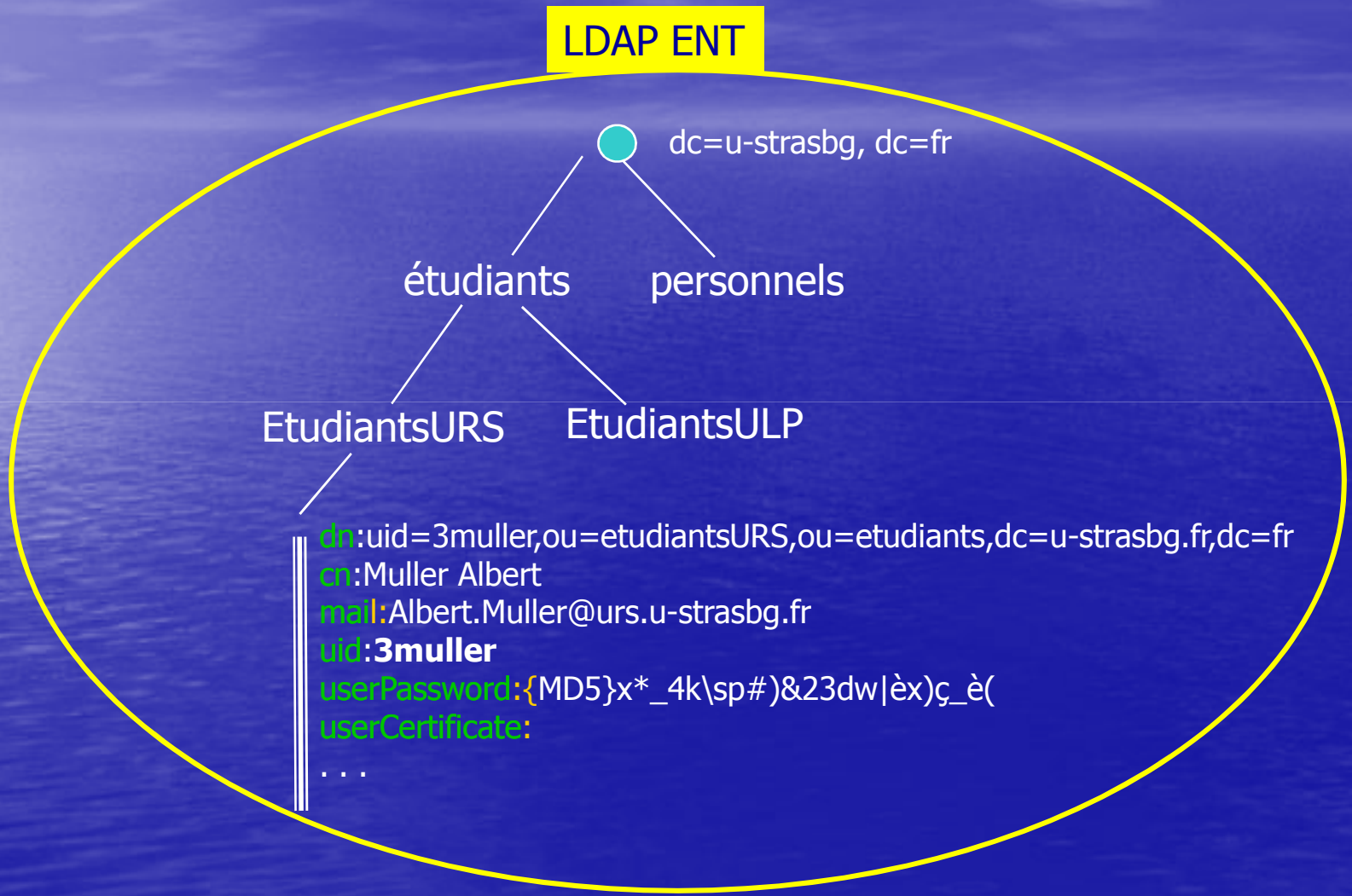
Services réseaux avancés

- Authentification
  - Annuaires
  - Single Sign On
- Réseaux sans-fil
  - Osiris, non sécurisé avec portail captif
  - Osiris-sec
- Vlan
  - 802.1Q
- IPv6

Inscription d'un étudiant



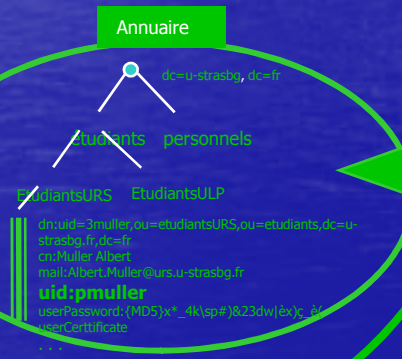
Authentification au Département

IUT

Connexion dans le domaine

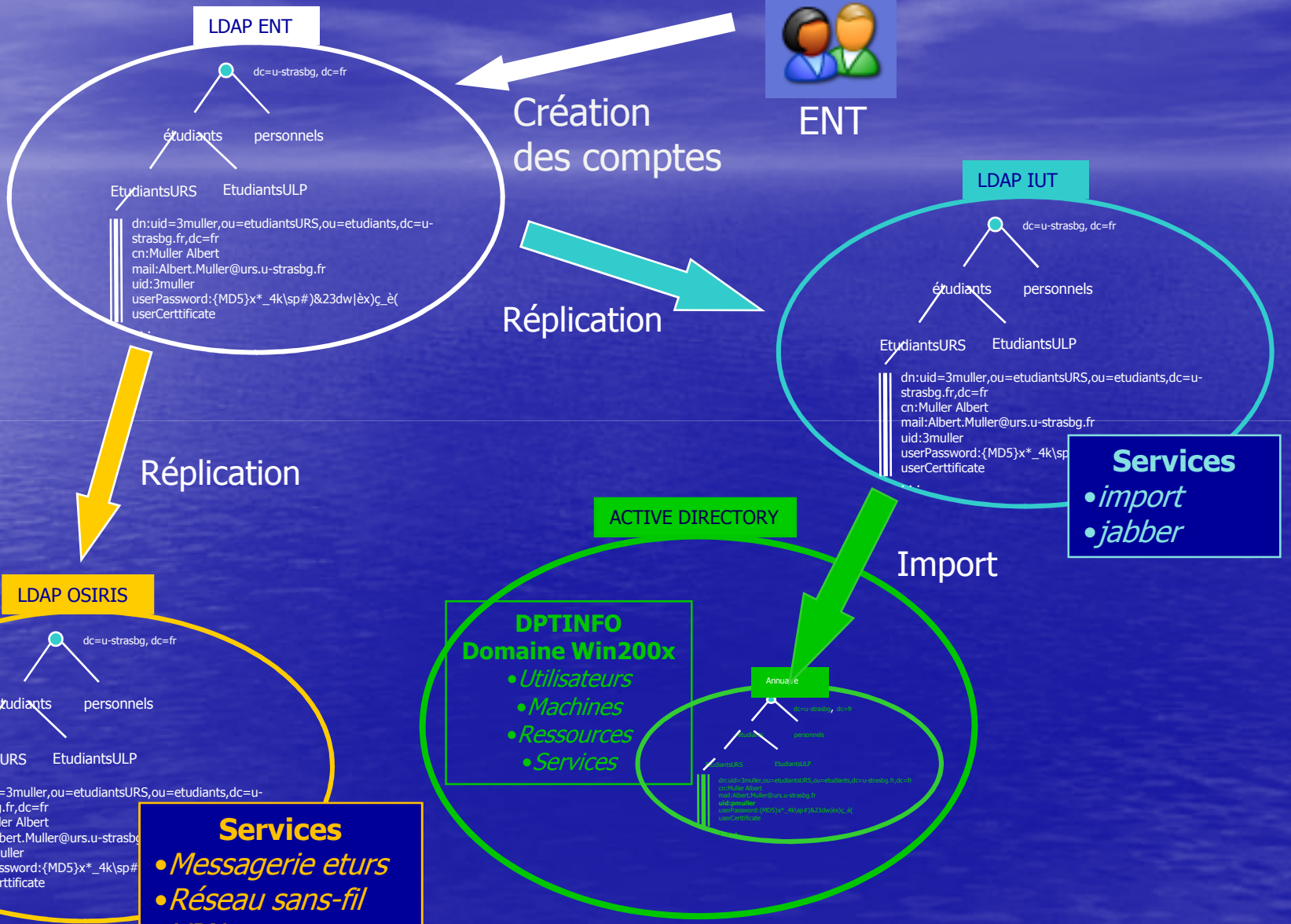
Active Directory

DPTINFO
Domaine Win200x
- *Utilisateurs*
- *Machines*
- *Ressources*
- *Services*

