Cartographie Réseau et Inventaire

CR&I

Ecole Nationale Supérieure de Chimie de Paris

Eric Chevigny, Kemal Ozcan
Et Bernard Bellamy

JRES 2005

SOMMAIRE

1. Présentation de l’ENSCP
2. Travail réalisé
3. Bilan
4. Démonstration

L'Ecole Nationale Supérieure de Chimie de Paris

- Formation d'ingénieurs chimistes généralistes
- Fondée en 1896 par Charles Friedel

- Membre fondateur de ParisTech
- Membre de la fédération Gay-Lussac
- Membre de l'UPMC

Charles Friedel

L'Ecole Nationale Supérieure de Chimie de Paris

300 élèves ingénieurs

45 enseignants

8 laboratoires (umr)

40 chercheurs

80 doctorants et post-doctorants

Formation

Recherche

1 RSSI

Service Réseau

1 administrateur

Administration

30 personnes

Sauvegardes

Sécurité

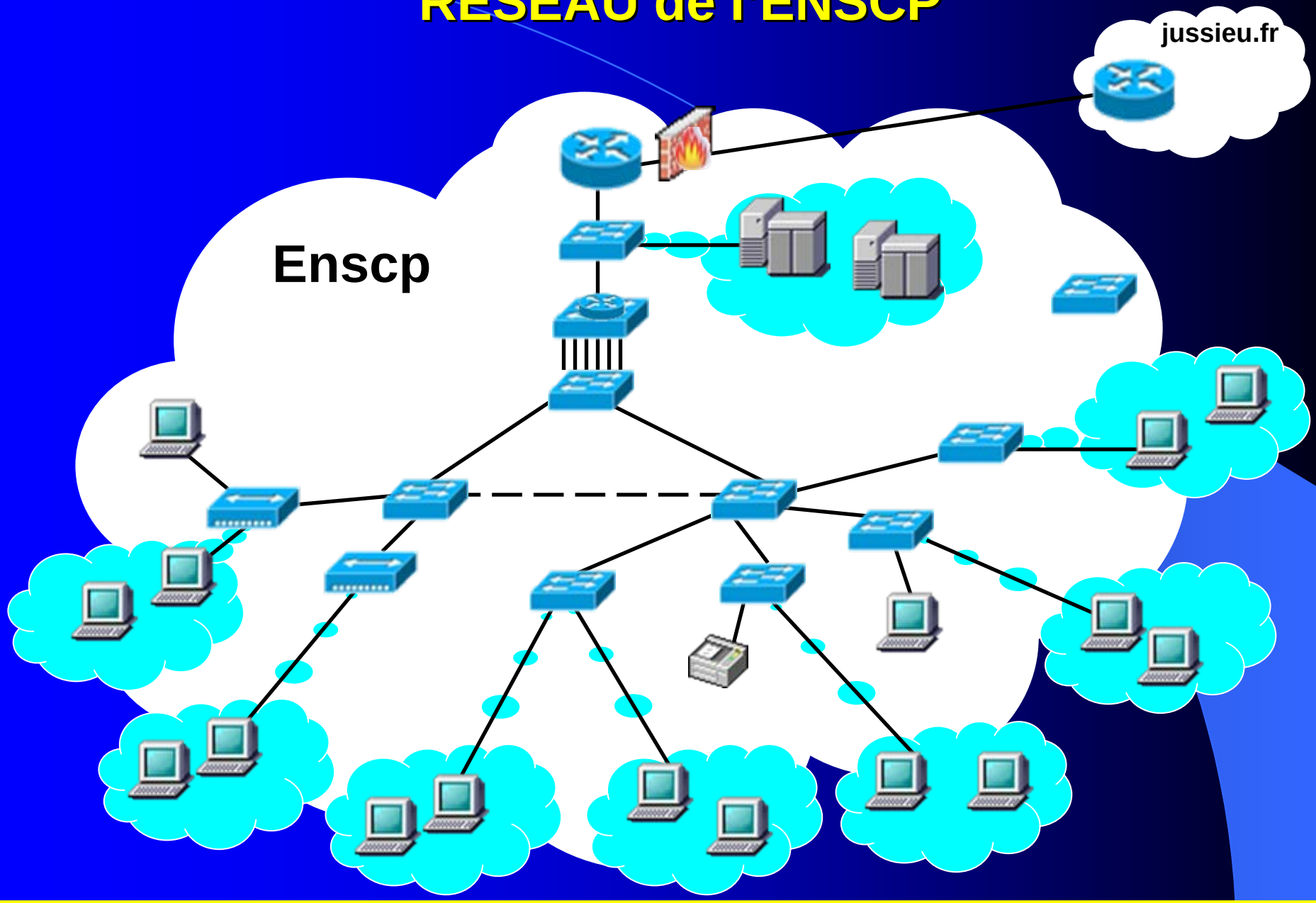
web

Développement

e-mail

Maintenance

RESEAU de l'ENSCP



SOMMAIRE

1. Présentation de l’ENSCP
2. Travail réalisé (le premier CR&I)
3. Bilan
4. Démonstration

SOLUTION

- Système réparti basé sur les protocoles de l'Internet

  - Protocoles : ARP, SNMP, ICMP, DNS, TCP
  - mib II
  - Langages : Perl, PHP, Java

ALGORITHME

Inventaire des éléments actifs

- **ETAPE 1 : récupérer la configuration réseau de l'hôte**

adresses IP

netmask

adresses MAC (physique)

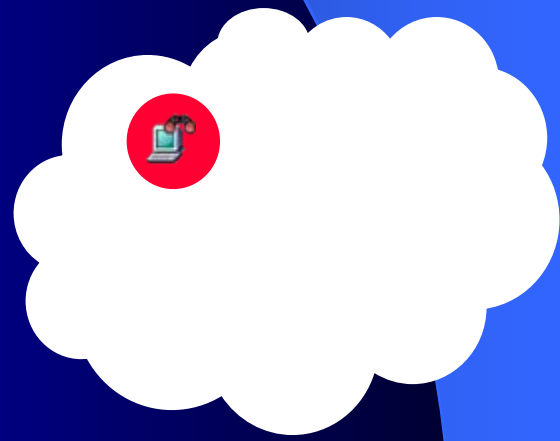
hostnames (noms DNS)

nicname (nom netBIOS, ...)

Default Gateways

DNS

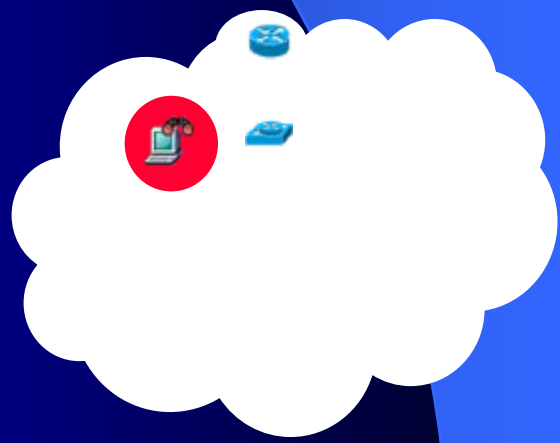
WINS



Inventaire des éléments actifs

➢ **ETAPE 2 : rechercher les routeurs du réseau administré**

# If	Route	next Hop	Type	Mask
#				
# 1	0.0.0.0	134.157.181.254	direct	0.0.0.0
# 12	169.18.0.0	0.0.0.0	direct	255.255.255.0
# 10	169.16.0.0	0.0.0.0	direct	255.255.255.0
# 4	169.10.0.0	0.0.0.0	direct	255.255.255.0
# 9	169.15.0.0	0.0.0.0	direct	255.255.255.0
# 6	169.12.0.0	0.0.0.0	direct	255.255.255.0
# 2	169.0.0.0	0.0.0.0	direct	255.255.0.0
# 1	134.157.180.0	0.0.0.0	direct	255.255.254.0
# 8	169.14.0.0	0.0.0.0	direct	255.255.255.0
# 3	169.32.0.0	0.0.0.0	direct	255.255.0.0
# 11	169.17.0.0	0.0.0.0	direct	255.255.255.0
# 7	169.13.0.0	0.0.0.0	direct	255.255.255.0
# 5	169.11.0.0	0.0.0.0	direct	255.255.255.0



