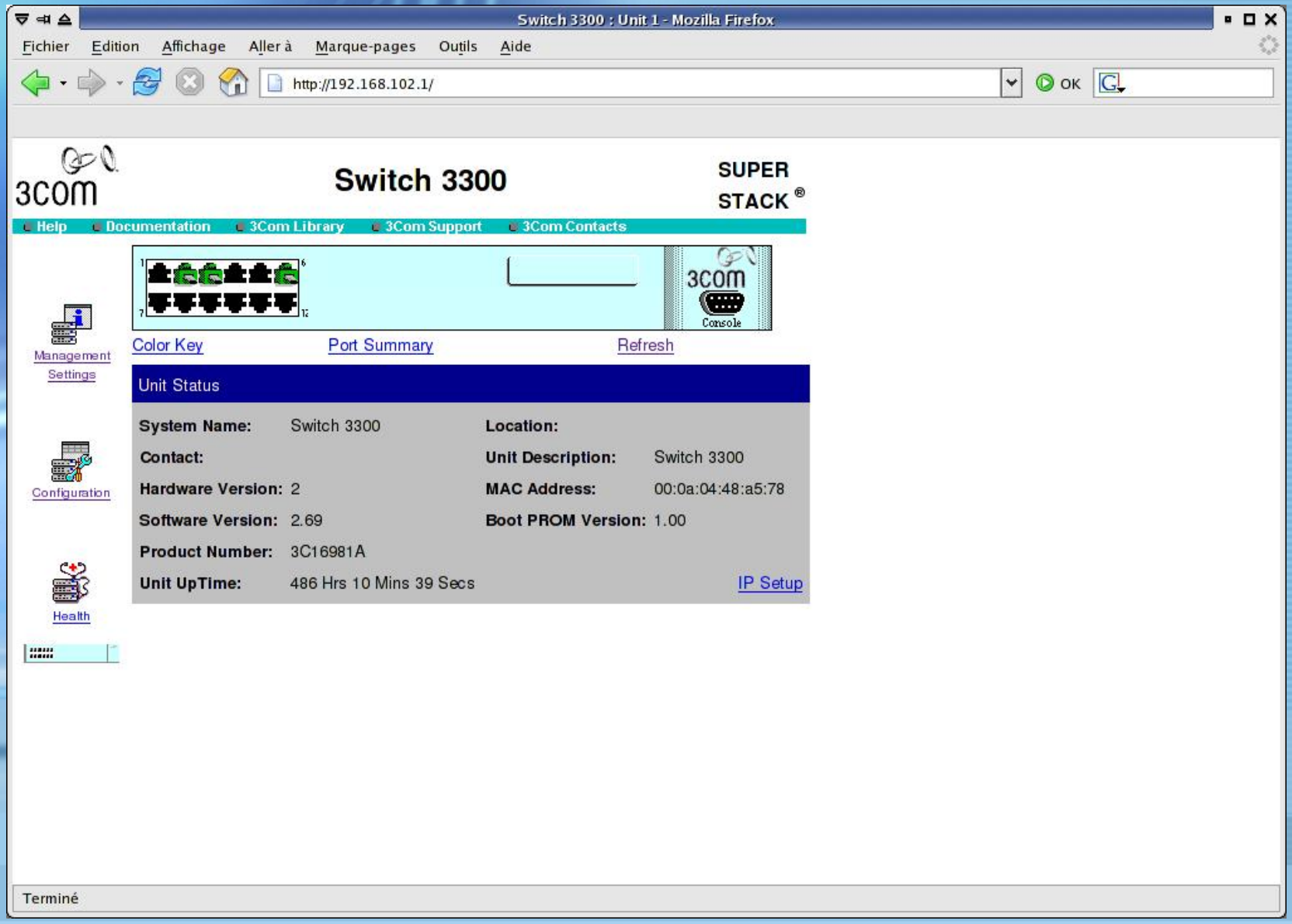
HUB/Switch

Table CAN

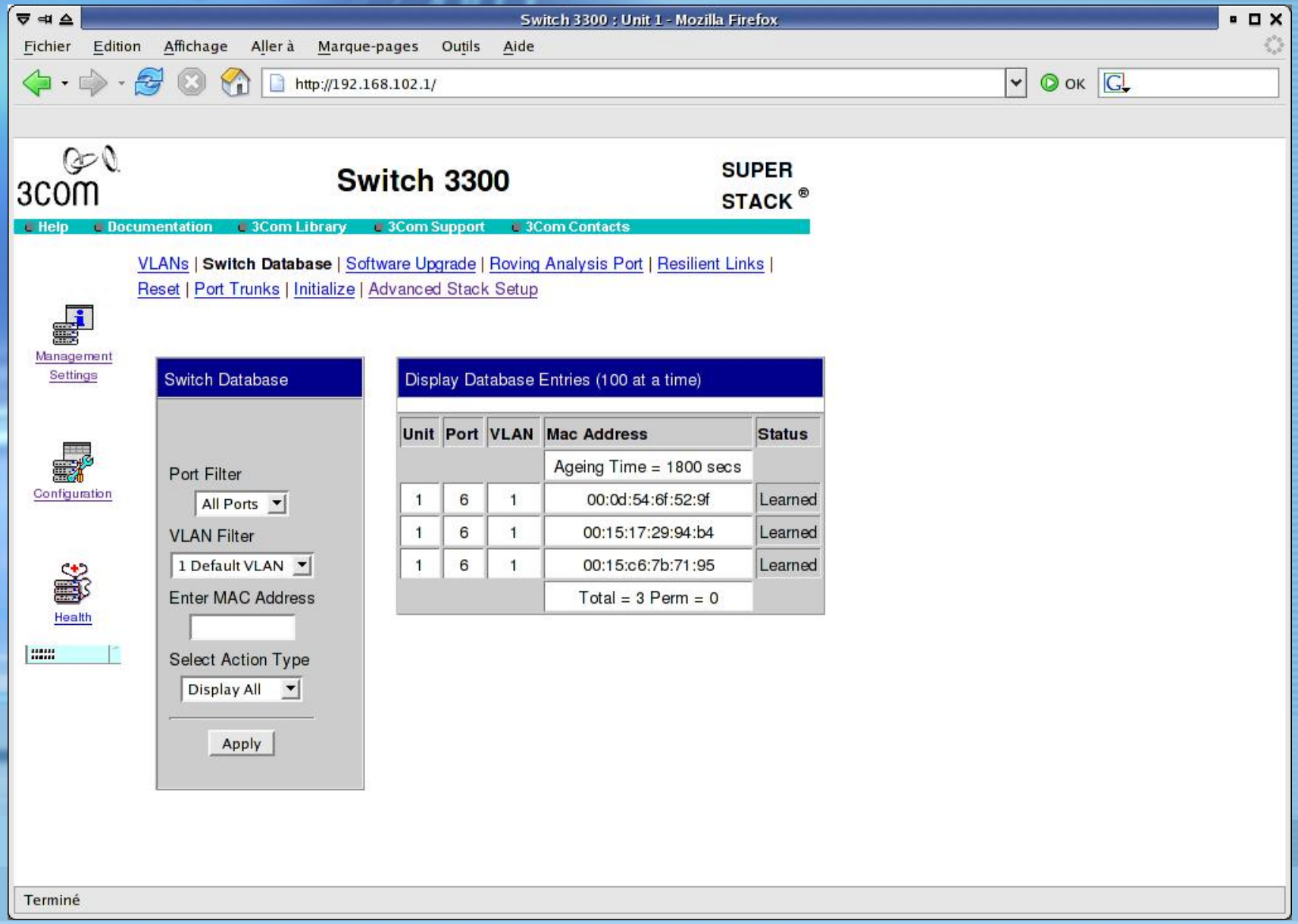
	E0:4C:22:14:44
2	3C:4E:FE:10:05
9	09:6B:FF:1D:45
9	09:6B:FF:10:00