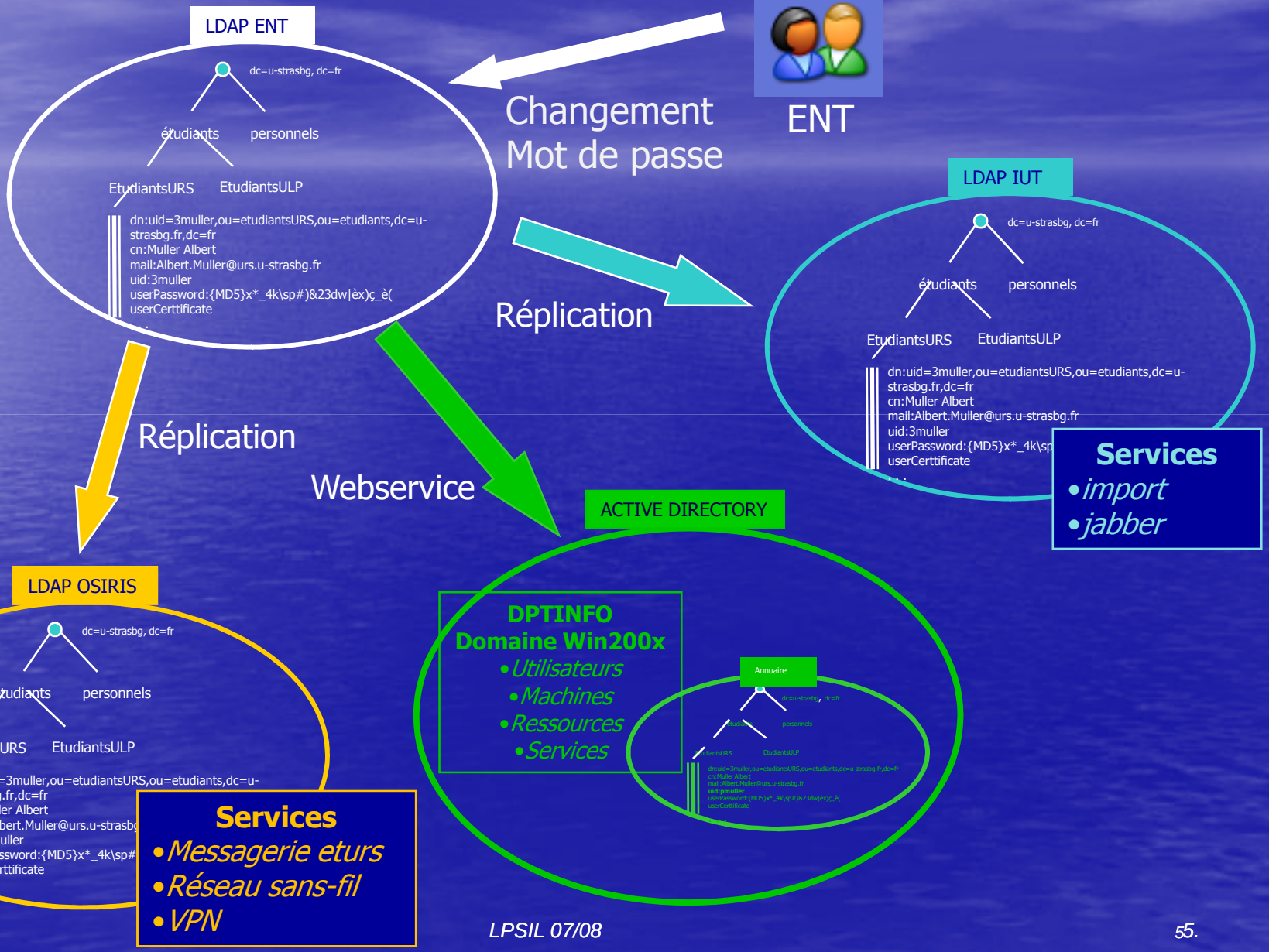


Authentification Kerberos SSO

Synchonisation des annuaires



Synchonisation des annuaires



Changement local du mot de passe

LDAP ENT

dc=u-strasbg, dc=fr

étudiants personnels

EtudiantsURS EtudiantsULP

dn:uid=3muller,ou=etudiantsURS,ou=etudiants,dc=u-strasbg.fr,dc=fr
cn:Muller Albert
mail:Albert.Muller@urs.u-strasbg.fr
uid:3muller
userPassword:{MD5}x*_4k\sp#)&23dw|èx)ç_è(
userCerttificate

LDAP IUT

dc=u-strasbg, dc=fr

étudiants personnels

EtudiantsURS EtudiantsULP

dn:uid=3muller,ou=etudiantsURS,ou=etudiants,dc=u-strasbg.fr,dc=fr
cn:Muller Albert
mail:Albert.Muller@urs.u-strasbg.fr
uid:3muller
userPassword:{MD5}x*_4k\sp
userCerttificate

Services
- *import*
- *jabber*

LDAP OSIRIS

dc=u-strasbg, dc=fr

étudiants personnels

EtudiantsURS EtudiantsULP

dn:uid=3muller,ou=etudiantsURS,ou=etudiants,dc=u-strasbg.fr,dc=fr
cn:Muller Albert
mail:Albert.Muller@urs.u-strasbg
uid:3muller
userPassword:{MD5}x*_4k\sp#
userCerttificate

Services
- *Messagerie eturs*
- *Réseau sans-fil*
- *VPN*

A éviter

ACTIVE DIRECTORY

DPTINFO
Domaine Win200x
- *Utilisateurs*
- *Machines*
- *Ressources*
- *Services*

Annuaire

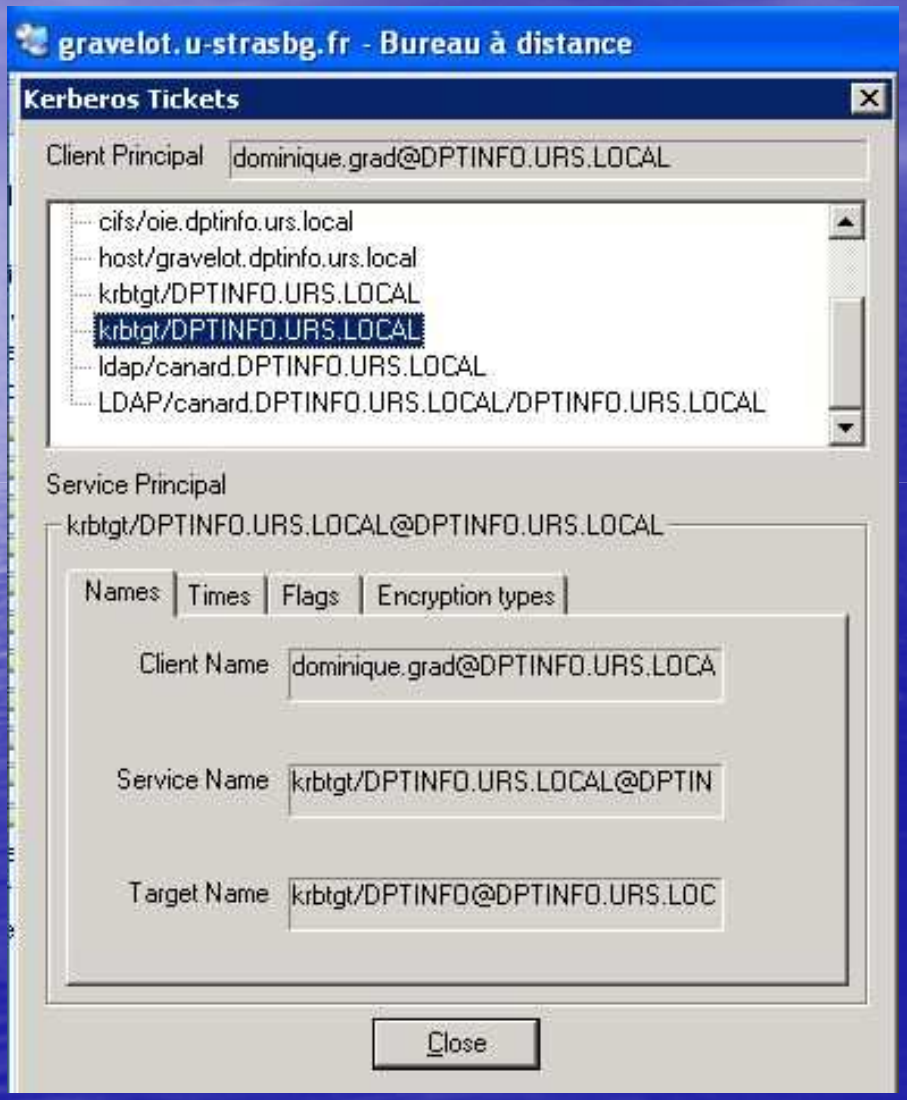
fou> **kpasswd**

Authentification et Annuaires

- LDAP : Lightweight Directory Access Protocol : protocole d'accès aux annuaires X500 (RFC 3377)
- Active Directory : annuaire des ressources partagées (Win2K Server), inclus un annuaire de type LDAP
- Kerberos : protocole d'authentification, à base de tickets
- SSO : Single Sign On, mécanismes permettant de ne s'authentifier qu'une seule fois