Inventaire des éléments actifs

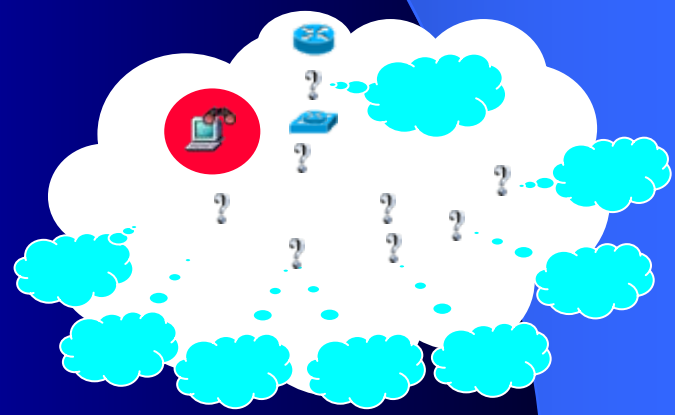
➢ **ETAPE 3 : déterminer les adresses des sous-réseaux**

# If	Route	next Hop	Type	Mask
#				
# 1	0.0.0.0	134.157.181.254	direct	0.0.0.0
# 12	169.18.0.0	0.0.0.0	direct	255.255.255.0
# 10	169.16.0.0	0.0.0.0	direct	255.255.255.0
# 4	169.10.0.0	0.0.0.0	direct	255.255.255.0
# 9	169.15.0.0	0.0.0.0	direct	255.255.255.0
# 6	169.12.0.0	0.0.0.0	direct	255.255.255.0
# 2	169.0.0.0	0.0.0.0	direct	255.255.0.0
# 1	134.157.180.0	0.0.0.0	direct	255.255.254.0
# 8	169.14.0.0	0.0.0.0	direct	255.255.255.0
# 3	169.32.0.0	0.0.0.0	direct	255.255.0.0
# 11	169.17.0.0	0.0.0.0	direct	255.255.255.0
# 7	169.13.0.0	0.0.0.0	direct	255.255.255.0
# 5	169.11.0.0	0.0.0.0	direct	255.255.255.0

Inventaire des éléments actifs

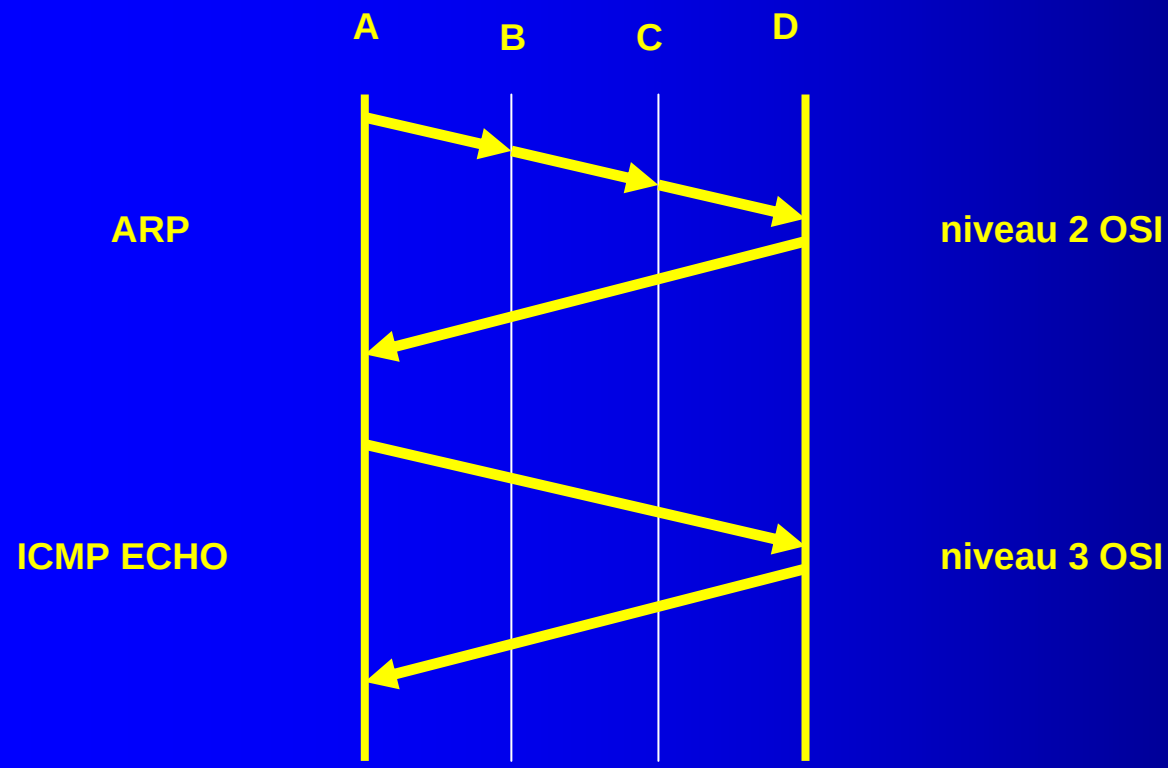
➢ ETAPE 4 : récupérer les tables arp

If	Adresse physique	Adresse IP	Type
5	00:03:93:xx:xx:xx	169.11.0.29	dynamic
1	00:0c:6e: xx:xx:xx	134.157.181.161	dynamic
6	00:a0:24: xx:xx:xx	169.12.0.50	dynamic
6	00:0c:6e: xx:xx:xx	169.12.0.20	dynamic
2	00:30:6e: xx:xx:xx	169.0.125.5	dynamic
7	00:02:3f: xx:xx:xx	169.13.0.200	dynamic
10	00:10:5a: xx:xx:xx	169.16.0.4	dynamic
8	00:02:e3: xx:xx:xx	169.14.0.56	dynamic
11	00:10:b5: xx:xx:xx	169.17.0.110	dynamic
2	00:50:fc: xx:xx:xx	169.0.30.1	dynamic
10	00:48:54: xx:xx:xx	169.16.0.2	dynamic
1	00:0b:fd: xx:xx:xx	134.157.181.254	dynamic
1	00:50:04: xx:xx:xx	134.157.181.180	dynamic



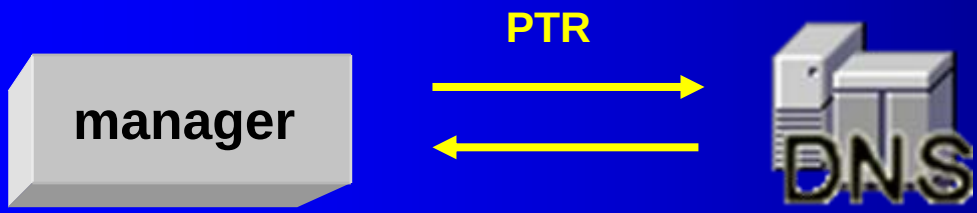
Inventaire des éléments actifs

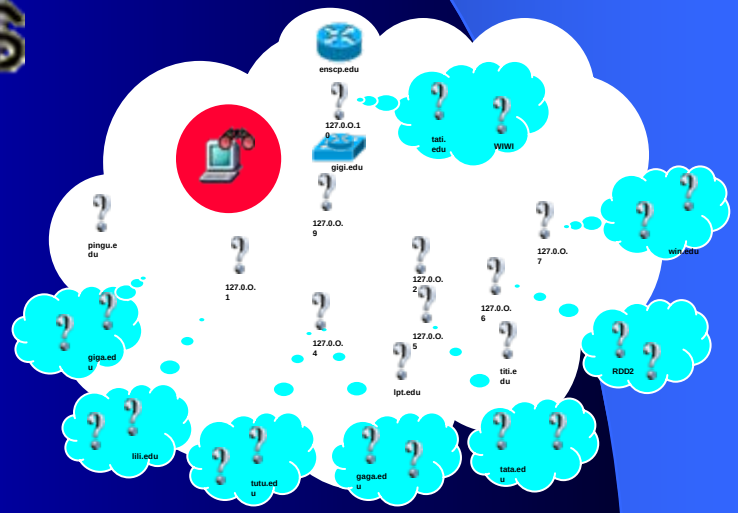
- **ETAPE 5 : sonder les sous-réseaux du réseau administré**