HUB/switch administration



HUB/switch administration



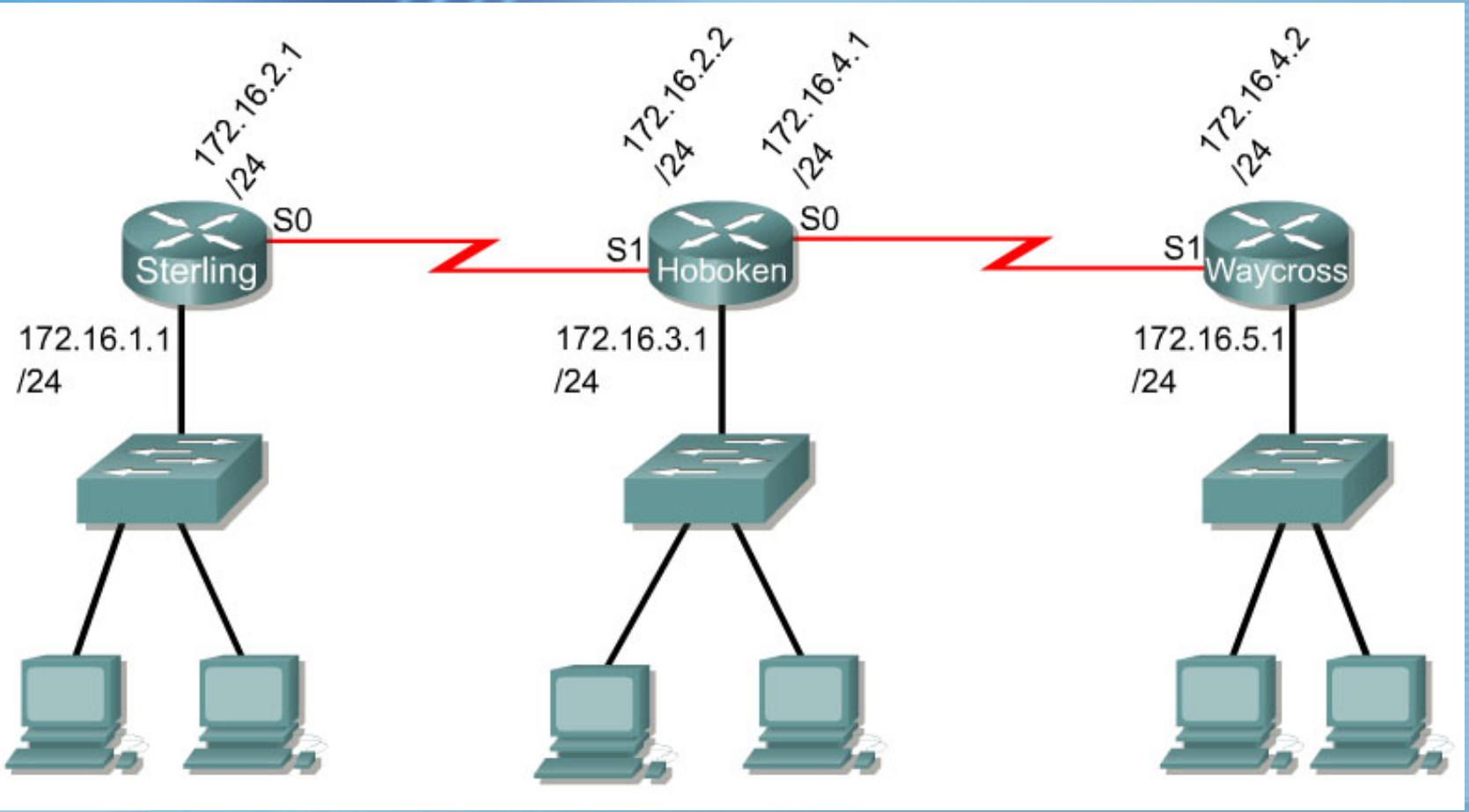
Router

- Commutateur niveau IP
- Plusieurs interface (réel/virtuel)
- Configurable
- Capacité de filtrage
- Capacité de masquage
- Capacité d'adressage dynamique
- Détermine et applique des routes