Authentification et Annuaires

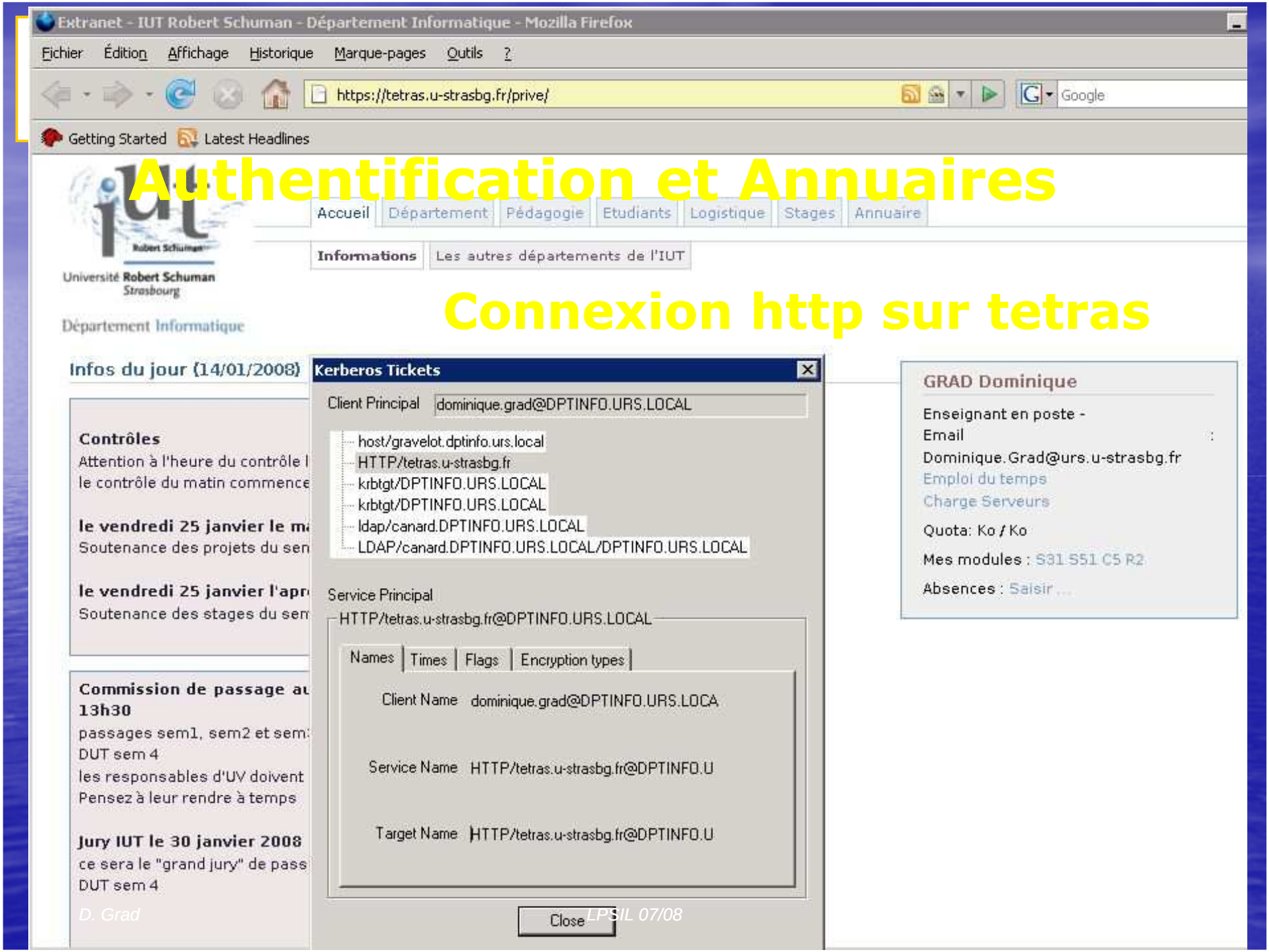
Connexion rdp sur gravelot



- Ticket TGT
- Tickets TGS
  - host : gravelot
  - ldap

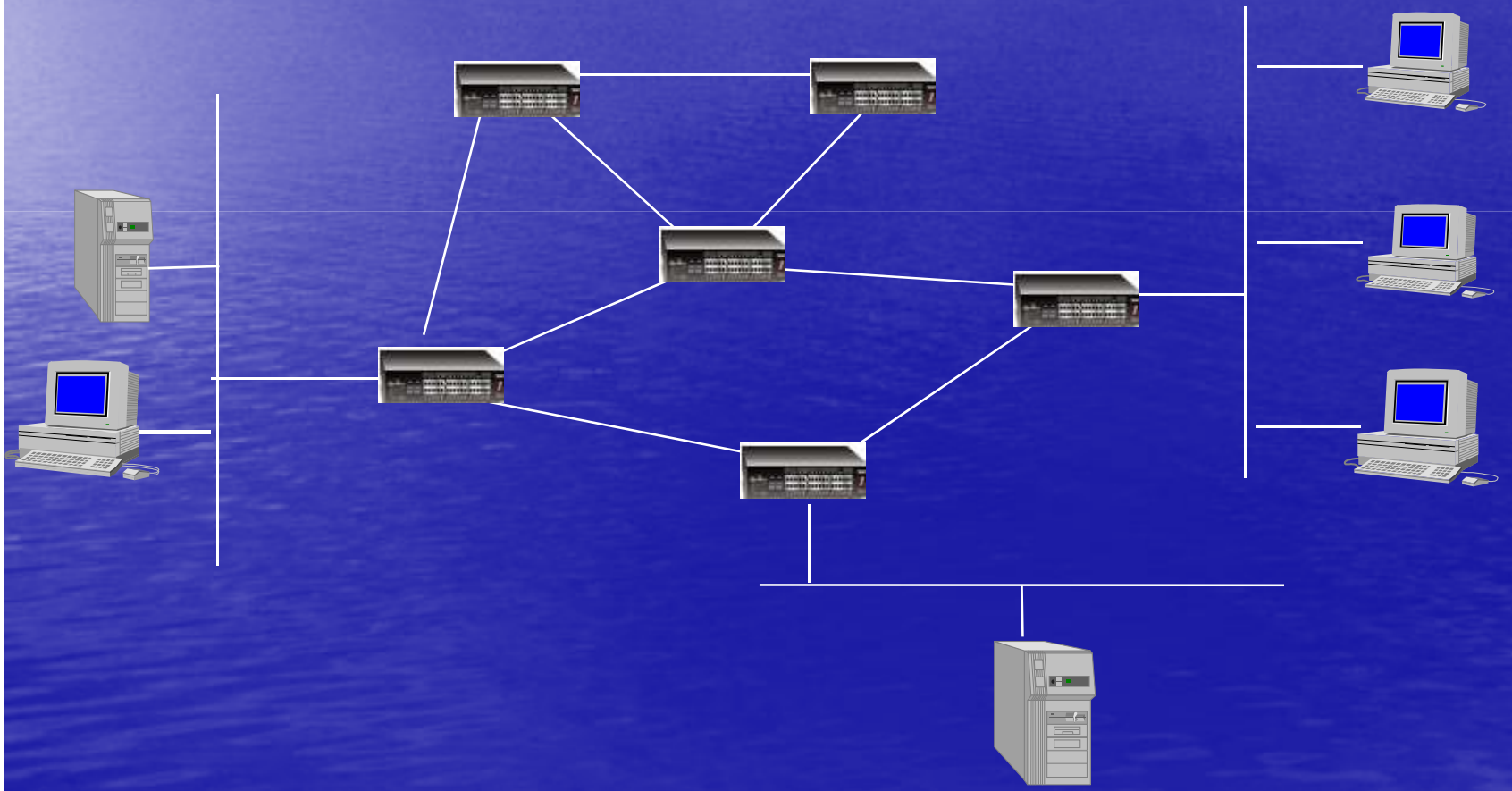
Authentification et Annuaires

Connexion http sur tetras



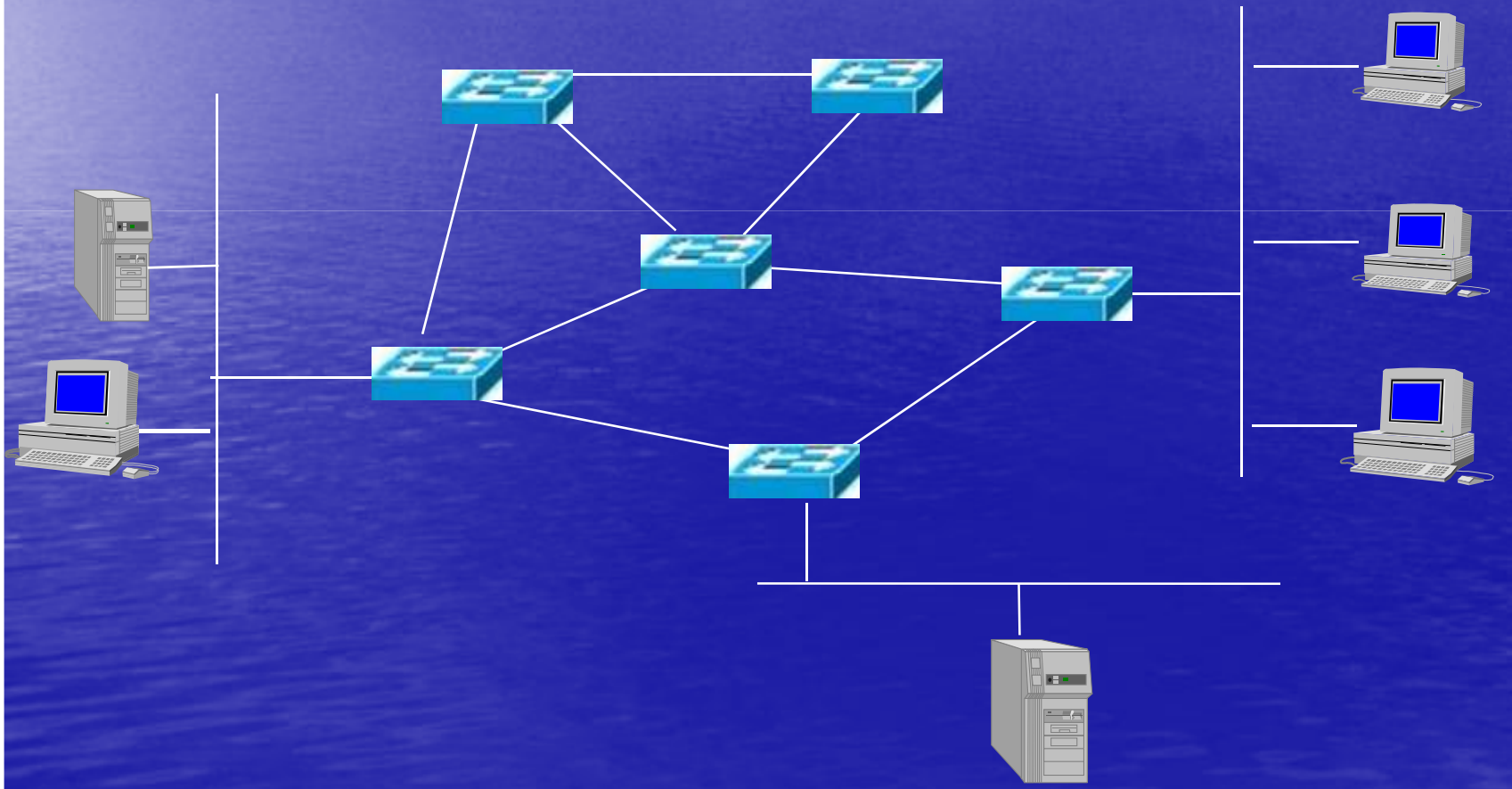
Architecture de Réseaux

- A base de répéteurs



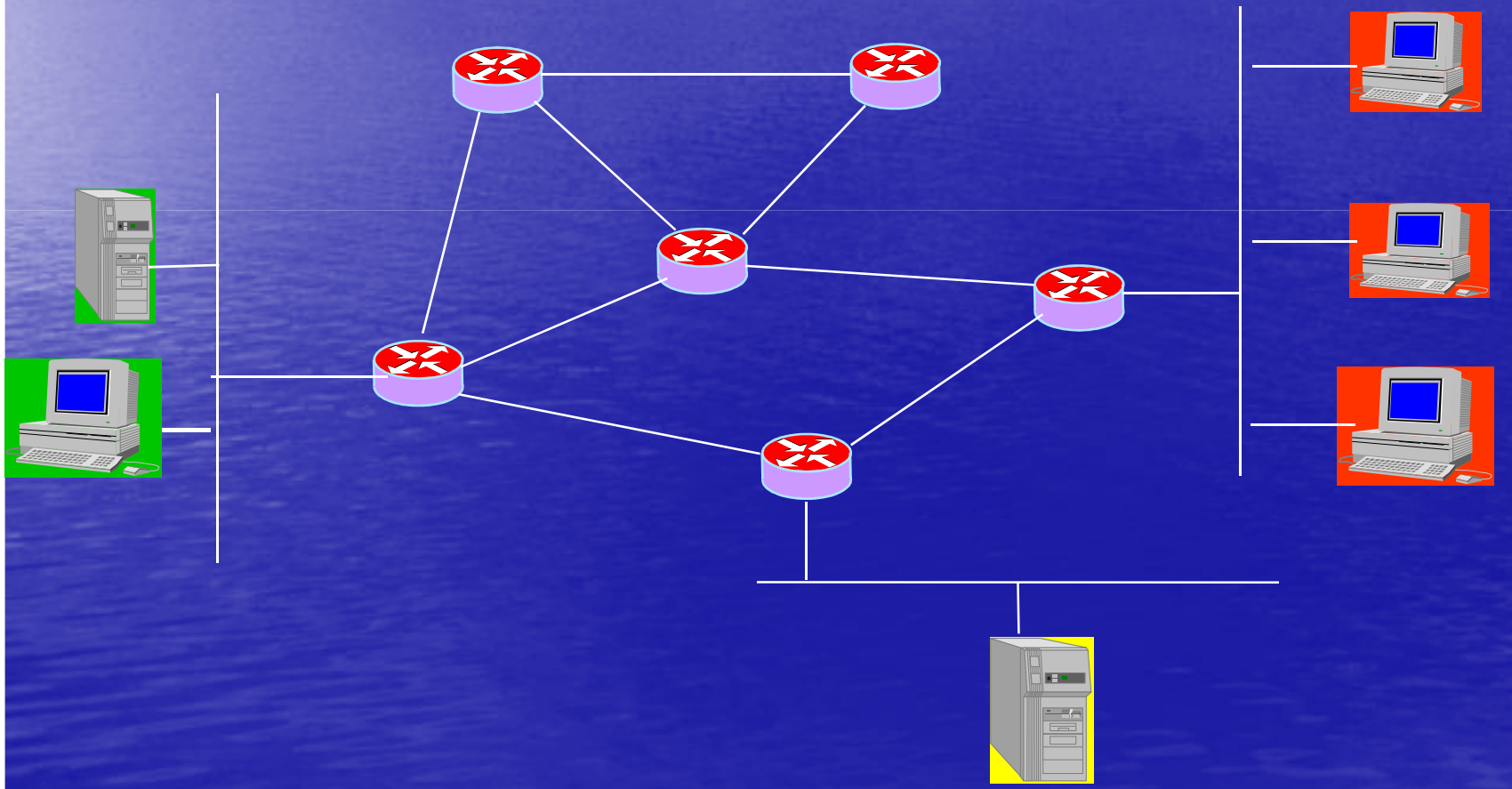
Architecture de Réseaux

- A base de commutateurs



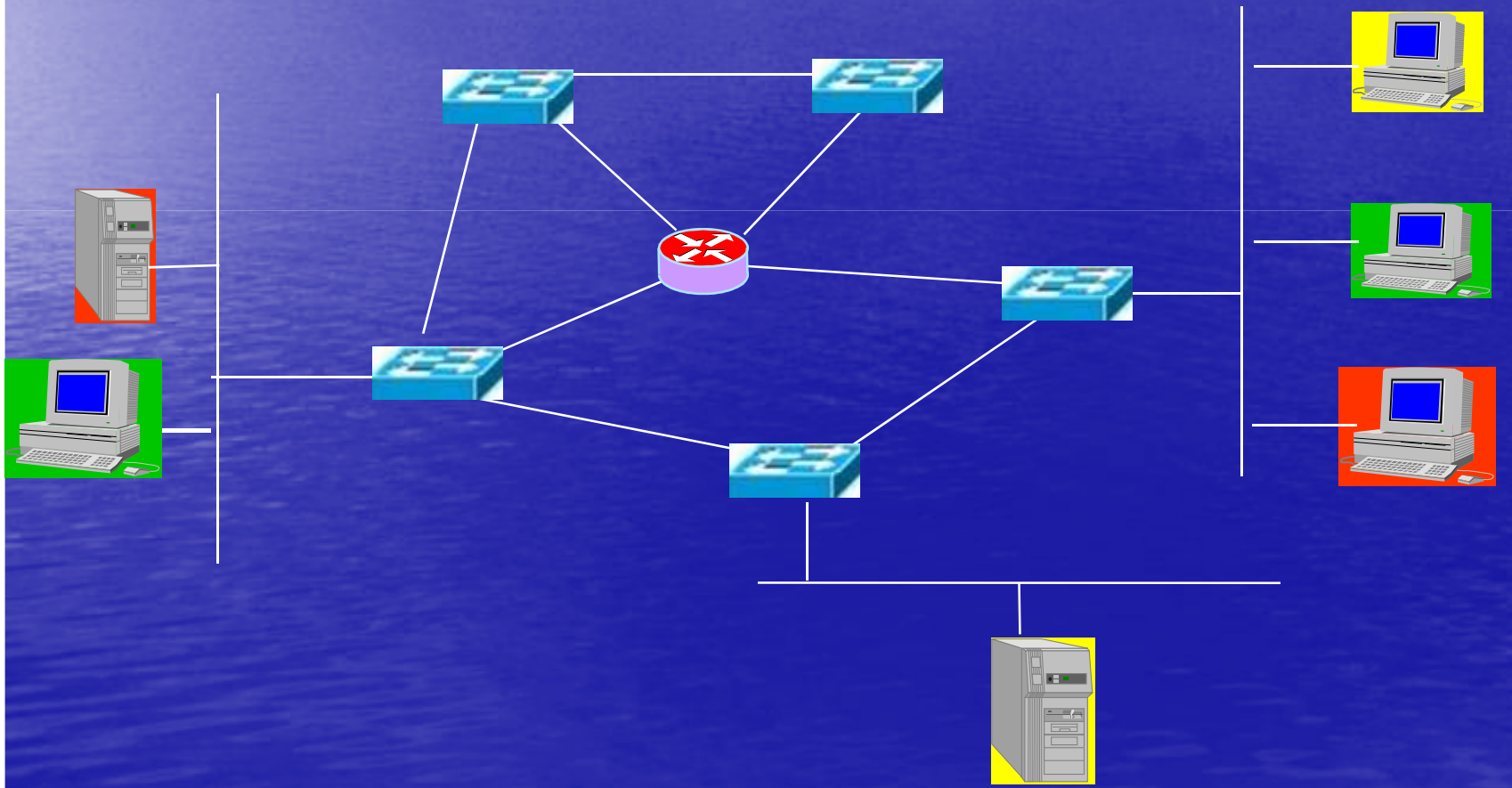
Architecture de Réseaux

- A base de routeurs



Architecture de Réseaux

- A base de vlan



Architecture de Vlan

- Réseaux logiques et flexibilité
- Limitation des domaines de broadcast
- Apporter une sécurité accrue
- Permettre la mobilité

- Niv 1 : Par ports (statique, répandu)
- Niv 2 : Par adresse MAC (dynamique)
- Niv 3 : Par sous-réseau, par type de protocole

Architecture de Vlan

- Nécessite la mise en œuvre
  - Transparent bridging (auto-apprentissage, table de commutation) 802.1D
  - Spanning Tree pour éviter les boucles
  - Marquage 802.1Q (tag, trunk)
  - Authentification et Autorisation 802.1x