Inventaire des éléments actifs

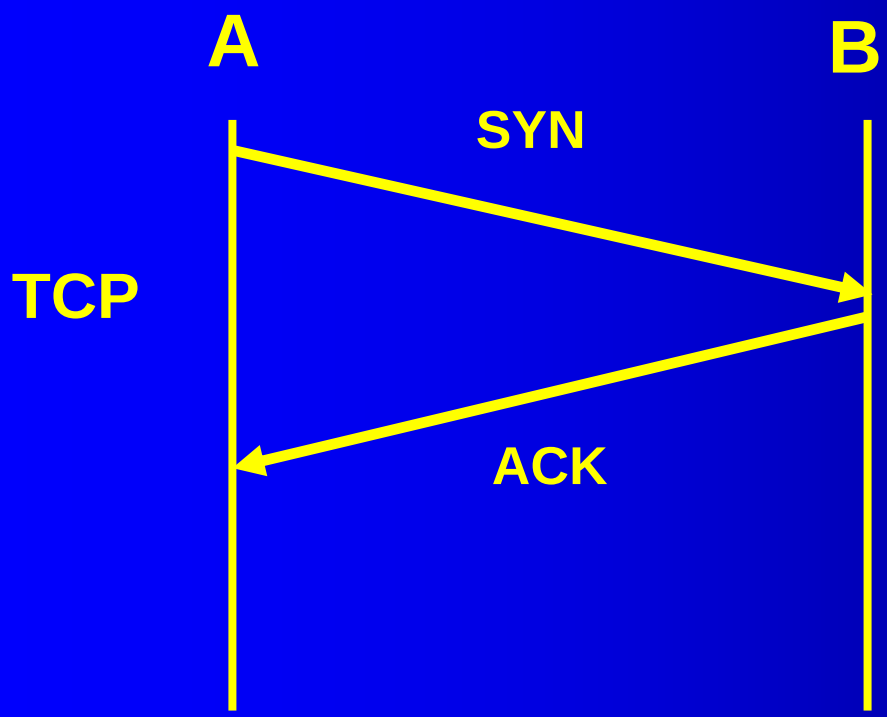
- **ETAPE 6 : résolution inverse de nom**

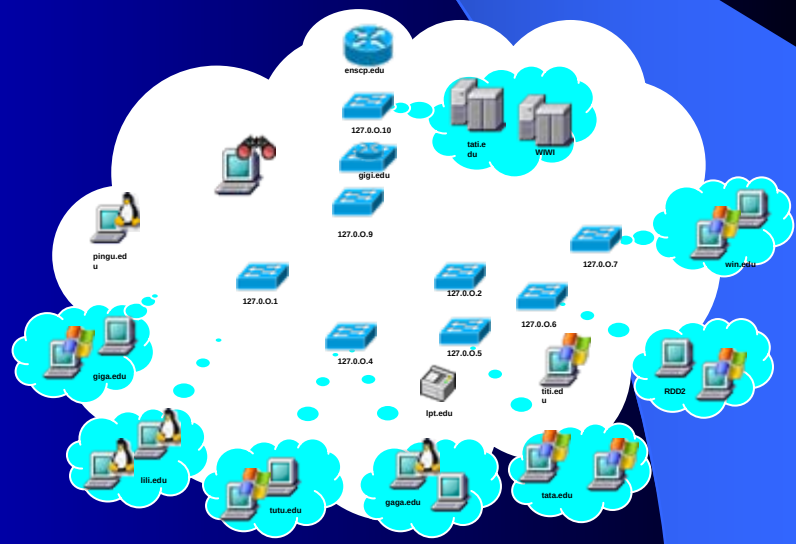




Inventaire des éléments actifs

- ETAPE 7 : déterminer le type de machine



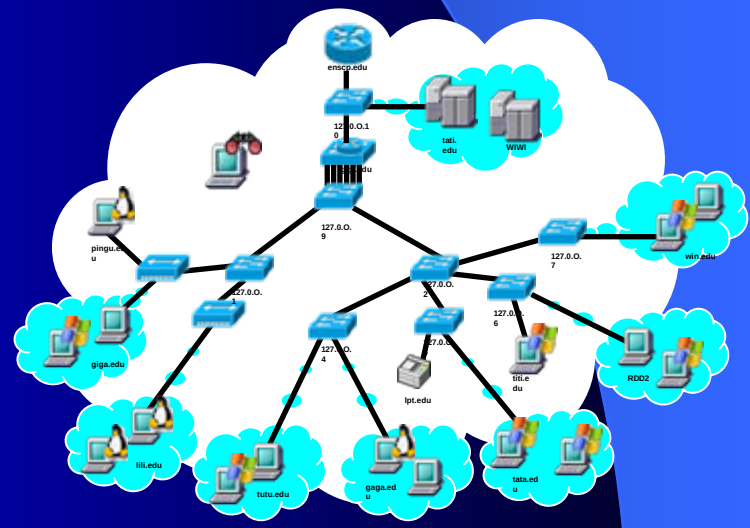


Découverte de la topologie

Découverte de la topologie

- **ETAPE 8 : définir la topologie à partir des AFT**

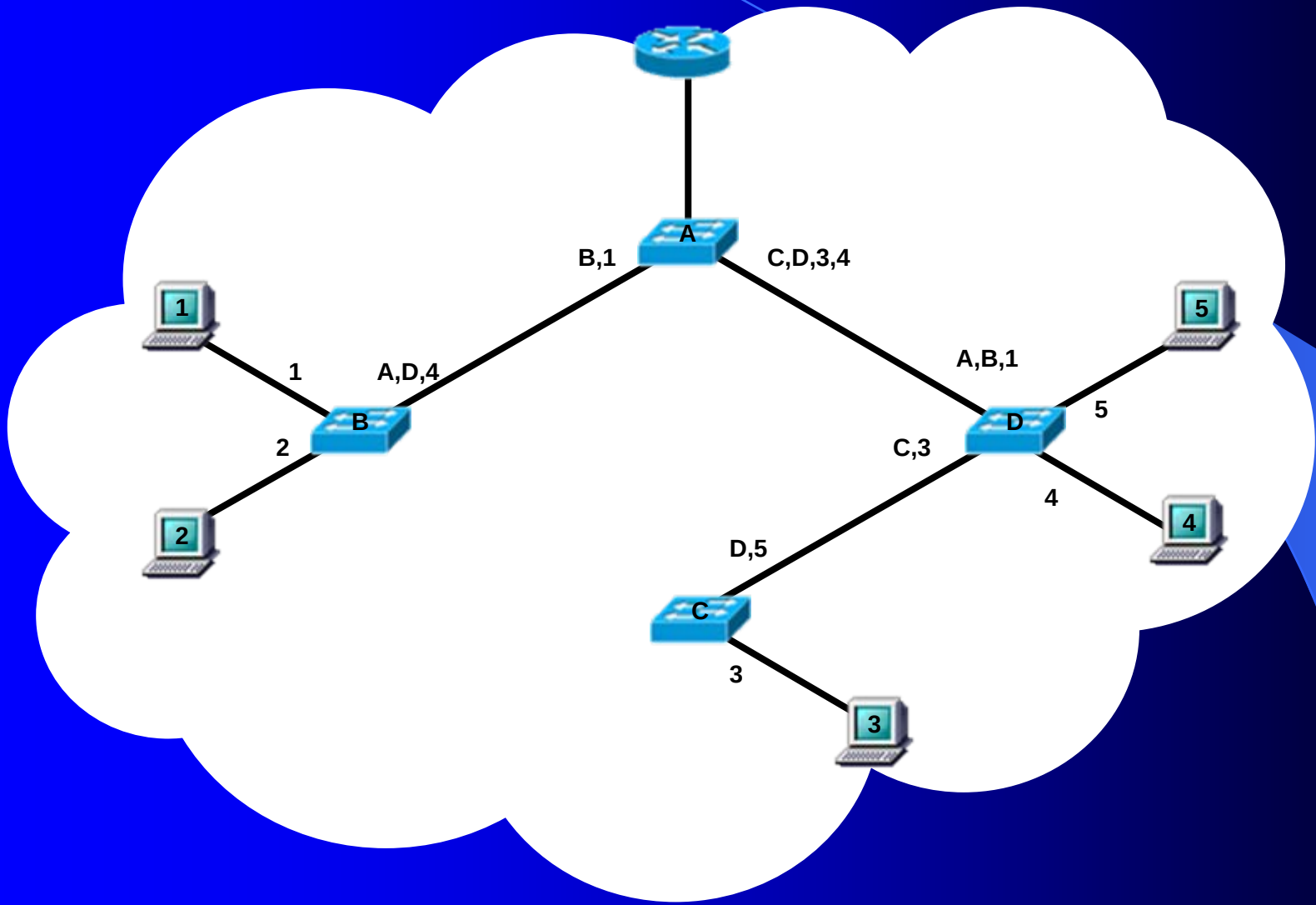
Adresse physique	If
00:03:93:xx:xx:xx	5
00:0c:6e: xx:xx:xx	1
00:a0:24: xx:xx:xx	6
00:0c:6e: xx:xx:xx	6
00:30:6e: xx:xx:xx	2
00:02:3f: xx:xx:xx	7
00:10:5a: xx:xx:xx	10
00:02:e3: xx:xx:xx	8
00:10:b5: xx:xx:xx	11
00:50:fc: xx:xx:xx	2
00:48:54: xx:xx:xx	10
00:0b:fd: xx:xx:xx	1
00:50:04: xx:xx:xx	1