Fonctionnement interne

- PC
  Carte interface + logiciel
- Appliance
  Joli boite + interface
- Constructeur
  ASIC + Système spécialisé

Utilisation des routeurs



Protocole de routage

- Statique
- Dynamique
  - Intérieur
    - A vecteur de distance, RIP, RIP V2
    - A état de lien

    IGRP,OSPF
  - Extérieur

    BGP

Proxy

- Passerelle logiciel
- Implémente un ou plusieurs protocole
  - http, https, ftp (ex squid)
  - Socks
  - Tunel ssh
- Cache le destinataire final

Firewall

- Fonction de filtrage IP
- Utilise des informations des 7 couches
- Plusieurs mode :
- Filtrage IP source:port dest:port
- Filtrage statefull (utilise la direction)
- Filtrage relais + masquage
- Relais de circuit (socks)

Différence routeur filtrant/firewall

- Les routeurs calcul le filtre pour chaque paquet
- Les routeurs n'inspecte pas le contenu
- Les deux fonts du relayage/masquage d'adresse

Sans fil (WIFI)

- Norme IEEE 802.11
- Un seul domaine de collision
- Un seul domaine d'écoute
- Problème spécifique
  - Roaming
  - Terminaux caché
  - Bruitage du signal/echo
  - Canaux de focntionement

Matériel WIFI

- Carte Réseaux
- Access point
  - HUB/SWICTH …
  - Liaison vers ethernet
  - Fonction DHCP
- Pont
  - Prolongation de réseau

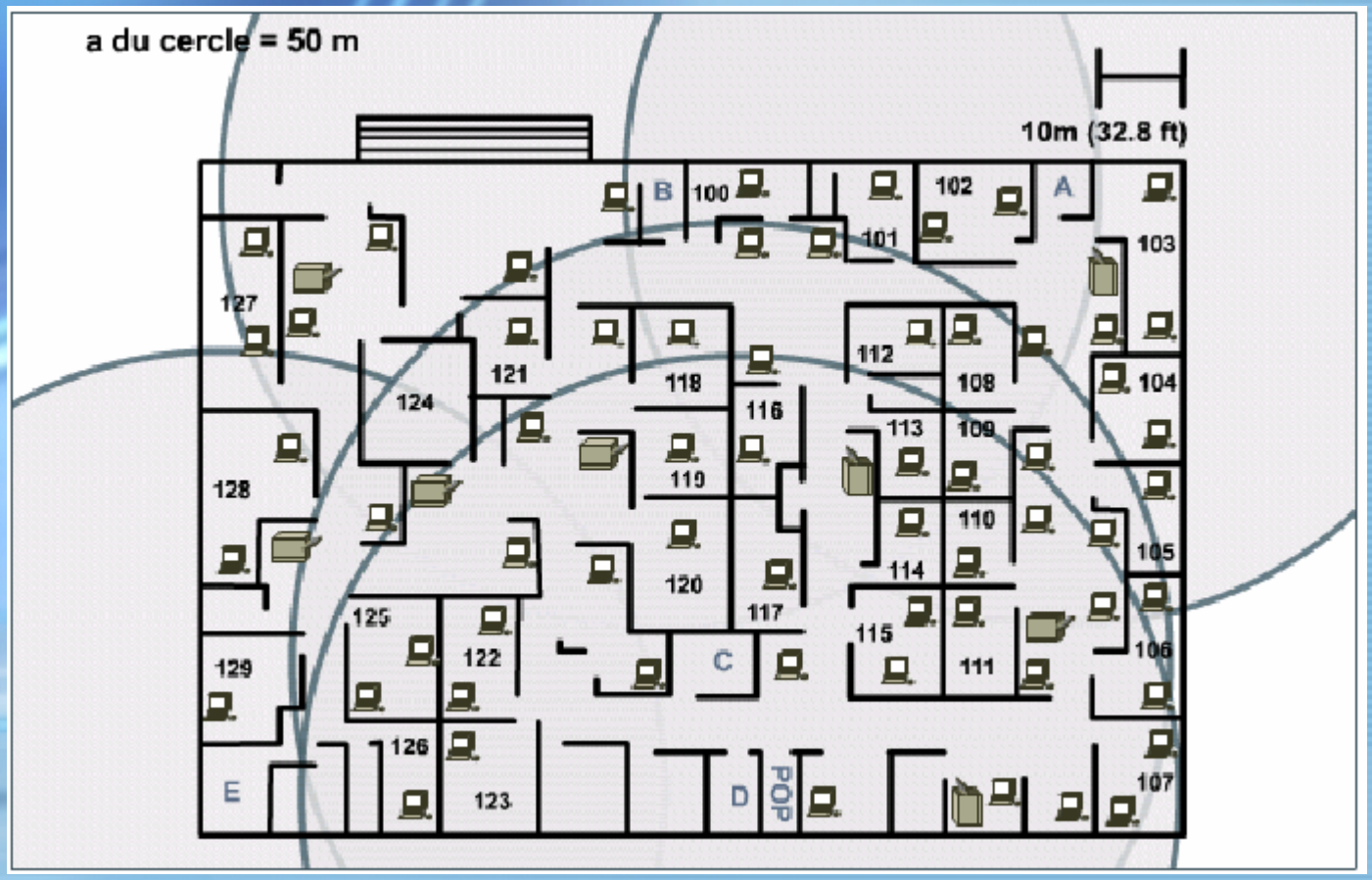
Deux façons de faire des réseaux

CABLAGE LAN 1

Coût et problèmes :

- Longueur des câble (10 %)
- Equipement terminaux (20 %)
- Installation (80 %)
  - Perçage
  - Pose de goulote
  - Prise

