

Technologies LANs

Local Area Networks

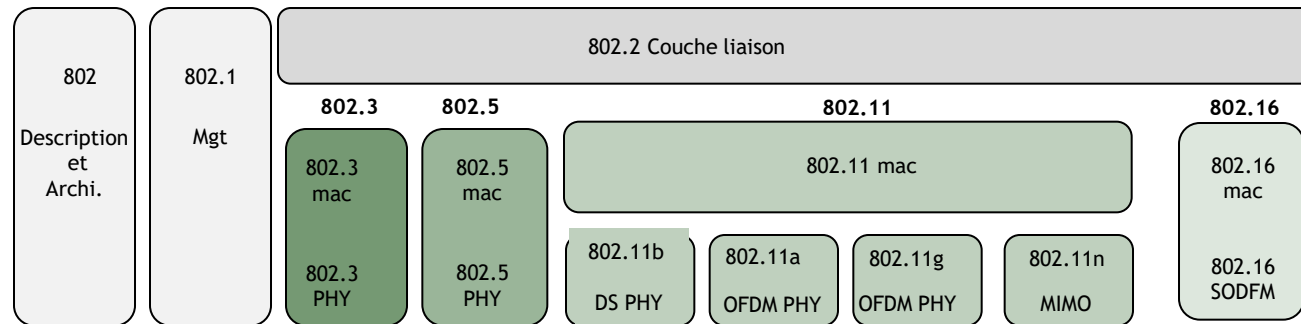
Réseaux locaux

Niveau 2
adresse mac liaison de données
trame ethernet 802.3
WiFi 802.11

22/05/2019

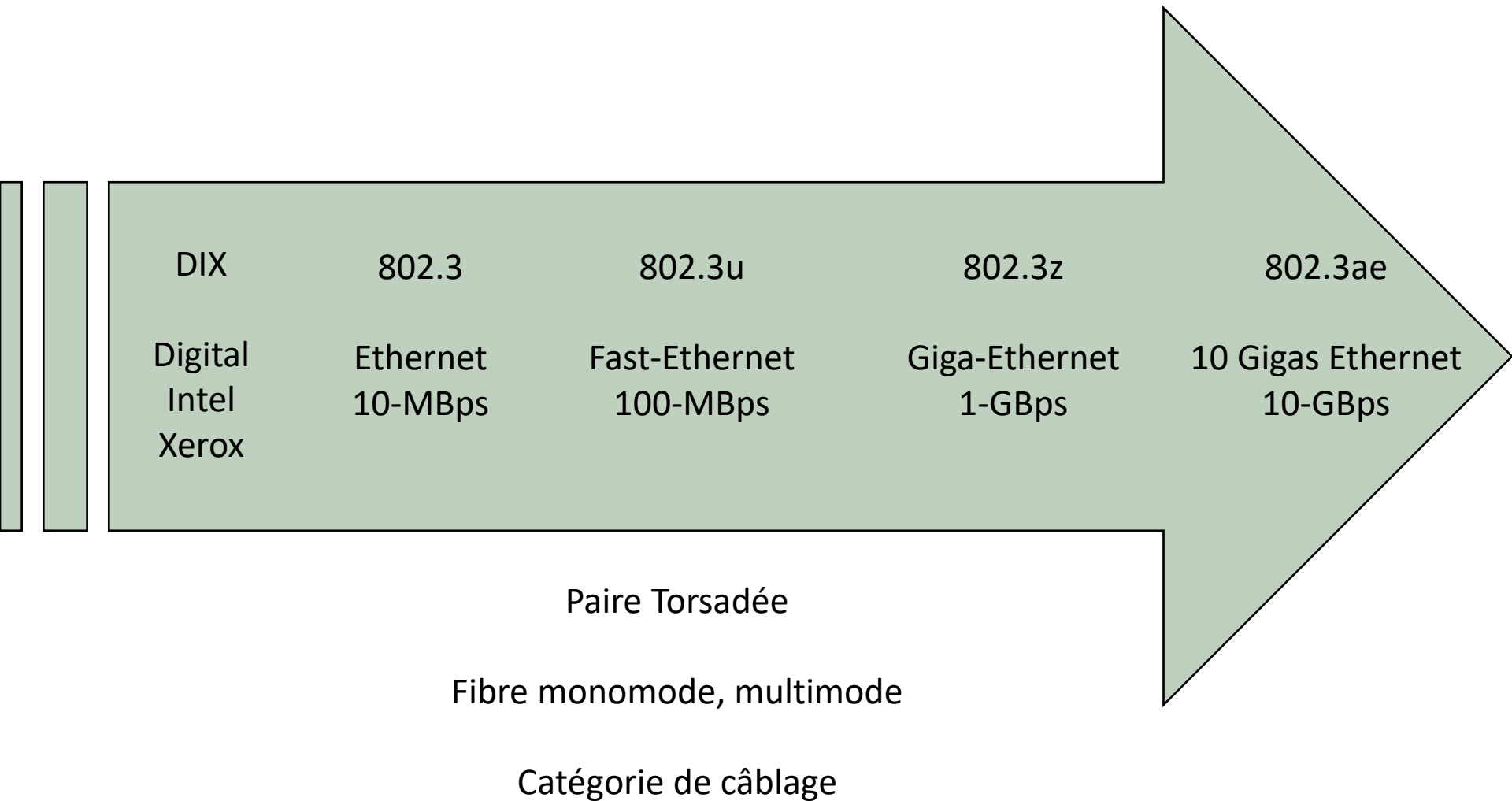
jp Grégoire/ Mac-IP

La famille des réseaux 802

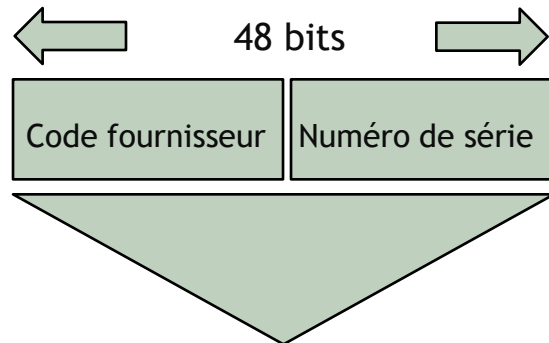


- Les spécifications IEEE 802 s'intéressent aux deux couches les plus basses du modèle OSI, elles incorporent des composants physiques et de liaison de données.
- Le MAC définit les règles d'accès au médium et d'envoi de données, la transmission ou la réception elle-même est gérée par la couche PHY.
- 802.2 décrit une couche liaison commune
- Les règles de gestion sont décrites dans la partie 802.1
Par exemple 802.1x pour la sécurité, 802.1Q pour les vlans, et 802.1D STP

Ethernet



Adresse Mac



Exemple:
00:11:95:91:86:dc