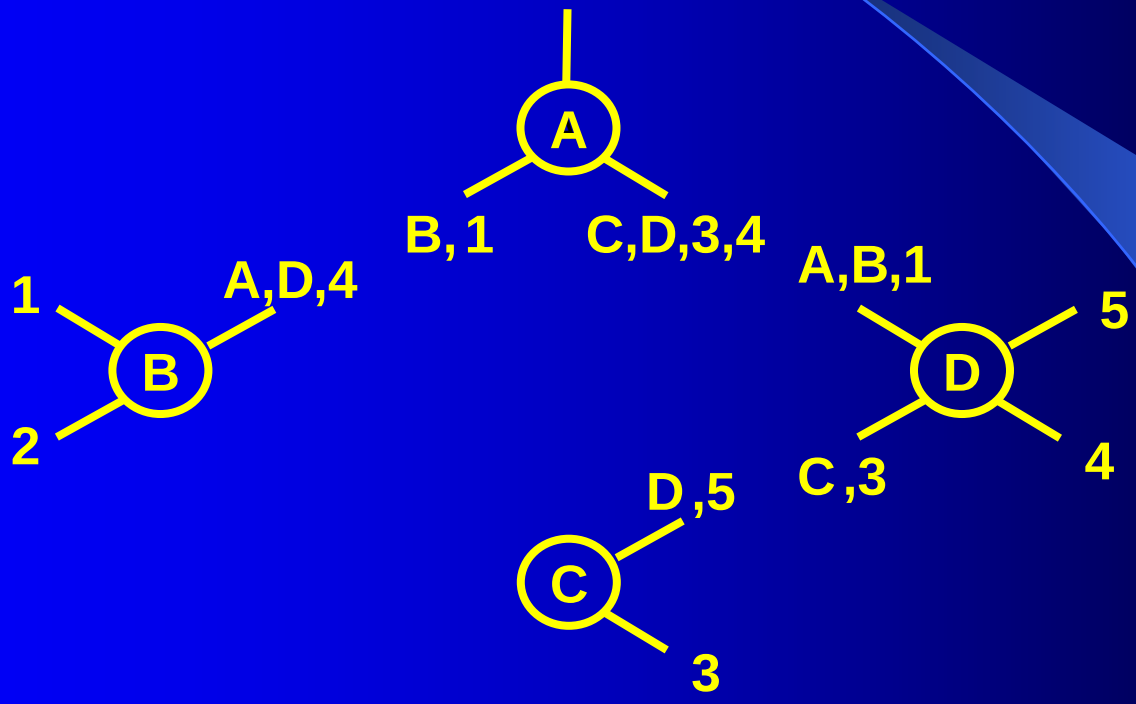
Découverte de la topologie

- Deux nœuds ne peuvent être connectés si ils sont visibles sur des ports différents !

Découverte de la topologie

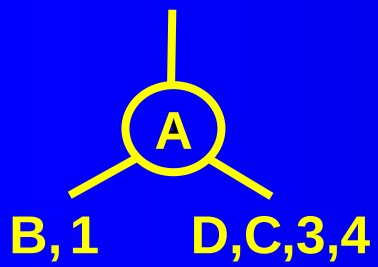


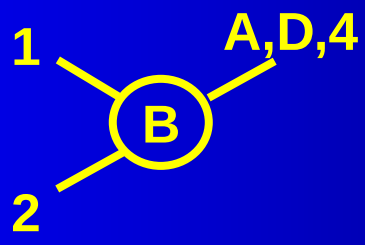
Découverte de la topologie

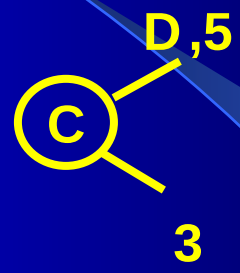


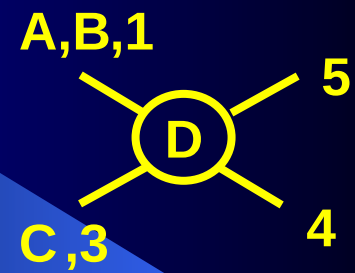
Découverte de la topologie

- A quel nœud l'hôte 1, est-il connecté ?









1 est connecté à A ?
- B non
- C peut être
- D oui

1 est connecté à B ?
- A oui
- C peut être
- D oui

1 est connecté à C ?
- A non
- B peut être
- D non

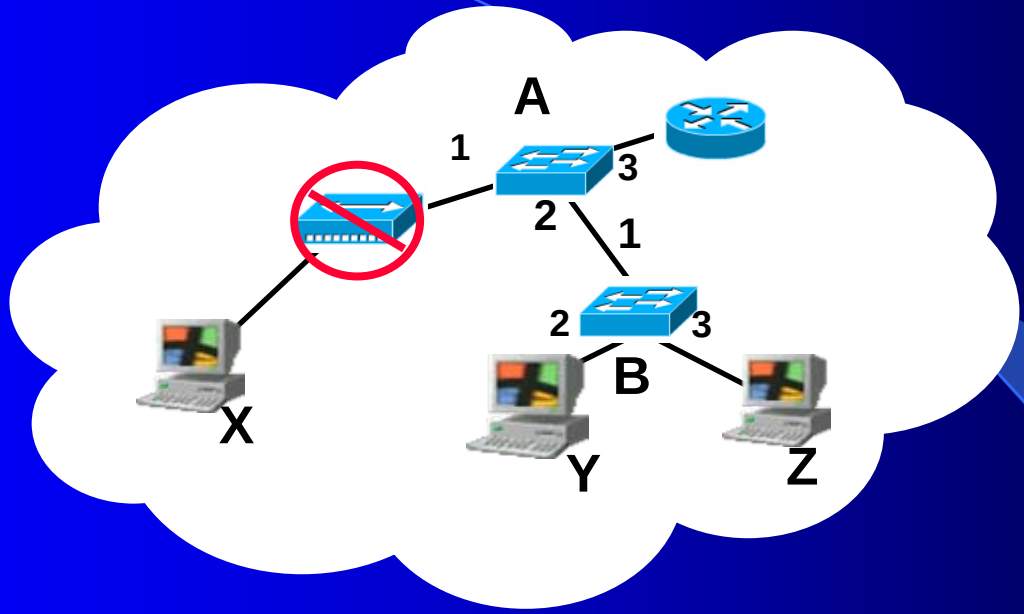
1 est connecté à D ?
- A non
- B non
- C peut être