Câblage LAN 2

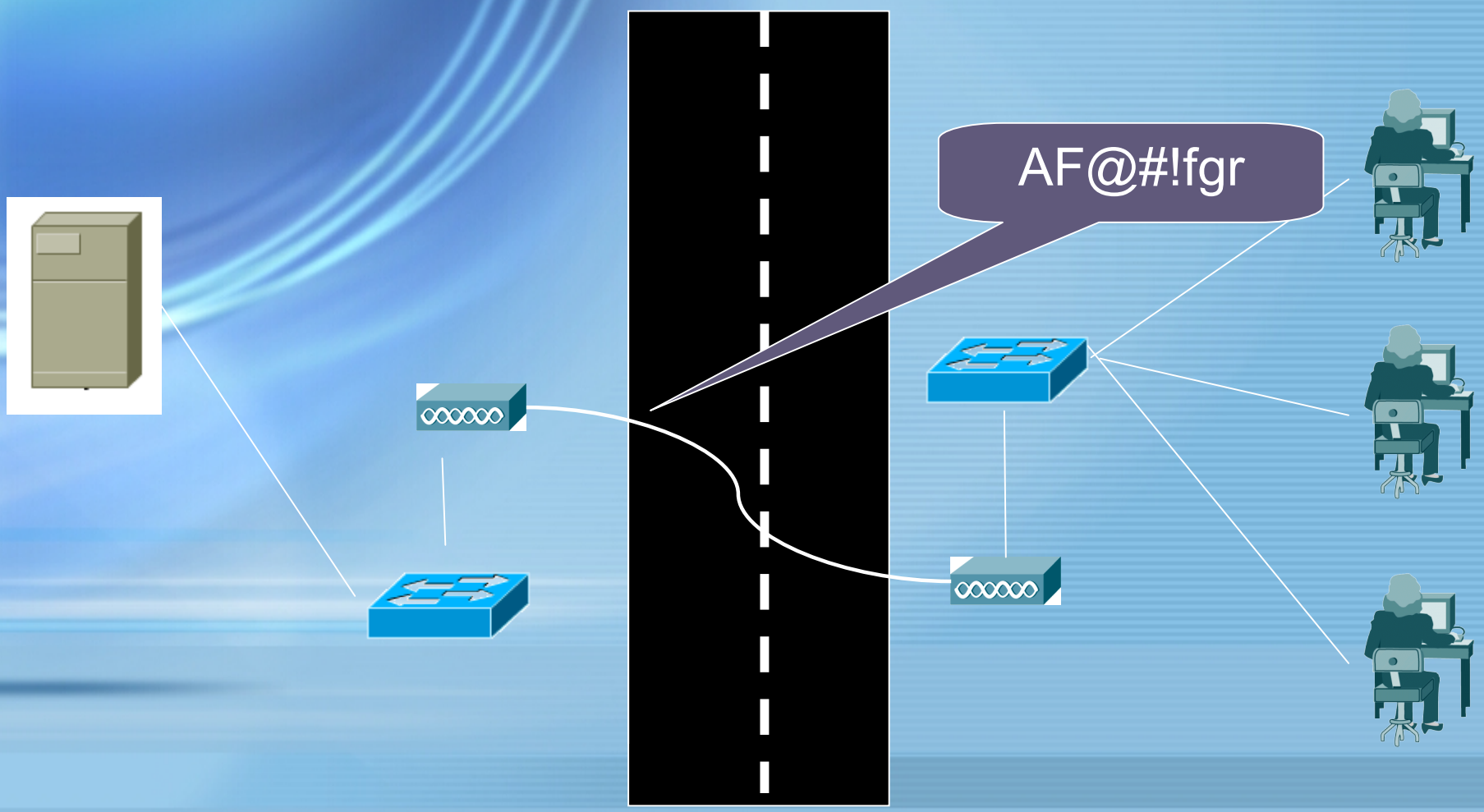


Câblage MAN

- Bâtiments d'un même campus
  Fibre optique monomode
- Bâtiments éloigné
  - Location de ligne
  - Micro-onde
  - Wifi
  - Wimax ?

Inversion des coût !

Traversé d'une rue



Câblage horizontal et vertical choix de média

- Vertical = desserte entre zone
  - Fibre optique = plus compliqué et couteux
  - Cuivre = distance max
- Horizontal = local de répartition vers bureaux
  - Cuivre (Cat 6 STP + RJ45)

Câblage WAN

- Câble fibre optique locaux
  - Protocole opérateur (Frame relay)
- Câble sous marin
  - Délais, prix
- Satellite
  - Délais de transmission

Câblage et sécurité

- Limiter les écoutes :
  - Fermer les portes
  - Crypter les liens publiques
  - Employer la fibre optique
  - Surveiller les branchements
- Eviter les pannes
  - Sérieux des branchements
  - Eliminer les câbles douteux

Appareil actif & topologie

- Les appareils actifs déterminent la topologie
- L'architecture est :
  - Leur disposition
  - Leur configuration
- Disposition contrainte

Locaux de brassage

3 Dangers :

- Vol
  - Porte qui ferme à clef
- Chaleur
  - Ventilation naturelle sufisante
- Ecoute
  - Fermeture des ports inutils

Chapitre III – Implémentation logique

Vlan

- Cloisonnement logique de réseau physique
- Plusieurs type de VLAN
  - Par port
  - Par adresse
  - Par utilisateur

Vlan 802.Q

- Implémentation simple
  - Modification de trame
  - Utilisation de la table CAN
- Trunk via un vlan particulier
- Pas de protocole de transport
- Pas d'authentification

Politique de vlan

- Cloisonnement essentiel
- Technique 80/20
  - Réseaux hiérarchique
  - Vlan niveau MAC par port
- Technique 20/80
  - Réseaux géographiques
  - Serveurs centralisés

Politique de VLAN sécurité

- Gestion par un serveur
- Cloisonnement par service
- Isolation des liens dangereux
- Définitions des chemins en Trunk
- Emploi de STP transparent
- Attention à l'electricité