- Commutation de Niveau 3

Département Informatique

S51

Réseaux sans-fil et Sécurité

D. Grad

Sécurité des réseaux sans-fil 802.11 a, b , g

- SSID : Service set Identifier (diffusion)
- Authentification ouverte / partagée
- Filtrage d'adresses MAC
- WEP : Wired Equivalent Privacy
  - Chiffrement pour 802.11
  - Algorithme RC4
  - Clés de 40 bits (opt. 128 bits)

Sécurité des réseaux sans-fil 802.11 a, b , g

→ Wep : Sécurité faible

- Implémentation faible de l'algotithme RC4
- Découverte de la clé de chiffrement
- Écoute et modification des données
- Attaque de machines internes
- Analogie : prise réseau dans la rue…

Principes de base & sécurité : Sécurité avancée

La nouvelle norme de sécurité IEEE 802.11i :

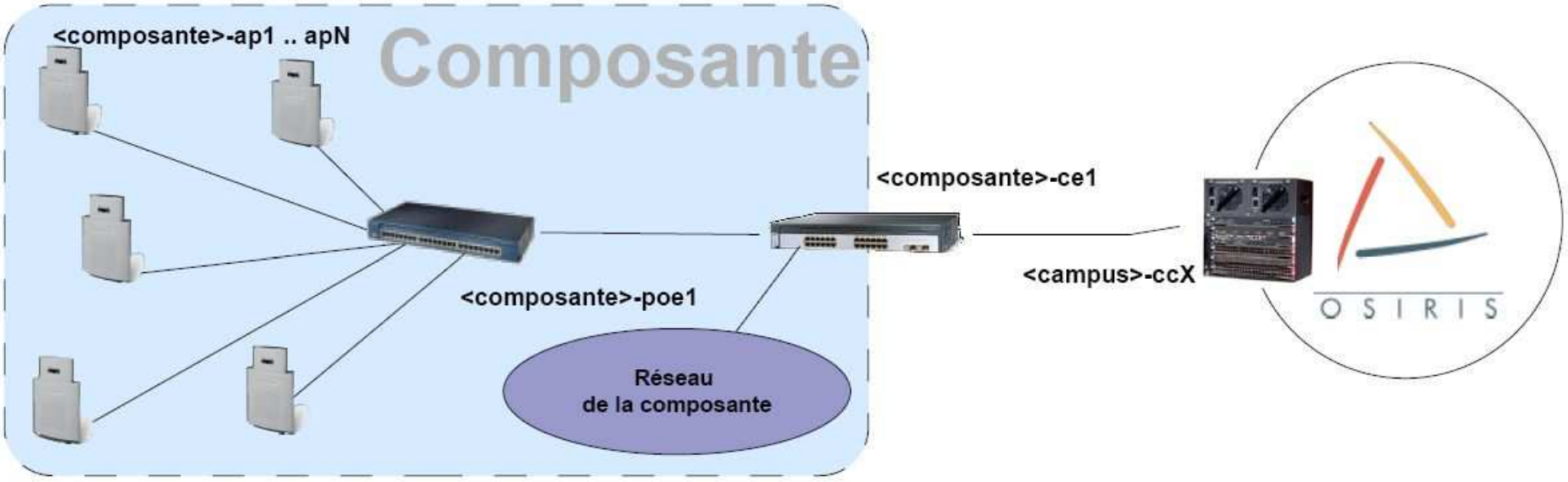
- VOLET 1: Solution de transition compatible avec le matériel existant (WPA):
  - 802.1x + EAP
  - Gestion des clés améliorée **(TKIP)**
  - algorithme de cryptage RC4
- VOLET 2: Solution définitive incompatible avec le matériel existant (WPA2):
  - 802.1x + EAP
  - Protection des données AES
  - Pré-authentification