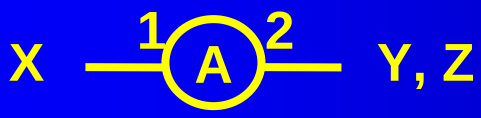
COMPLEXITE

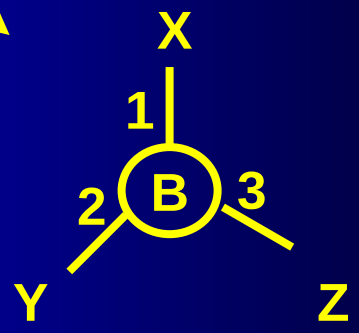
- nb hôtes x (nb nœuds -1) x nb noeuds

ex : 5 x (4 – 1) x 4 = 60

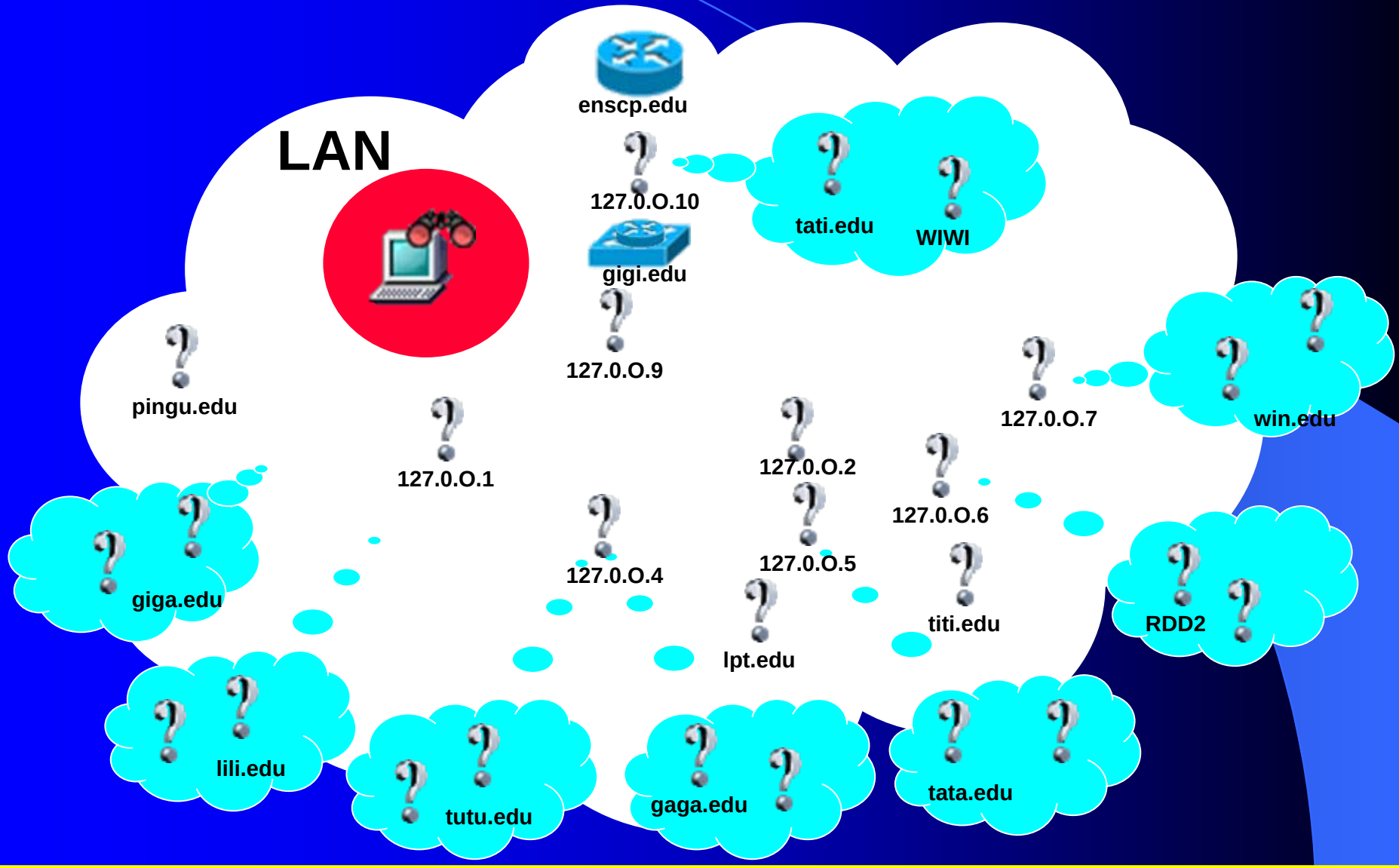
Découverte de la topologie



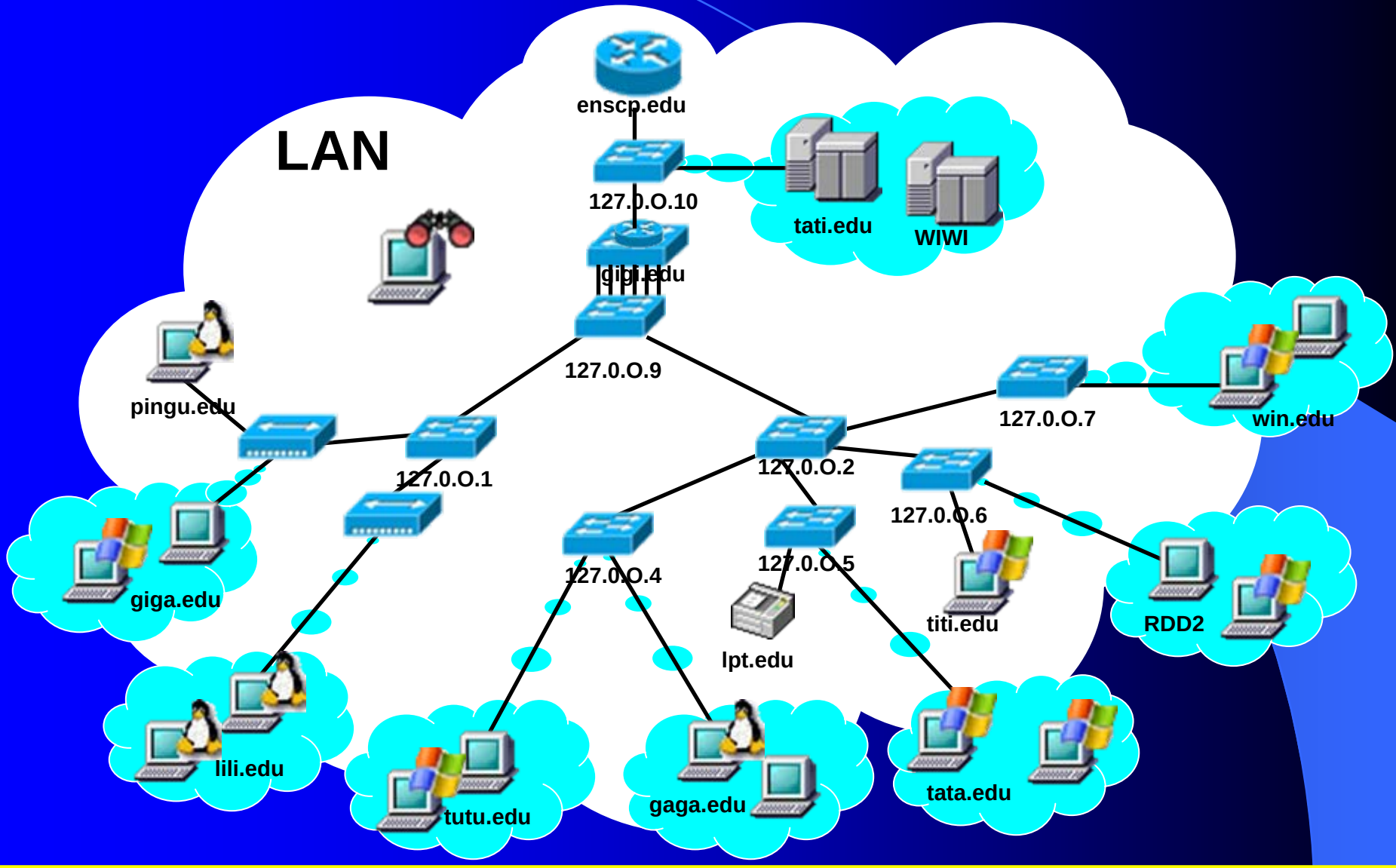




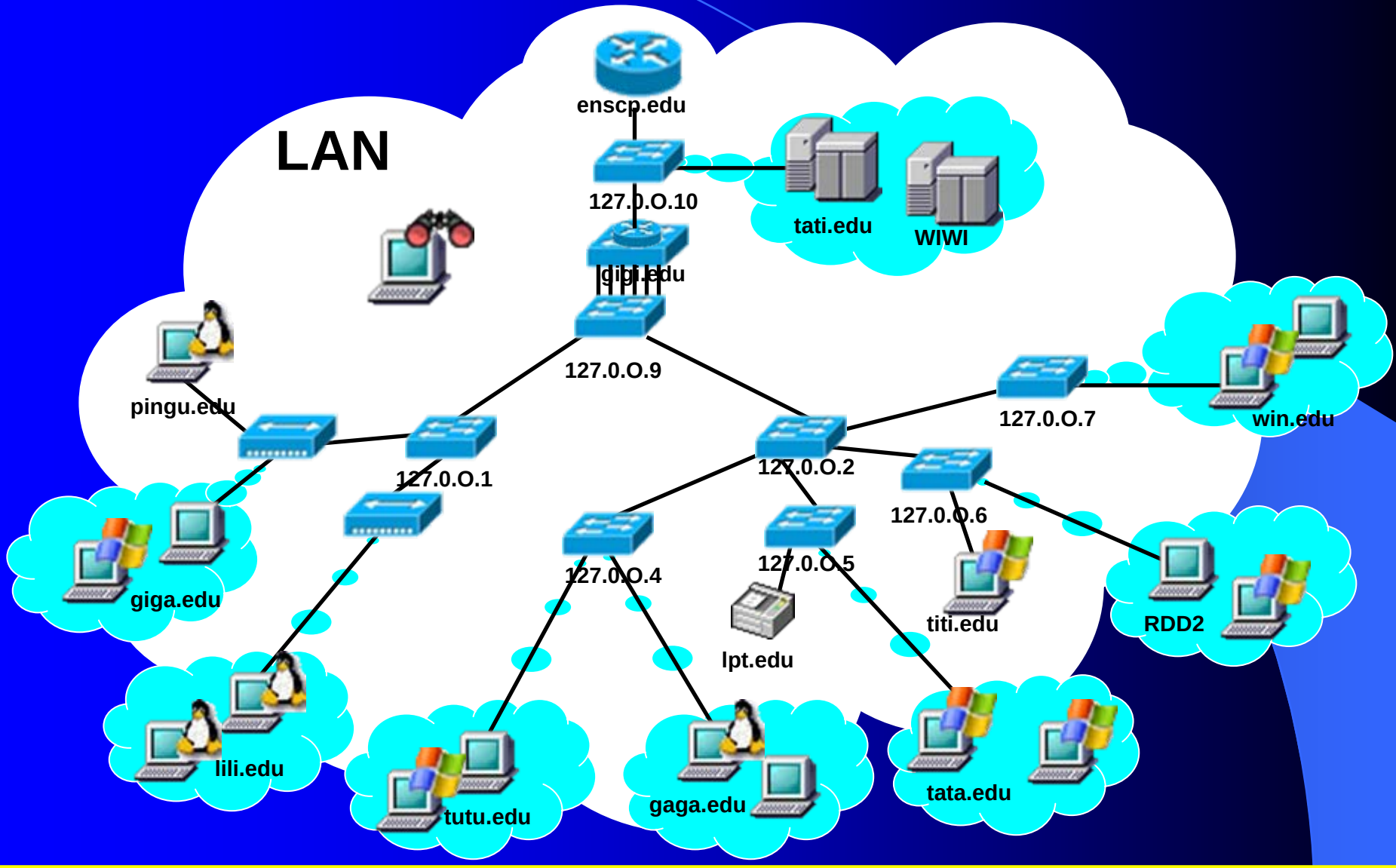
Inventaire des éléments actifs