NAT et PAT

- Network Adress Translation
  - Masquage de l'emmeteur
  - Permet le routage
  - Sécurise la source
- Port adresse Translation
  - Masquage de la cible
  - Sécurise la cible

VPN

- Prolonger un réseau local
- Encryptions d'un flux niveau IP
  - Dialogue client serveur
  - Après authentification
  - Tunnel sur TCP (L2P)
- Ne pas confondre avec PPOE

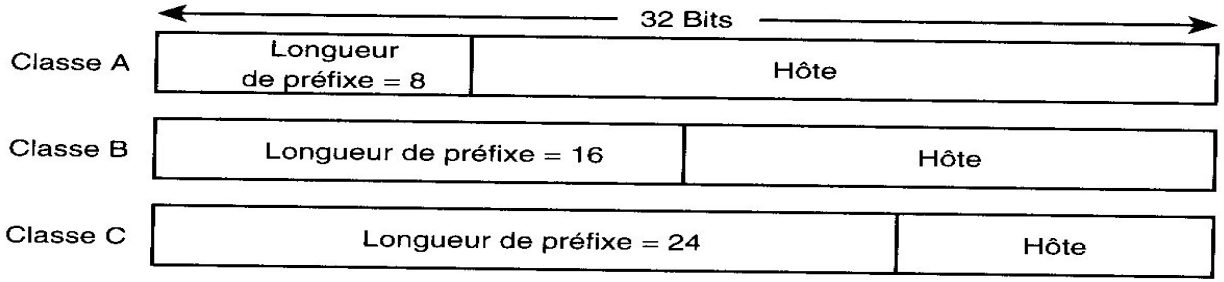
Plan d'adressage

- Il révèle la hiérarchie du réseaux
- Il comporte une partie publique
- Il comporte une partie privé
  10.0.0.0/255.0.0.0
  172.16.0.0 à 172.31.0.0/255.0.0.0
  192.168.0.0/255.255.0.0

Introduction plan IP

- Adressage hiérarchique : oui et non
- Routage par préfixe = simplification de routage mais complique la migration
- L'étanchéité niveau 3 est importante, mais impose un routage
- Comment choisir ses adresses

Classe et mask (rappel)



- Classe A : 255.0.0.0 commence par 00

Libre 10.x.y.z

- Classe B : 255.0.0.0 commence par 10

Libre 172.16.x.y

- Classe C : 255.255.0.0 commence par 11

Libre 192.168.x.y

Mask Variable Lenght

Les classes posent les pbs suivants :

- Les routeurs ne s'échangent pas les masques
- Les réseaux ne sont pas contigüs

193.55.95.0 ISIMA

193.54.51.1 CUST

=> table de routage pb avec risque de boucle

=> décision de routage hiérarchique impossible

Mask Variable Lenght

- Consiste à utiliser des réseaux contigüs
- Avec des masques variables suivant les sites
- Exemple :