D-Link_91:86:dc

- Une longueur fixe de 48 bits, permettant d'attribuer un identificateur unique au moment de la fabrication de la carte réseau
- On dit parfois des adresses MAC qu'elles sont rémanentes (BIA - *burned-in addresses*) parce qu'elles demeurent en mémoire morte (ROM) et sont copiées en mémoire vive (RAM) lors de l'initialisation de la carte réseau

Un peu plus loin

- Unicast
Une interface une adresse
- Multicast
Une adresse un ensemble de machines
- Broadcast
Une adresse toutes les machines du réseau

Utilisée pour émettre des informations vers toutes les stations actives du réseau.

Exemple adresse mac

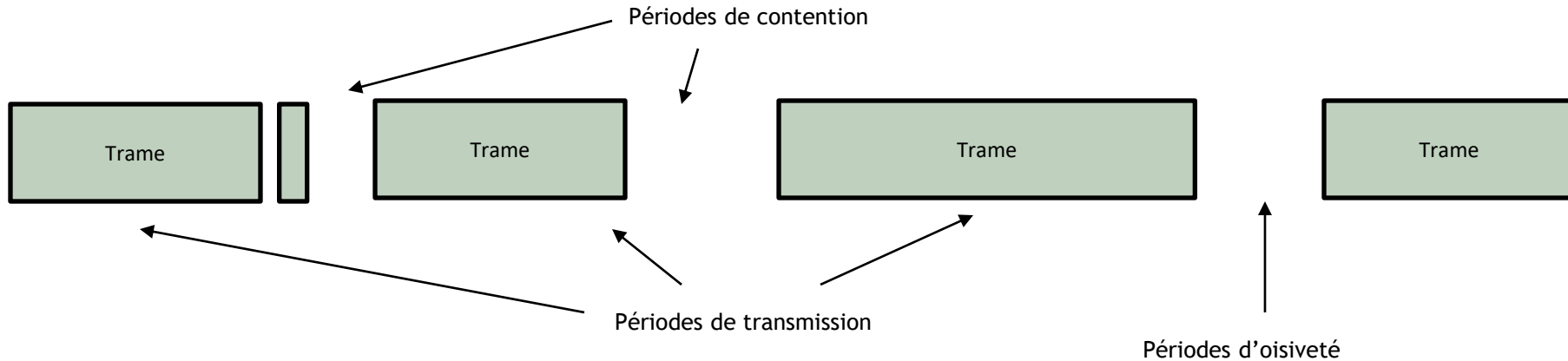
Carte Ethernet ethernet:

```
Statut du média . . . . . : Média déconnecté
Description . . . . . : Intel(R) PRO/100 VE Network Connection
Adresse physique . . . . . : 00-0D-60-CC-CF-33
```