Principes de base & sécurité : Systèmes d'authentification

La norme IEEE 802.1x propose un ensemble de protocoles d'authentification EAP

- **Authentifications par noms d'utilisateurs / mots de passe:**
  - **LEAP: méthode propriétaire Cisco**
  - **EAP-MD5 : le client s'authentifie par mot de passe (CHAP)**
- **Authentifications basées sur des certificats:**
  - **EAP-TLS (Transport Layer Security): Certificats côté client (machine et/ou utilisateur) & côté serveur**
  - **PEAP (Protected EAP): authentification par login / mot de passe + Certificat côté serveur (authentification sécurisée par tunnel TLS)**
- **Authentifications par cartes à puces sécurisées, Biométrie**
- **Ces solutions requièrent un serveur d'autorisations RADIUS pour les utilisateurs.**

Le réseau sans-fil OSIRIS

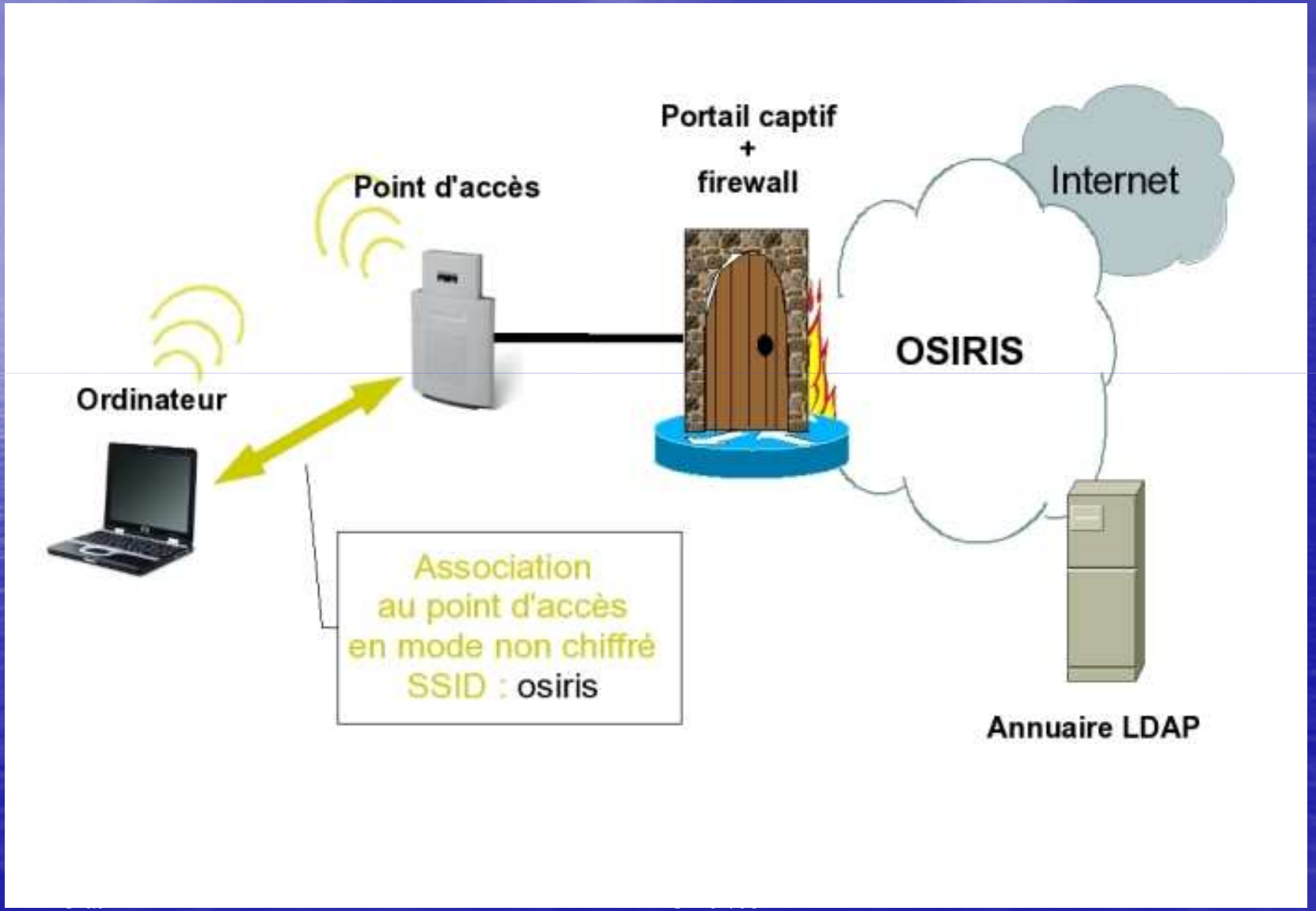


Equipements « sans-fil » dans Osiris

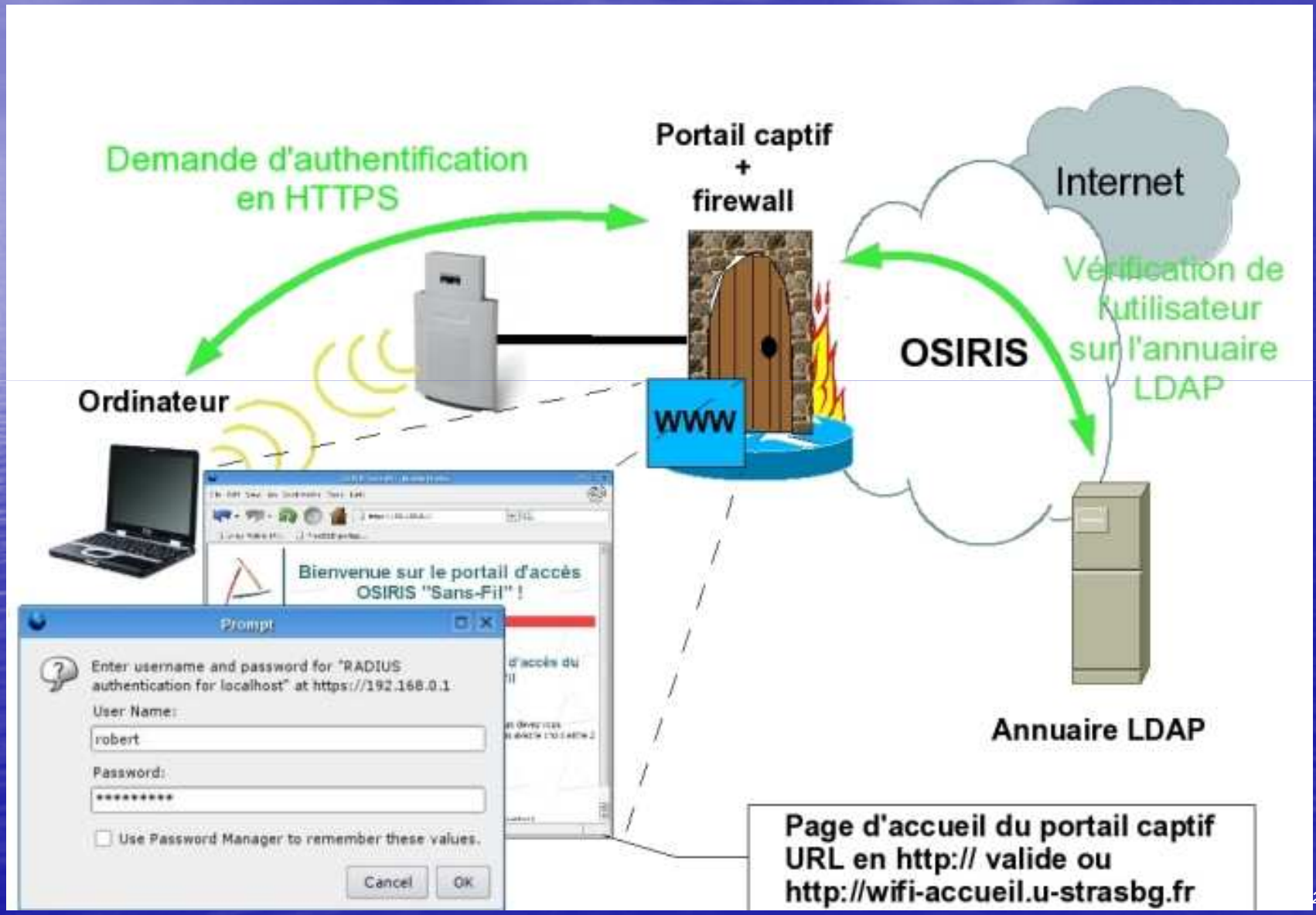
Le réseau sans-fil OSIRIS

- OSIRIS : Non sécurisé, portail captif
  - Configuration adressage privé
  - Toutes les requêtes sont redirigées vers un portail
  - Authentification ENT
  - Ajout dynamique de règles de pare-feu/Nat pour les protocoles autorisés uniquement (https, imaps pops,..)
- http://www-crc.u-strasbg.fr/osiris/services/wifi/
- http://www-crc.u-strasbg.fr/osiris/services/wifi/public/osiris_open.html