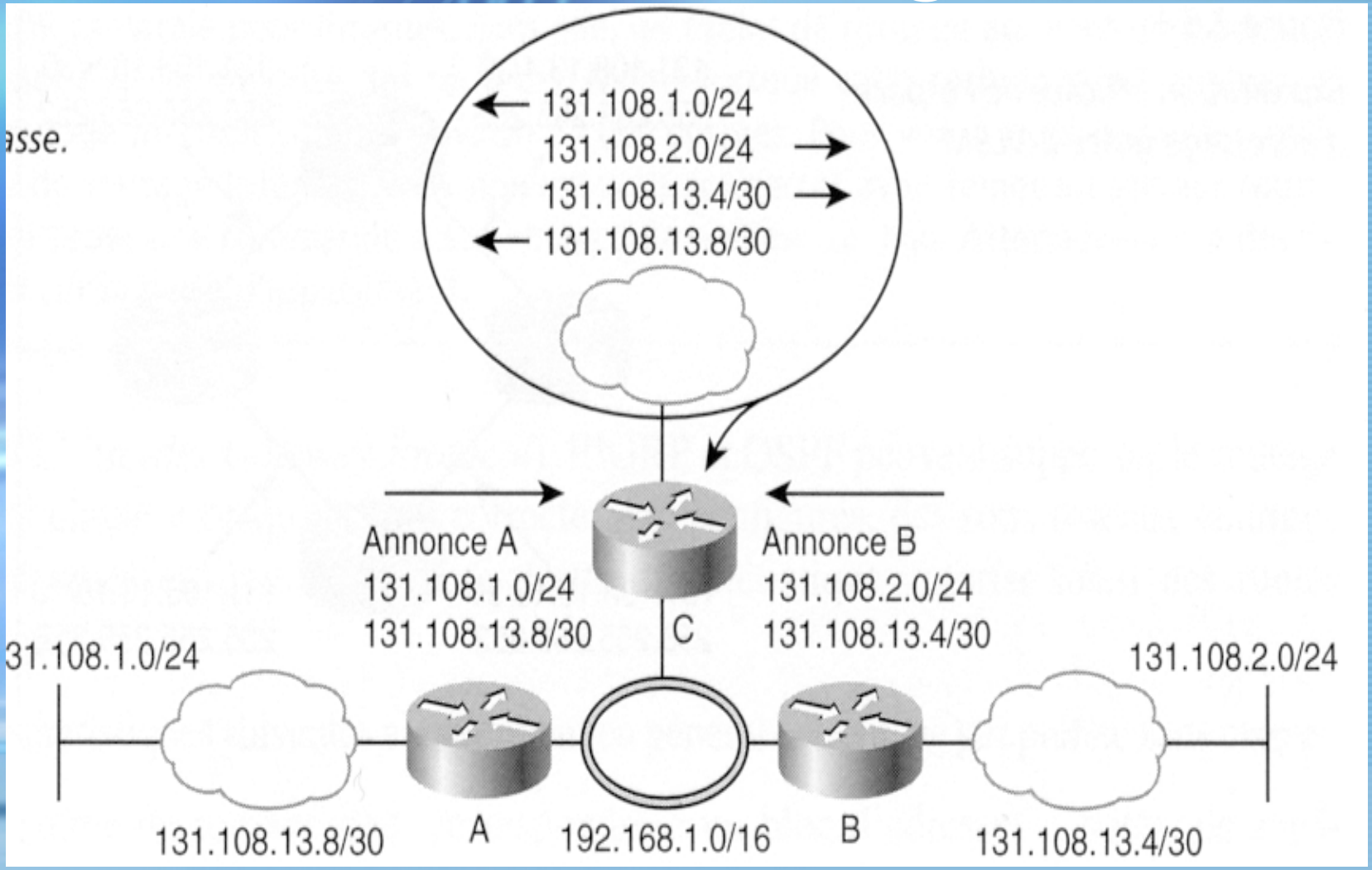
192.168.0.0 ISIMA 255.255.255.0

192.168.1.0 CUST 255.255.255.0

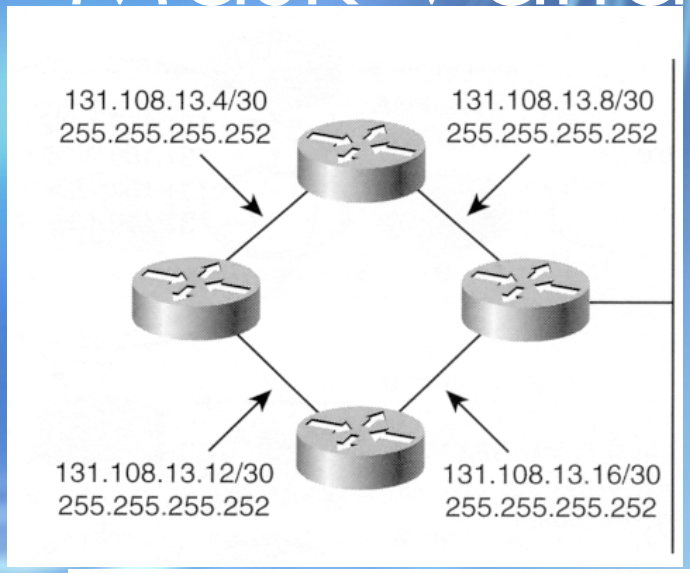
192.168.0.0 UBP 255.255.0.0

Le retour de la hiérarchie !