Définition de la topologie

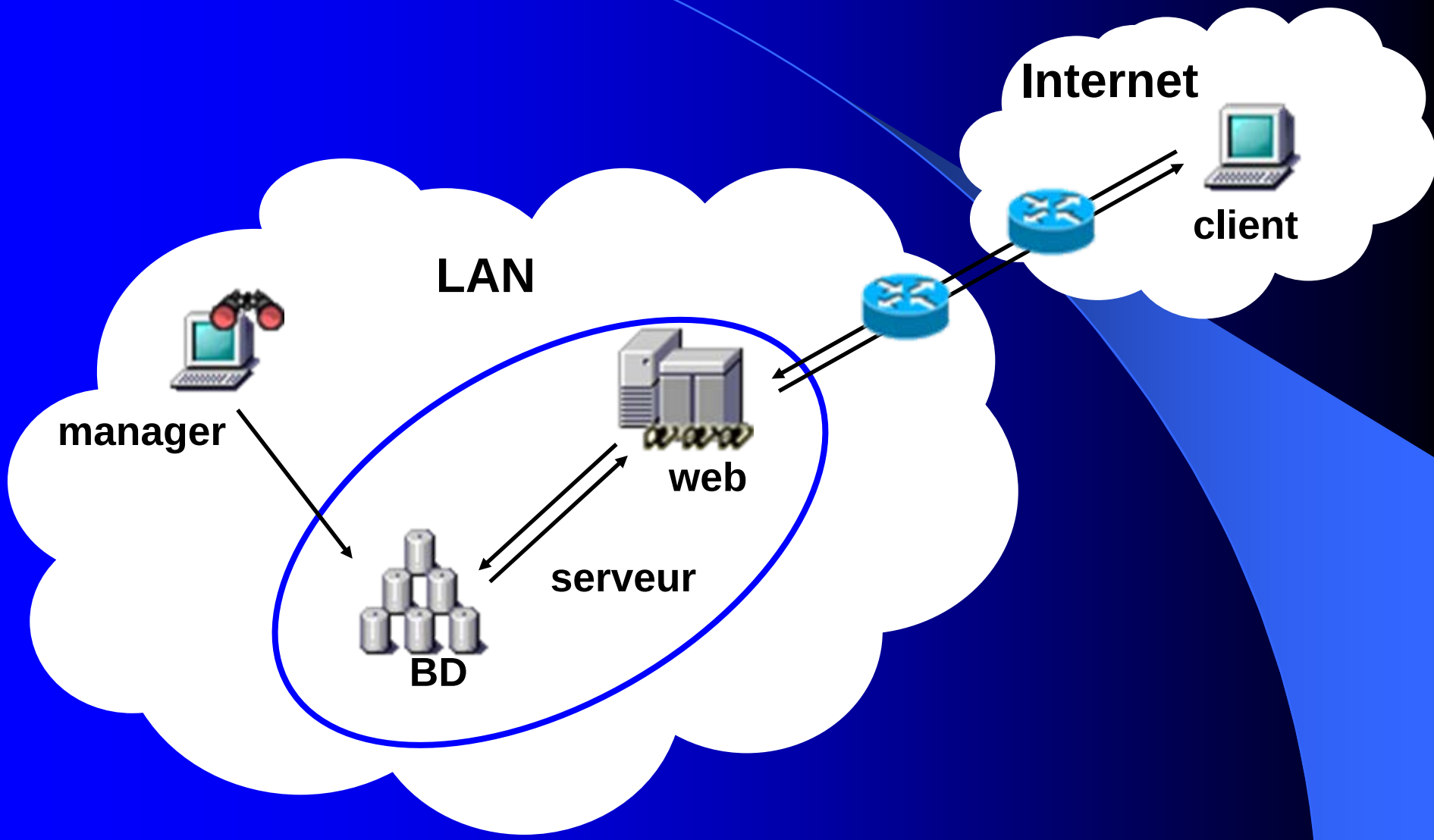


Définition de la topologie



ARCHITECTURE

Architecture de l'application



PREREQUIS POUR L'INSTALLATION

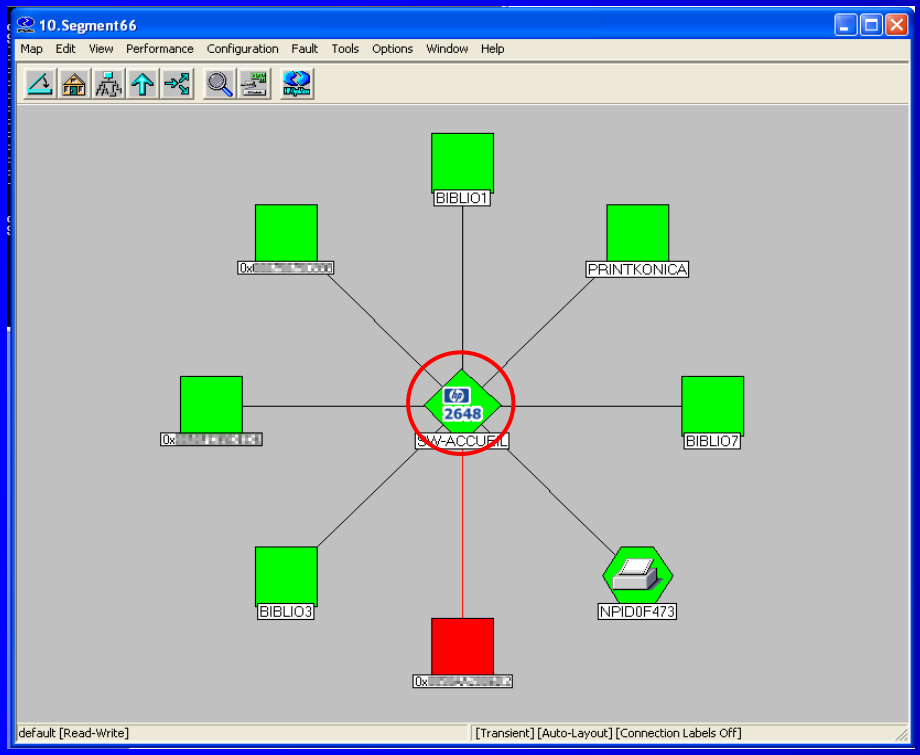
- **Perl : ActivePerl de ActiveState**
- **Serveur web : Apache ou IIS**
- **SGBD Mysql & Bases de données :**