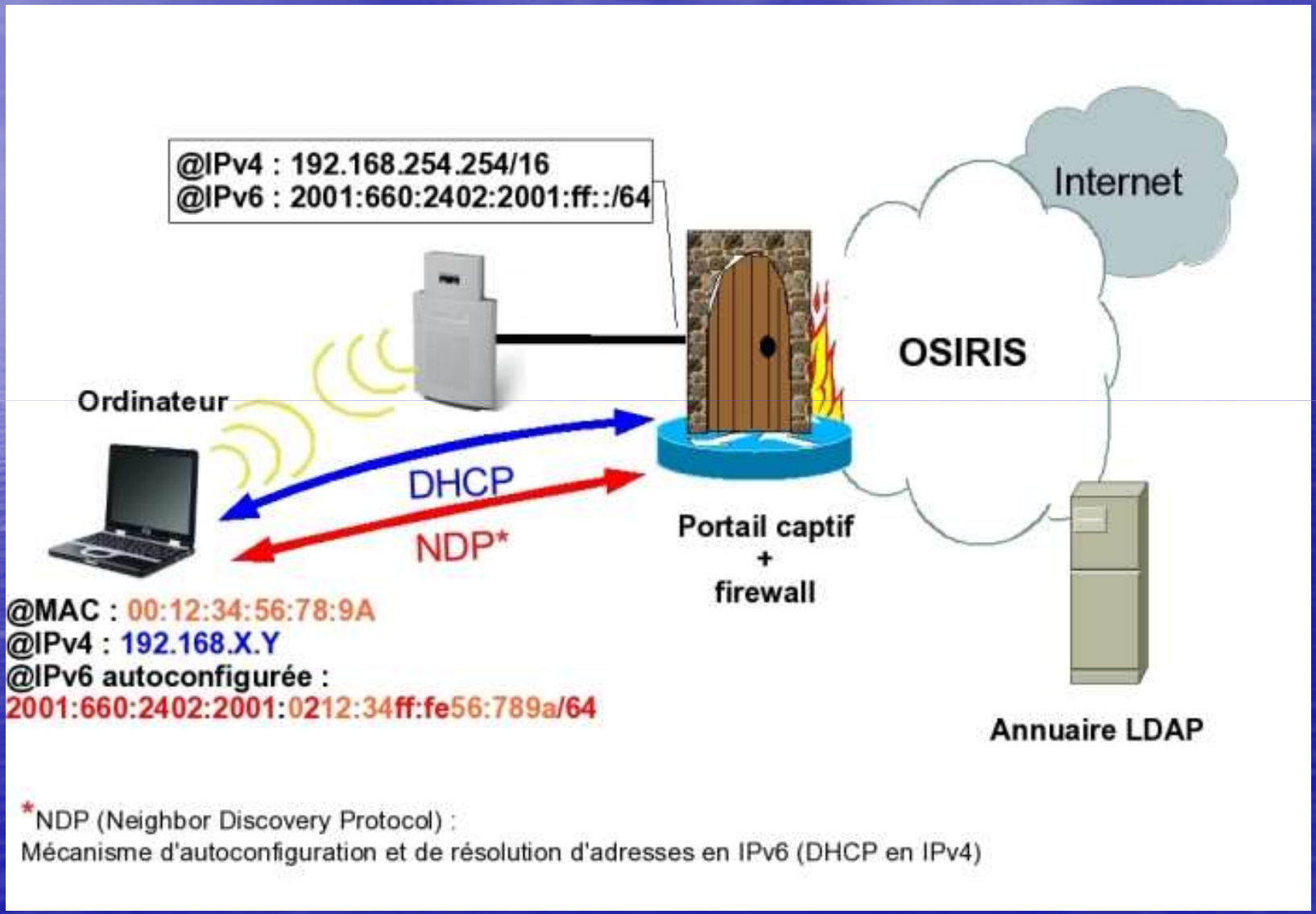
Le réseau sans-fil OSIRIS



Le réseau sans-fil OSIRIS

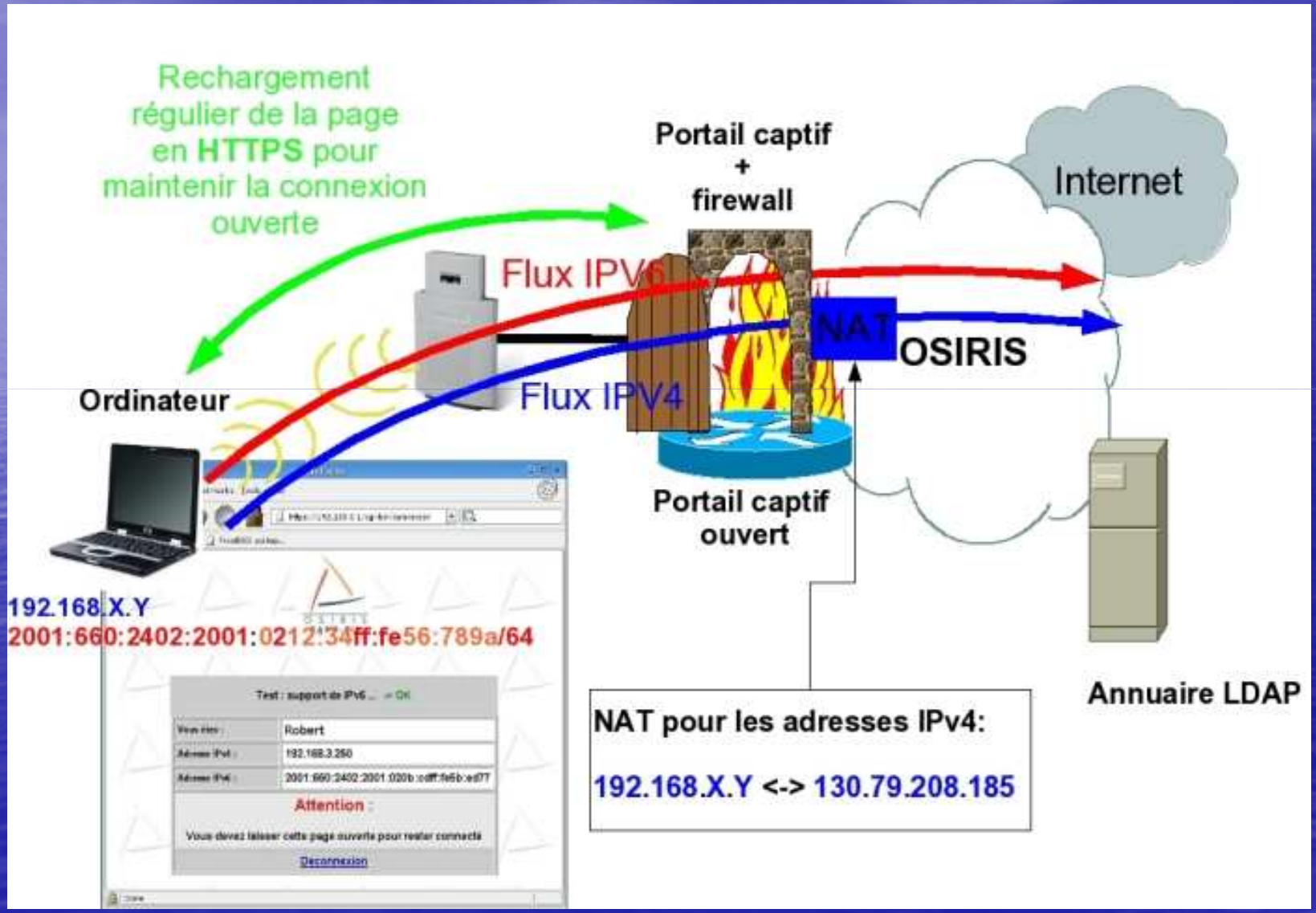


Le réseau sans-fil OSIRIS



*NDP (Neighbor Discovery Protocol) :
Mécanisme d'autoconfiguration et de résolution d'adresses en IPv6 (DHCP en IPv4)