Mask Variable Lenght

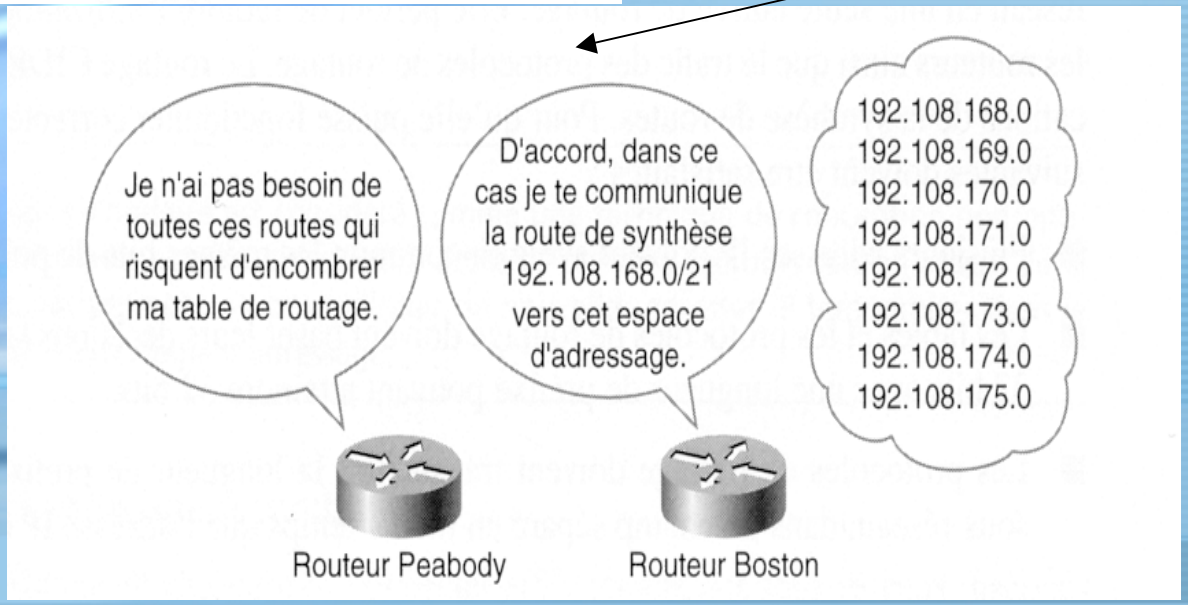


Mask Variable Lenght



Création économique
de boîte de redondance

Agrégation de route



Routage sans classe CIDR

Une entrée = hôte | | réseau | | groupe de réseaux

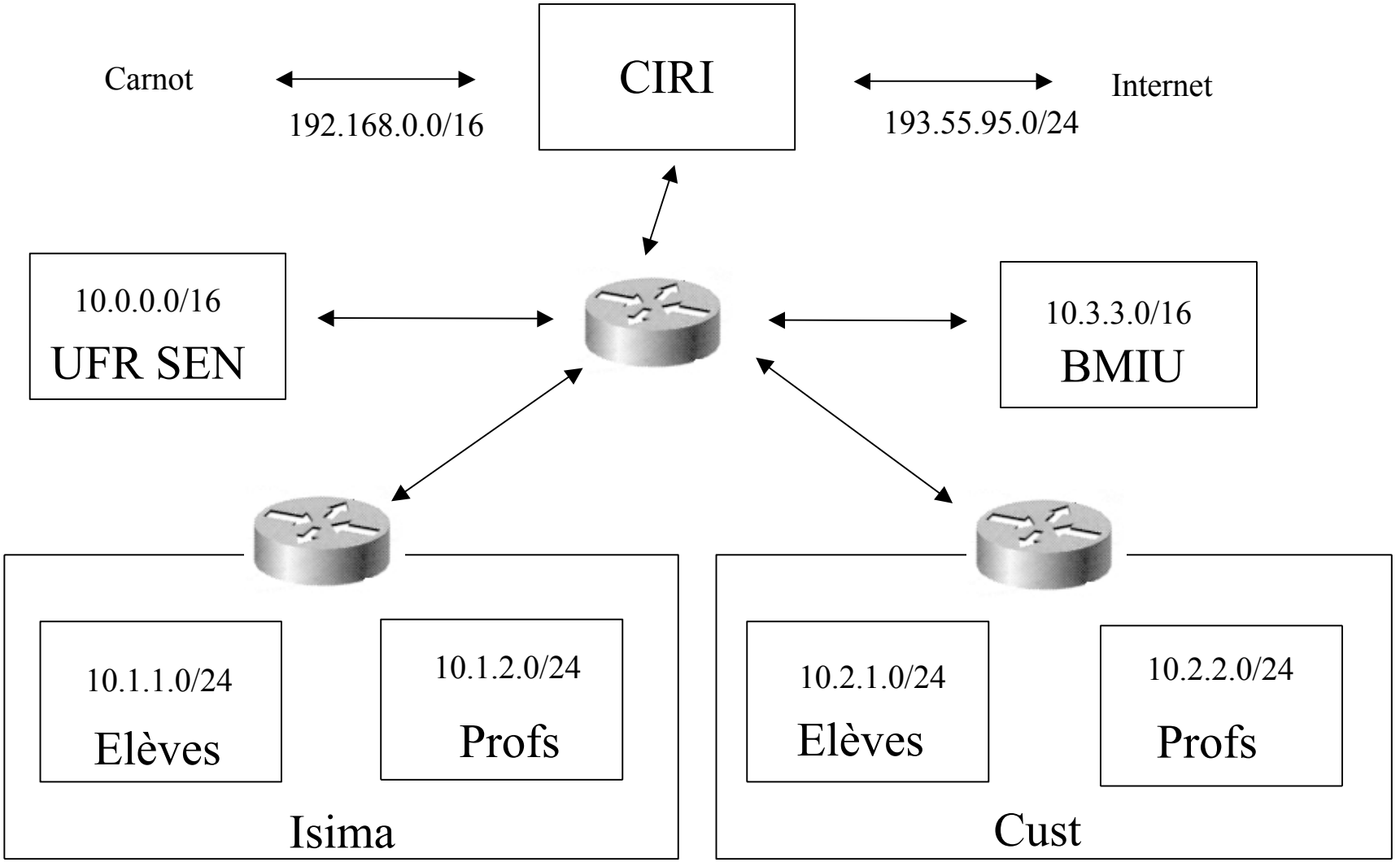
- Les tables de routage sont plus petites
- Pas de gâchis
- La traversée des routeurs est rapide
- L'overhead de routage est faible
- Le changement d'échelle se fait facilement
- La hiérarchie est facile à implémenter

Conception d'un plan IP

Les règles sont :

- Attribuer un numéro de réseau par service
- Les services d'un même lieu doivent être contigüs en IP
- Si routage niveau 2, mettre 255.255.0.0
- Utiliser un réseau non public pour le tiers fédérateur
- Utiliser un réseau pour le point à point
- VPN non public

Exemple IP


Carnot
192.168.0.0/16
CIRI
193.55.95.0/24
Internet
10.0.0.0/16
UFR SEN
10.3.3.0/16
BMIU
10.1.1.0/24
Elèves
10.1.2.0/24
Profs
Isima
10.2.1.0/24
Elèves
10.2.2.0/24
Profs
Cust

Sécurité IP et Firewall

- Tout ce qui n'est pas utile est interdit
- Le filtrage se fait au niveau le plus haut
- L'intérieur et l'extérieur sont insécures
- Les communications doivent être explicite
- Quand on filtre on le dit !
- L'utilisateur ne doit rien sentir

Politique de sécurité !

Serveur et services

- Serveur d'infrastructure
  dhcp, dns, active directory,…
- Serveur de service système
  Fichier (cif,nfs, …), NAS, SAN, bd
- Serveur de communication
  Mail, téléphonie, messagerie instantanée
- Serveur d'application
  RDP,X11,WEB

Sécurisation physique des serveurs

- Vol
- incendie, inondation
- Sécurisation des données
- Système SAN
- Système de sauvegarde
  - Robot/support
  - Procédure de sauvegarde

Sécurisation des serveurs niveau système

- Limiter l'accès au port suivant les sources (firewal local, ex netfilter) pour les machines exposés
- Avoir des mots de passe robuste
- Crypter les ouvertures de session
- Flux d'information connus et explicite

Sécurisation des services

- Mail
  - SMTP avec grey liste
  - SSL sur pop ou IMAP
- WEB
  - https
  - Intranet a mots de passe/IP
- FTP = sftp
- Interactif = ssh /freenx

Authentification

- Problème multiple
- A différent niveau
  - Système
  - Applications
  - Réseau
    - PPOE
    - VPN

Authentification et identification

- Identification = identité !
  - Login
  - Nom Prénom
  - téléphone
- Authentification = mots de passe !
  - Association au login
- Problème ouvert

Solutions auth machine

- Kerberos
- Local type Pam Unix
- A la main

Mais :

- Pas de stockage en clair
- Pas de circulation en clair

Solutions auth réseaux (802.X)

- Reconnue par les clients
- Matérialisé par un commutateur particulier (broadcom)
- Verse utilisateurs dans :
  - VLAN (par adresse, physique, geo…)
  - Réseau WIFI
  - VPN
  - Gestion de bande passante
  - DHCP
  - Routage simple

Cas général

- Simple Un seul bâtiment
  - Câblage en étoile
  - 1 firewall
  - 1 routeur des Switchs
- Plusieurs bâtiments
  - 1 router
  - N router