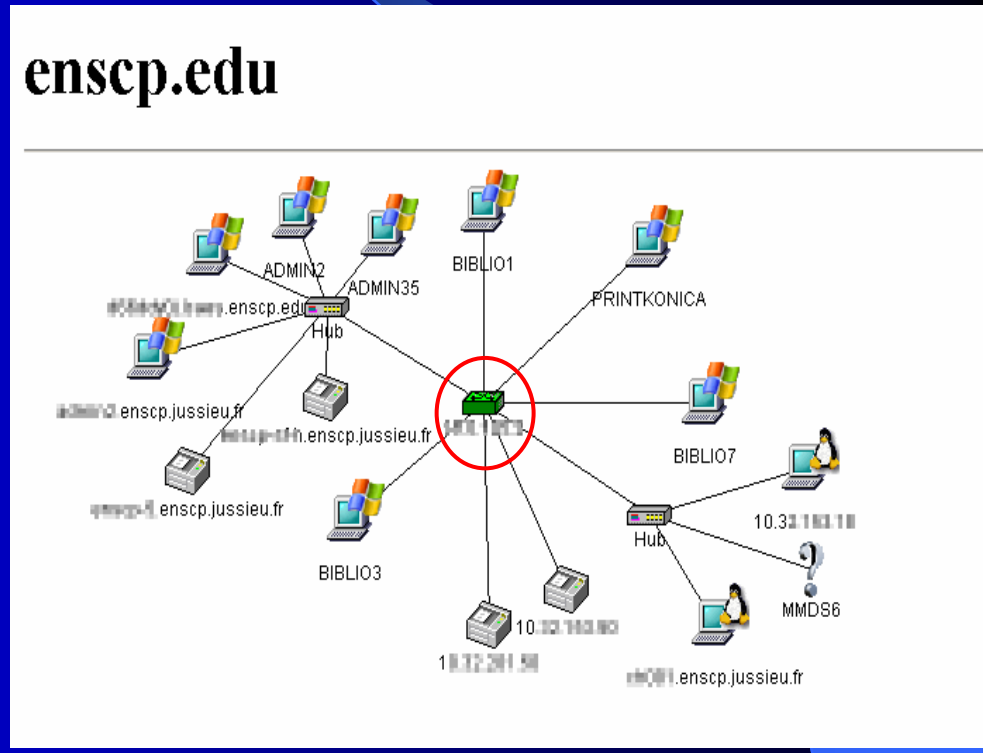
  Inventory,Topology, Admin
- **PHP**
  - **Authentifier**
  - **exécuter des processus sur le serveur (scan …)**
  - **traitements d'informations sur la base**

RESULTATS

TESTS COMPARATIFS

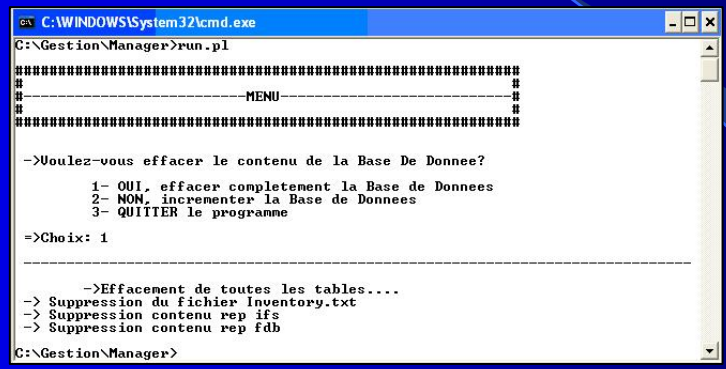
Comparaison avec Network Nodes Manager de HP