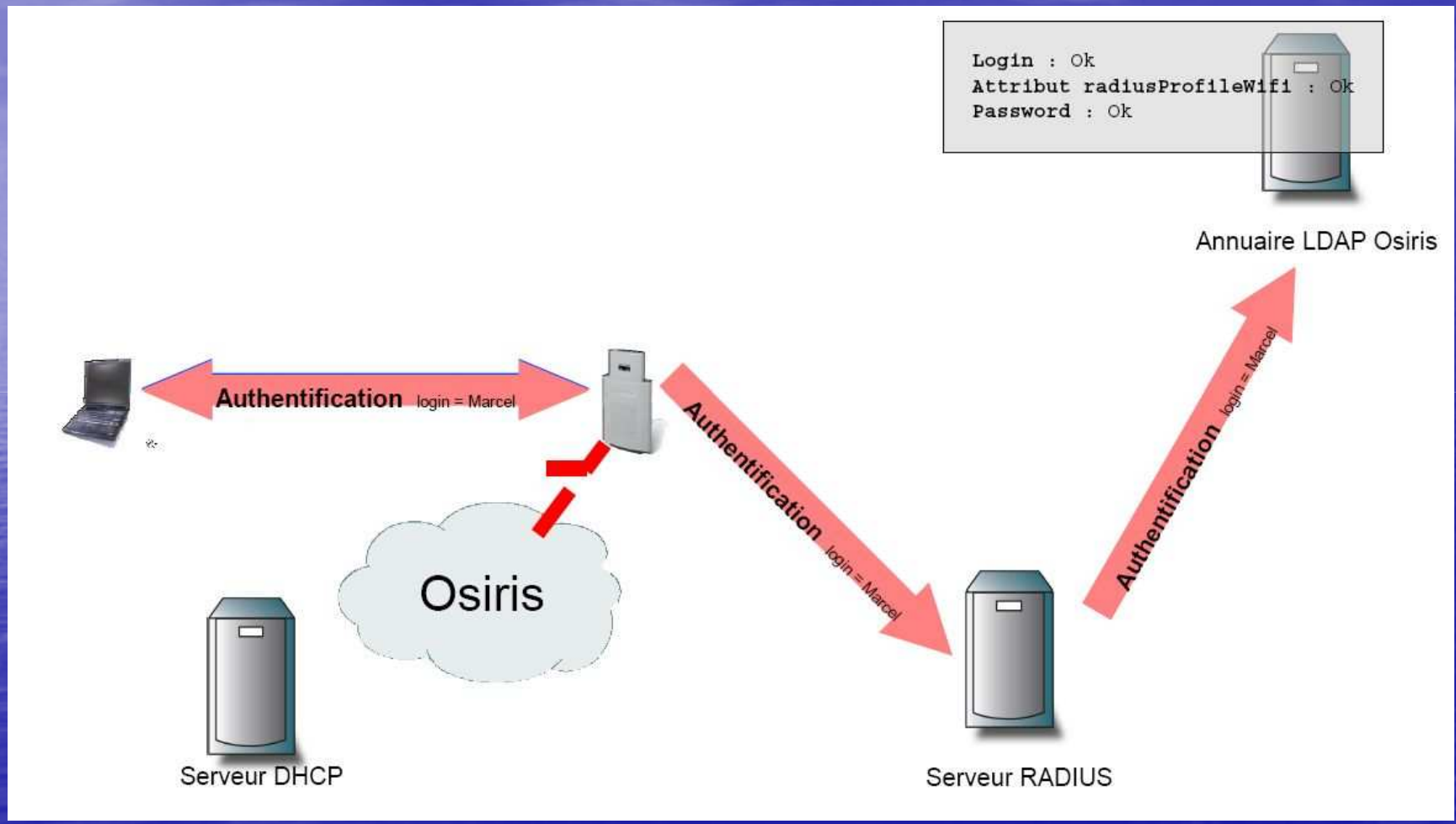
Le réseau sans-fil OSIRIS



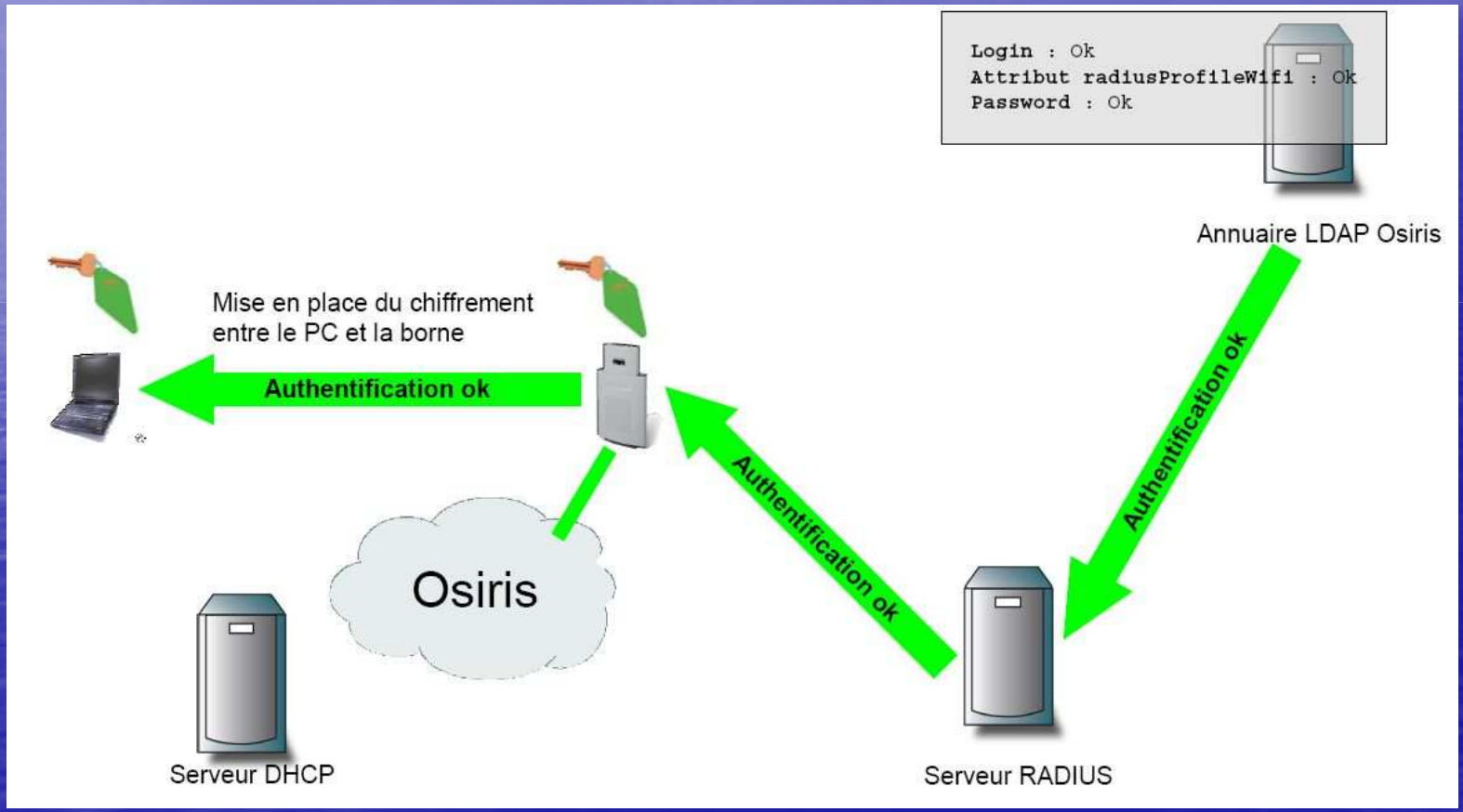
Le réseau sans-fil OSIRIS-SEC

- OSIRIS-SEC : sécurisé
  - Client dédié
    - SecureW2 pour 2000/XP
    - WPASupplicant pour Linux)
  - Ssid osiris-sec
    - Basé sur 802.1X
    - Authentification EAP/TTLS/PAP
    - Chiffrement TKIP, attribution/rotation
- http://www-crc.u-strasbg.fr/osiris/services/wifi/
- http://www-crc.u-strasbg.fr/osiris/services/wifi/public/osiris_open.html