Cas particuliers – Accès nomades

- Connexion arrivant de partout
- Utilisation des application d'entreprise
- Utiliser les VPN
- Accès sur demande
- Filtrage d'opérateur
- Droits restreint ou pas

Cas particuliers – Accès sans fils

Deux possibilité de conception :

- A base d'acces points
  - Similaire au réseaux LAN ethernet
  - Le wifi vient en plus
  - Gestion du roaming
- A base de pont
  - Réseau pure wifi
  - Problème d'accès
  - Vlan gérer par les access points

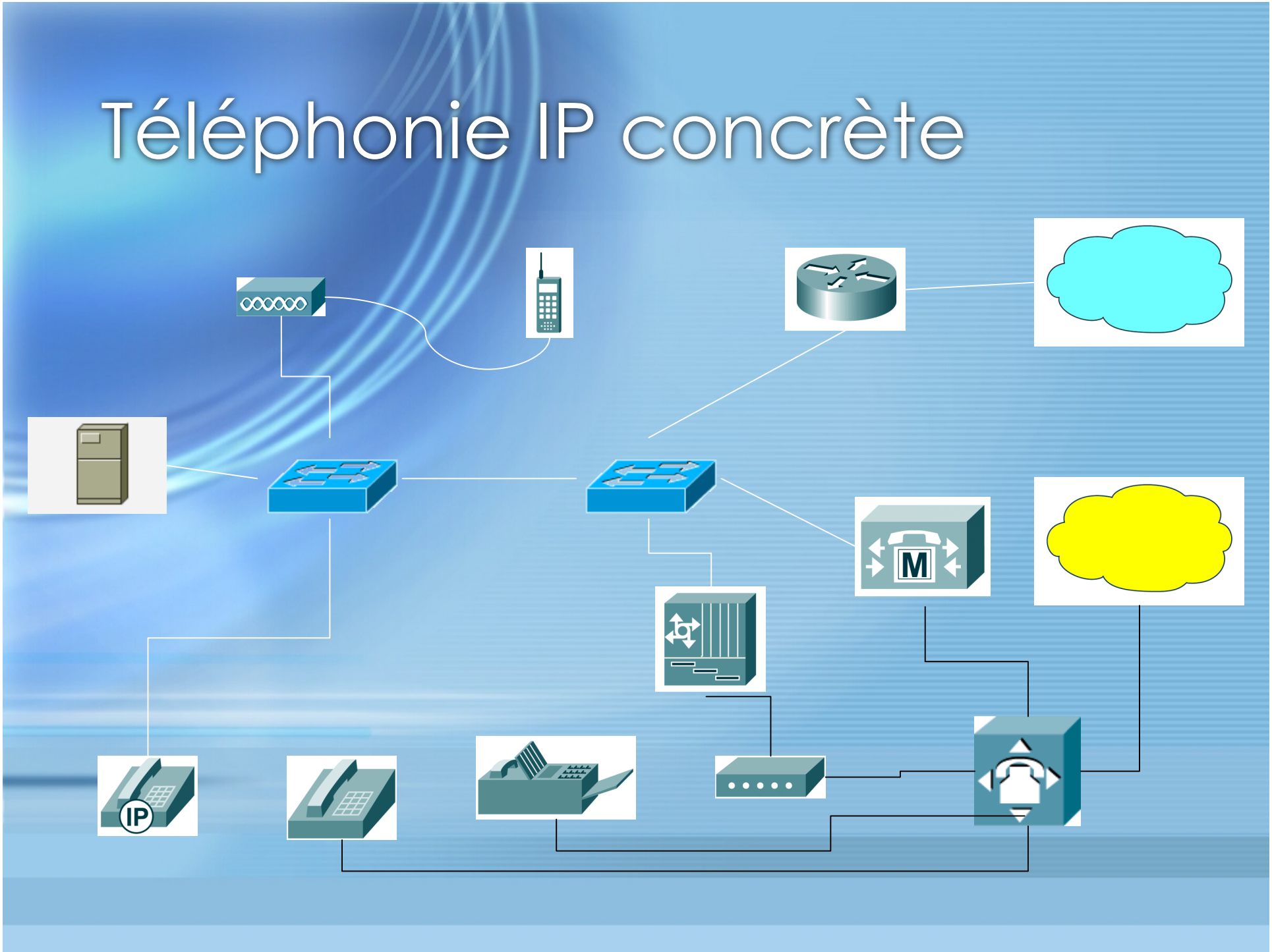
Sécurisation du sans fils :

- Eviter les abus
  Authentification 802.X
- Confidentialité => Cryptage
  - WEAP – WEP + rotation de clef auto
  - VPN – en plus
  (permet de gérer les accès des hôtels)
- Santé – attention à la proximité

Cas particuliers – Téléphonie IP

- Coûte directement du flouz
  - Quand il marche pas
  - Quand il marche mal
  - Quand quelqu'un s'en sert
- Mesure à prendre :
  - Utilisé SIP
  - Utlisé un VLAN particulier
  - Implémenté de la QOS

Téléphonie IP concrète



Métrologie

Un réseau sure est un réseaux bien surveillé :

- SNMP simple network management
- Nagios
- Se servir de nos quatre sens :

  Température, bruit, odeur, vibrations, aspect

  – se découvrir les oreilles
  – enlever les lunettes de soleil

Conclusions

- Réfléchir avant
- Agir avec rigueur
- Faire au plus simples
- Surveillé quotidiennement
- Ecouté les utilisateurs
- Etablir des procédures
- Avoir une sauvegarde

Etude d'un cas

Une université :

- Des étudiants
  - Portable WIFI
  - Accès libre
  - TP
- Des profs
  - Préparation test
  - Portable
- Des administratifs
  - Gestion administrative
  - Gestion pédagogique

Des besoins :

- Accès web
- Messagerie
- Stockage de données
- Utilisation d'application dédier
- Téléphonie Skype