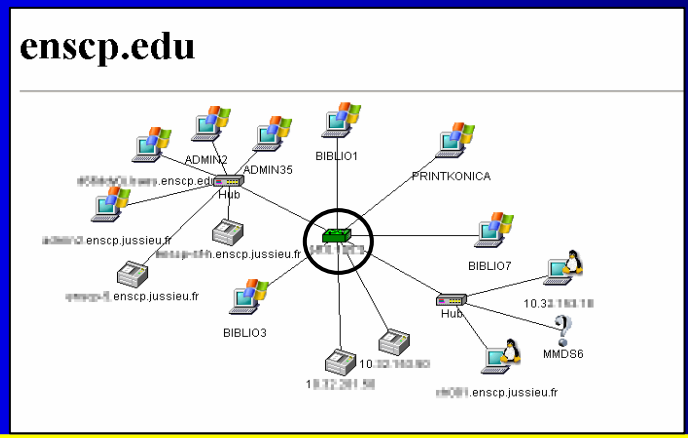


DEMONSTRATION

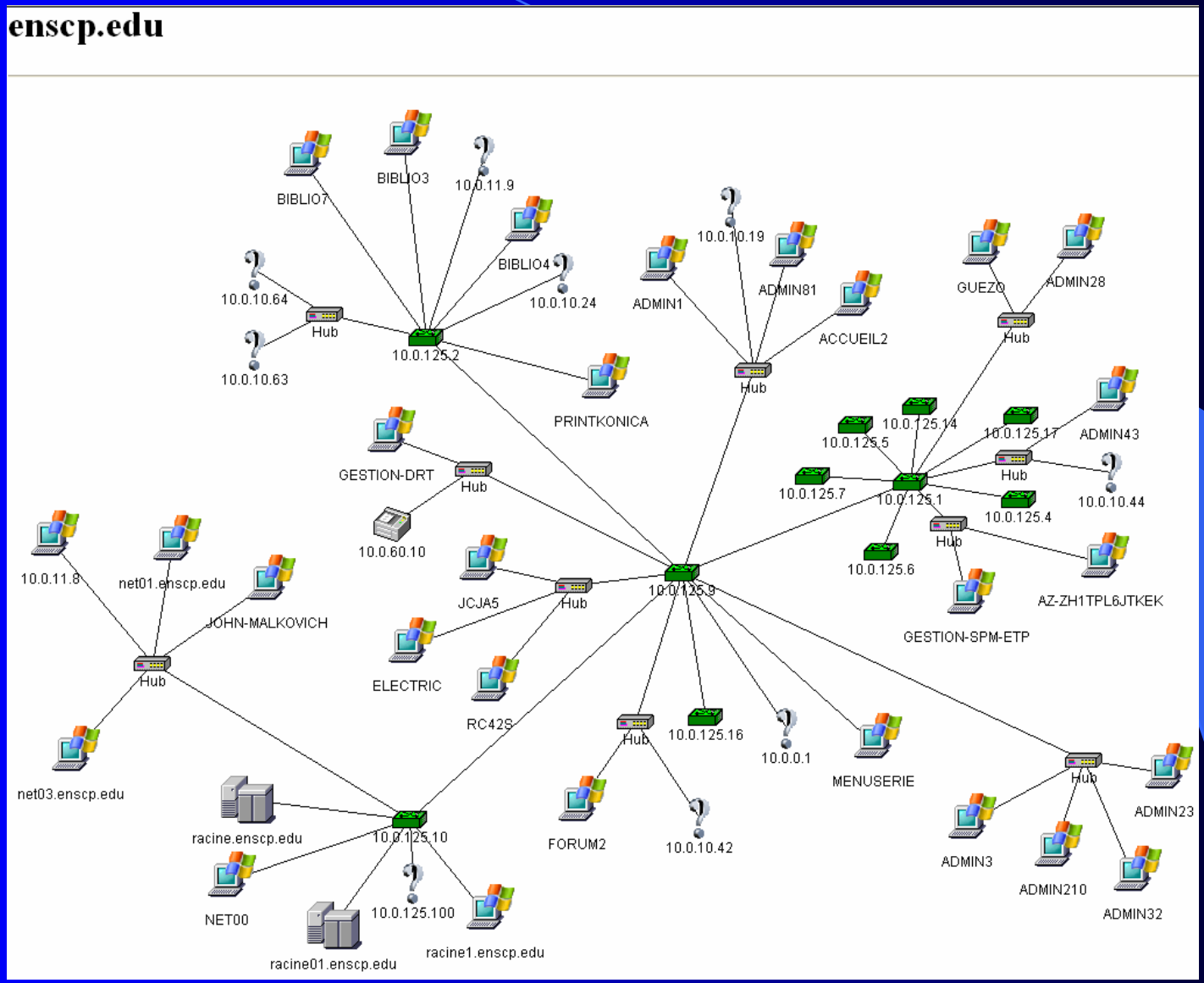
- **Inventaire en Lignes de Commande**



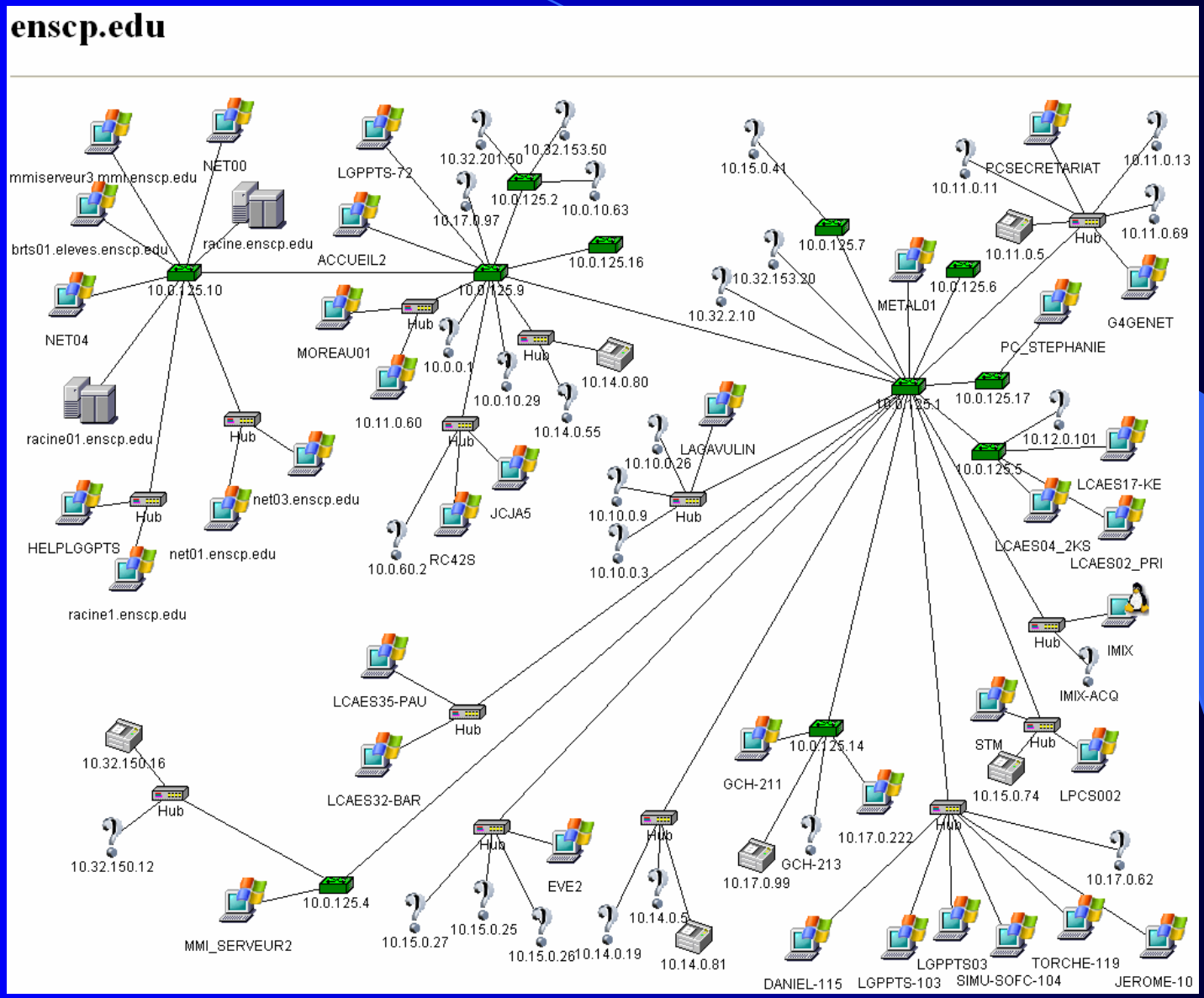
- **Cartographie depuis le Réseau**



Résultats scan 10.0.x.y 0<x<126



Résultats scan 10.x.0.0 0<x<32



A VENIR ?

- Gestion de parc
- Fault management
- ???