Le réseau sans-fil OSIRIS-SEC



Le réseau sans-fil OSIRIS-SEC

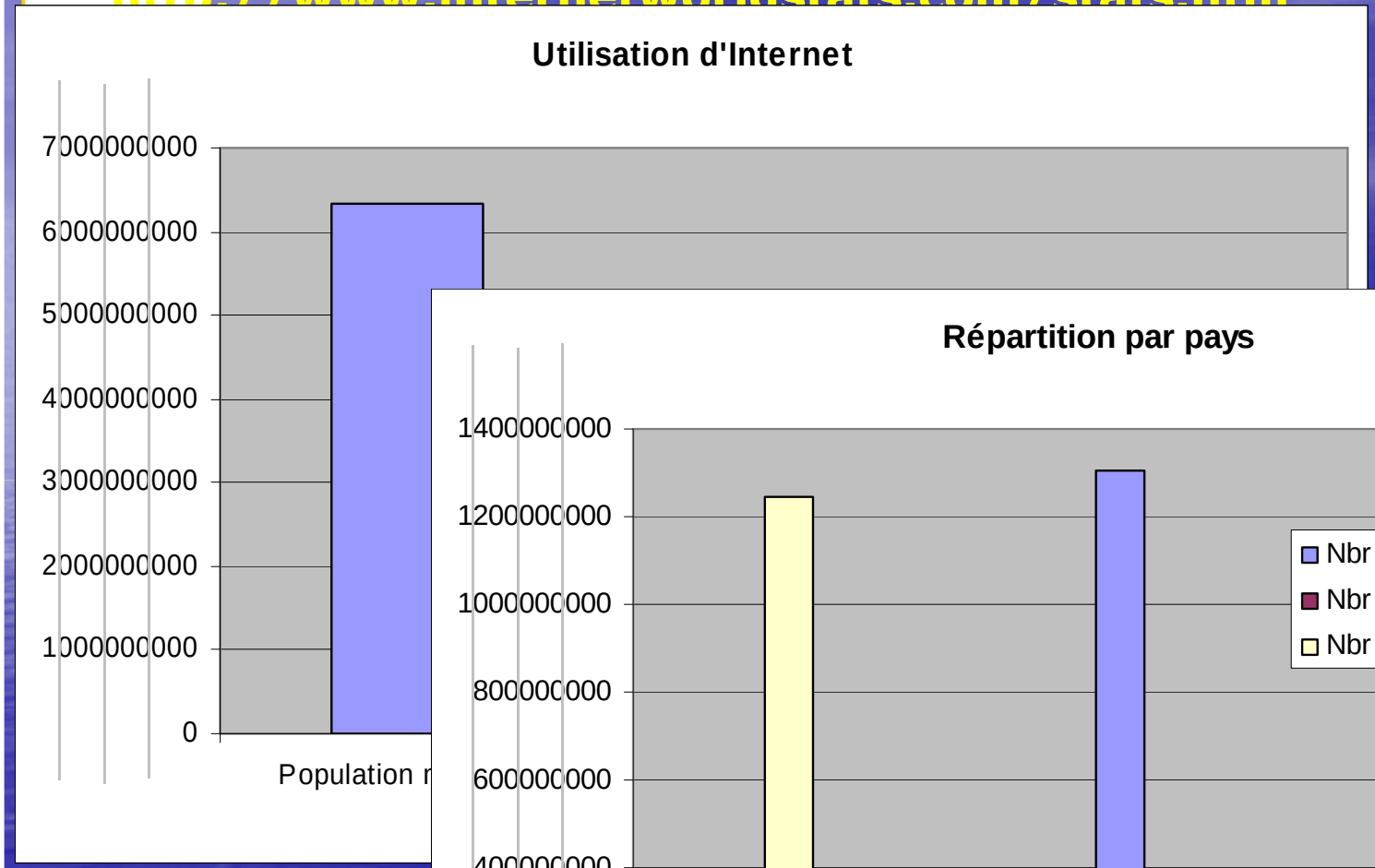


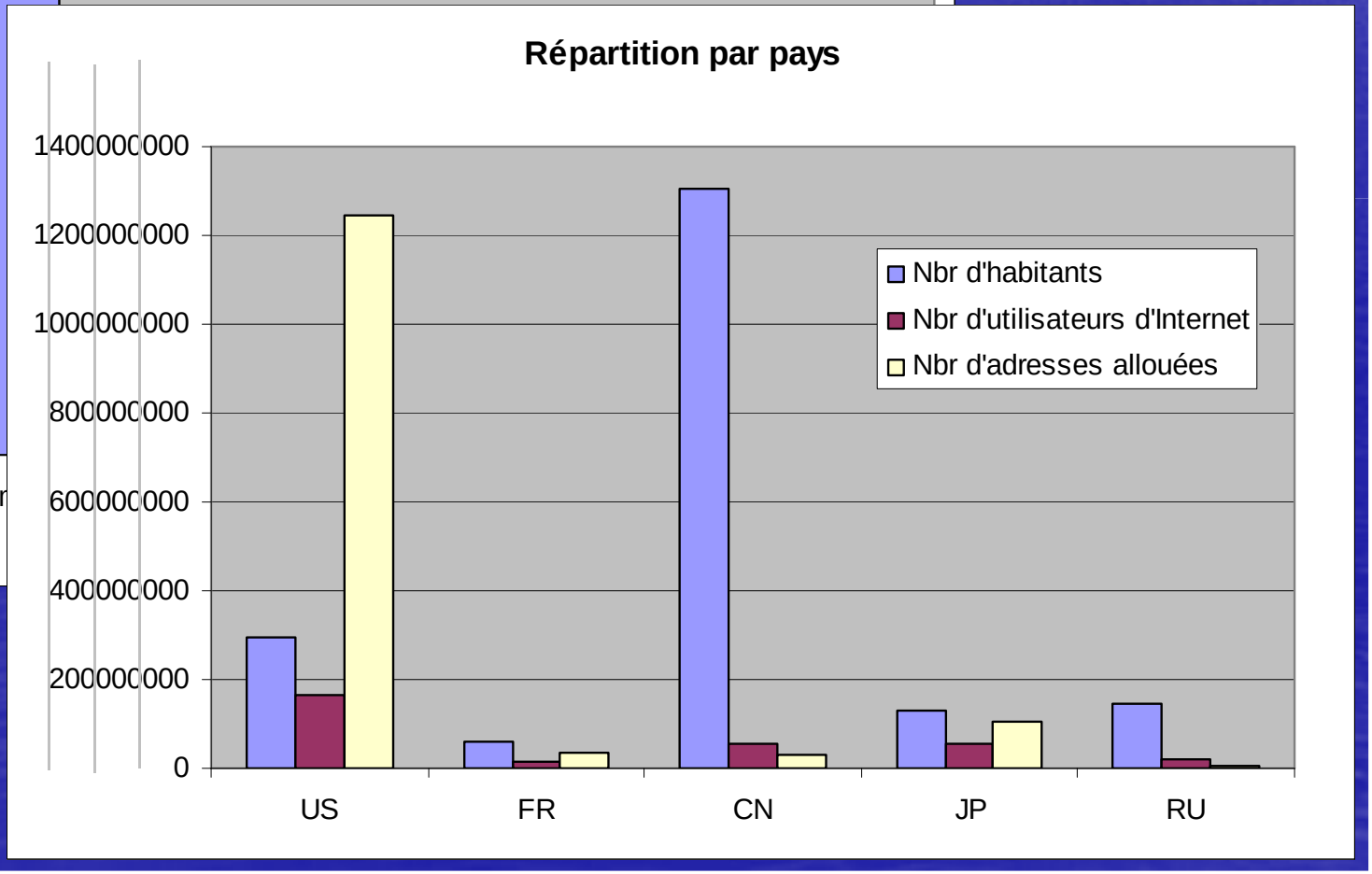
Adressage IP : l'avenir ?

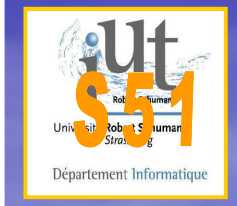
- Problèmes :
  - Découpage statique en classes
  - Espace d 'adressage insuffisant
  - Explosion des tables de routage
  - Qualité de service, sécurité, flexibilité
- Solutions
  - NAT : Translation d'adresses et proxy
  - CIDR : Classless Inter Domain Routing
  - IPv6 adressage et services

Espace d ’adressage IPv4

http://www.internetworldstats.com/stats.htm







IPv6

- Pourquoi un nouveau Protocole IP ?
- Caractéristiques d'IPv6
- Format et adressage
- Les nouvelles fonctionnalités
- La transition vers IPv6

IPv6 : Caractéristiques

- Adresse étendue : 128 bits (16 octets)
  - adressage de 340 x 10 e36 équipements
  - adressage hiérarchique
  - Autoconfiguration avec adresse MAC (IEEE802)
- 3 types d'adresses :
  - Unicast
  - Multicast
  - Anycast

plus d'adresse de broadcast

IPv6 Caractéristiques

- En-tête simplifié
  - nombre de champs réduit de moitié

  => augmente l'efficacité de commutation des équipements de routage
- Extension de l'en-tête pour les options
  - Les options IPv6 sont placées dans des en-têtes séparés, intercalés entre l'en-tête IPv6 et l'en-tête de la couche transport

    => introduction aisée de nouvelles fonctionnalités
  - la longueur des options n'est plus limitée à 40 octets

IPv6 Nouvelles fonctionnalités

- Autoconfiguration : "*plug and play*"
  - Gestion de la mobilité
  - Renumérotation facile si changement de prestataire
  - Protocole de découverte de voisinage
    - ND Neighbor Discovery
    - RA Router Advertisement

IPv6 Nouvelles fonctionnalités

- "Marquage" des flux particuliers : (*Flow Label*)
  - applications temps réel, Qualité de Service (QoS)
  - Priorité du trafic de contrôle
- Sécurité :
  - authentification et intégrité des données
  - confidentialité par chiffrement
- Routage à partir de la source
  - Source Demand Routing Protocol

Représentation des adresses

- Format de Base (16 octets):

  Adresse IPv6 Globale :

  - 0300:BA98:7654:3210:FEDC:BA98:7654:3210
- Format compressé :
  - FF01:0:0:0:0:0:0:43 => FF01::43

  Notation spéciale pour compatibilité IPv4 :
  - 0:0:0:0:0:0:FFFF:134.157.4.16 => ::FFFF:134.157.4.16

IPv6 : Préfixes

- La notion de préfixes développée par CIDR est reprise
- On les note sous la forme :

  Adresse IPv6 / longueur du préfixe

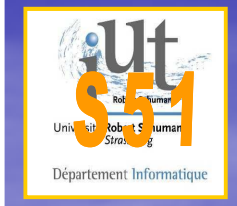
  Exemples :

  ff00::/8 3FFE:302:12::/48
- On peut indiquer qu'une adresse fait partie d'un réseau dont le préfixe est de longueur déterminée (netmask)

  3FFE:302:12:2:a00:20ff:fe18:964c/64

IPv6 : Préfixes Renater

- 2001:0660::/32 RENATER
- 2001:0660:4700::/40 OSIRIS
- 2001:0660:4701::/48 ULP-STRASBOURG
- 2001:0660:4703::/48 U-RSCHUMAN-STRASBOURG
- 2001:0660:4749::/48 U-HAUTEALSACE-MULHOUSE
- 2001:0660:4703:2001::/64 DPT Informatique IUT
- 2001:660:4703:2001:220:EDFF:FE70:CF0B/128 pipit


Département Informatique

IPv6 : Caractéristiques

- Adresse étendue : 128 bits (16 octets)
  - adressage de 340 x 10 e36 équipements
  - adressage hiérarchique
  - Autoconfiguration avec adresse MAC (IEEE802)
- 3 types d'adresses :
  - Unicast
  - Multicast
  - Anycast

plus d'adresse de broadcast

IPv6 Caractéristiques

- En-tête simplifié
  - nombre de champs réduit de moitié

  => augmente l'efficacité de commutation des équipements de routage
- Extension de l'en-tête pour les options
  - Les options IPv6 sont placées dans des en-têtes séparés, intercalés entre l'en-tête IPv6 et l'en-tête de la couche transport

    => introduction aisée de nouvelles fonctionnalités
  - la longueur des options n'est plus limitée à 40 octets

IPv6 Nouvelles fonctionnalités

- Autoconfiguration : "*plug and play*"
  - Gestion de la mobilité
  - Renumérotation facile si changement de prestataire
  - Serveurs d'adresses (DHCP : *Dynamic Host Configuration Protocol)*
  - et SAA : *Stateless Address Autoconfiguration (RFC 1971)*

IPv6 Nouvelles fonctionnalités

- "Marquage" des flux particuliers : (*Flow Label*)
  - applications temps réel, Qualité de Service (QoS)
  - Priorité du trafic de contrôle
- Sécurité :
  - authentification et intégrité des données
  - confidentialité par chiffrement
- Routage à partir de la source
  - Source Demand Routing Protocol

Représentation des adresses

- Format de Base (16 octets):

  Adresse IPv6 Globale :
  - 0300:BA98:7654:3210:FEDC:BA98:7654:3210
- Format compressé :
  - FF01:0:0:0:0:0:0:43 => FF01::43

  Notation spéciale pour compatibilité IPv4 :
  - 0:0:0:0:0:0:FFFF:134.157.4.16 => ::FFFF:134.157.4.16

IPv6 : Préfixes

- La notion de préfixes développée par CIDR est reprise
- On les note sous la forme :

  Adresse IPv6 / longueur du préfixe

  Exemples :

  ff00::/8 3FFE:302:12::/48
- On peut indiquer qu'une adresse fait partie d'un réseau dont le préfixe est de longueur déterminée (netmask)

  3FFE:302:12:2:a00:20ff:fe18:964c/64

IPv6 : Préfixes Renater

- 2001:0660::/32 RENATER
- 2001:0660:4700::/40 OSIRIS
- 2001:0660:4701::/48 ULP-STRASBOURG
- 2001:0660:4703::/48 U-RSCHUMAN-STRASBOURG
- 2001:0660:4749::/48 U-HAUTEALSACE-MULHOUSE
- 2001:0660:4703:2001::/64 DPT Informatique IUT
- 2001:660:4703:2001:220:EDFF:FE70:CF0B/128 pipit

Ipv6 sous Windows XP

```
F:\Documents and Settings\>ipv6 install …
F:\Documents and Settings\>ipv6 if
Interface 6 :  Ethernet: Connexion au réseau local
   utilise la découverte de voisins
  utilise la découverte de routeur
  adresse de la couche de liaison : 00-0c-6c-36-6f-64
    preferred global 2a01:5d8:48f3:3b9d:b1c8:90c6:fa5e:a690, vie 23h59m9s/17h43m7s (temporaire)
    preferred global 2a01:5d8:48f3:3b9d:20c:6cff:fe36:6f64, vie 23h59m9s (public)
    preferred link-local fe80::20c:6cff:fe36:6f64, vie infinite
    multidiffusion interface-local ff01::1, 1 références, non signalable
    multidiffusion link-local ff02::1, 1 références, non signalable
    multidiffusion link-local ff02::1:ff36:6f64, 2 références, dernier informateur
    multidiffusion link-local ff02::1:ff5e:610, 1 références, dernier informateur
  MTU de liaison 1480 (MTU de liaison réelle 1500)
  limite de sauts actuelle 64
  durée d'attente pour la communication 25000ms (base 30000ms)
  intervalle de retransmission 1000ms
  transmissions DAD 1
  longueur par défaut du préfixe de site 48
```

Ipv6 à l'insu de …

```
F:\Documents and Settings\>ping ftp.u-strasbg.fr

Envoi d'une requête 'ping' sur anubis.u-strasbg.fr [2001:660:2402::6] avec 32 octets de
    données :

Réponse de 2001:660:2402::6 : temps=45 ms
Réponse de 2001:660:2402::6 : temps=44 ms
Réponse de 2001:660:2402::6 : temps=44 ms
Réponse de 2001:660:2402::6 : temps=45 ms

Statistiques Ping pour 2001:660:2402::6:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 44ms, Maximum = 45ms, Moyenne = 44ms
```