Carte Ethernet wifi:

```
Statut du média . . . . . : Média déconnecté
Description . . . . . : Cisco Systems PCI Wireless LAN Adapter
Adresse physique . . . . . : 00-0E-9B-85-A5-B2
```

L'accès au média - Process



- CSMA (Carrier Sense Multiple Access),
Ecoute si libre émission
- Si deux émettent en même temps collision d'où CSMA/CD (collision detection)
Détection de collision: la station écoute la ligne indépendamment de ce qu'elle transmet. Si il y a identité: pas de problème.
Si ce n'est pas la même chose => il y a eu une collision avec une trame transmise par une autre station.
- Bien entendu il faudra réémettre les trames détruites avec un algorithme d'attente (Backoff: Binary exponential backoff)

Structure d'une trame



- Adresse mac destination et adresse mac source
- Longueur des données comprises entre 46 et 1500 octets => taille totale de trame de 64 à 1518 octets (hors flag et amorce) ou EtherType (au delà de 1500 octets)
- FCS (Frame Control Sequence)
CRC contrôle de redondance cyclique (polynôme générateur de degré 32)
- **CRC-32 (Ethernet)** : $= X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$

Trame CaptureEthernet.cap

TrameADecoderTP142143.cap
Trame 50

IP

Best effort

couche 3

adresse

paquet

ARP

ICMP

host

masque

Sous-réseaux

routeur

routage

adresse privée/publique

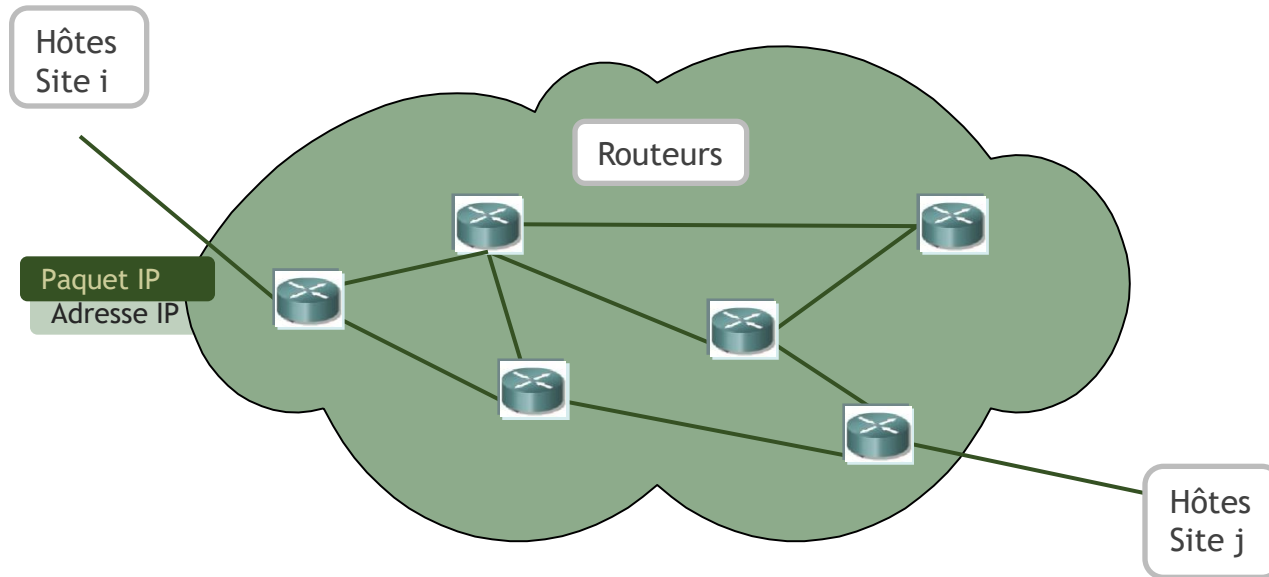
OSPF

RIP

22/05/2019

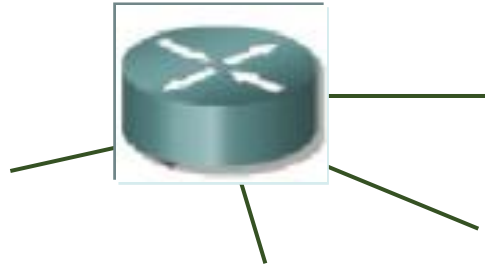
jp Grégoire/ Mac-IP

Introduction

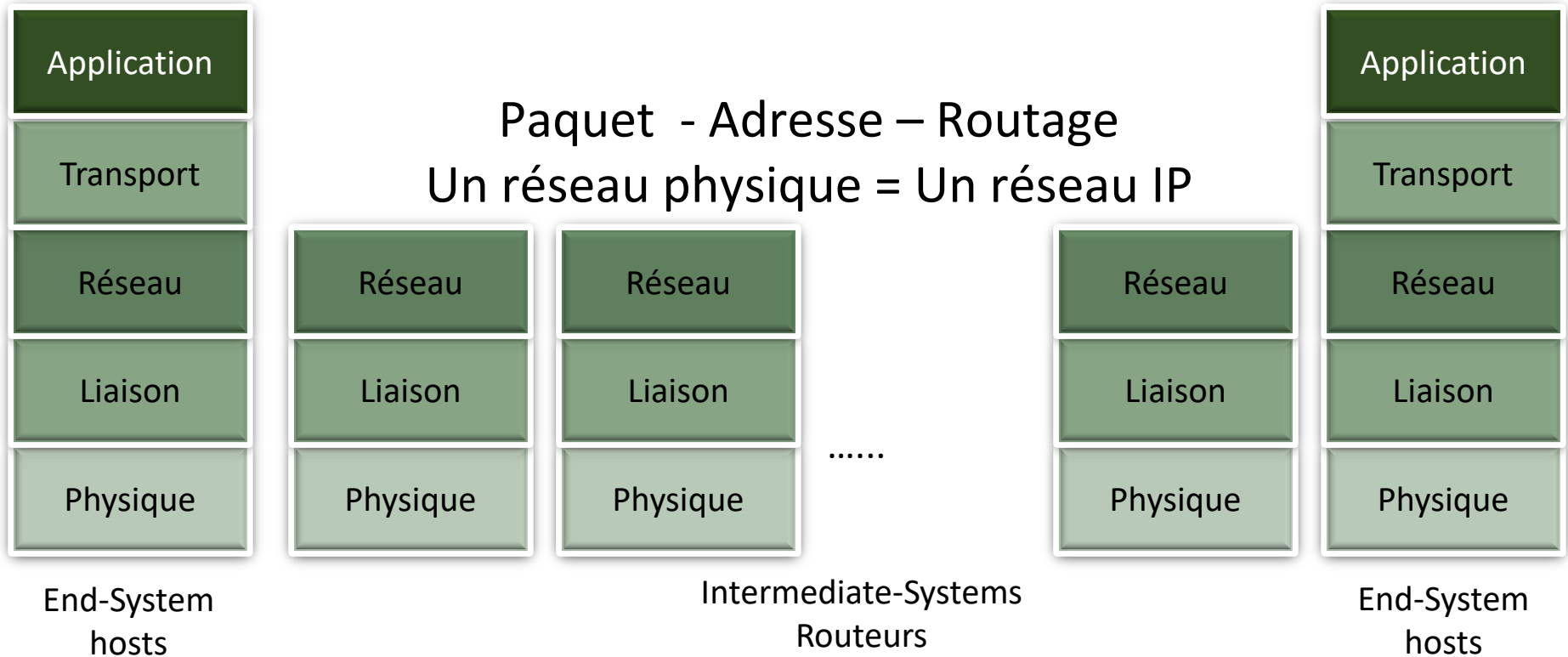


- IP est un protocole assurant la transmission de paquets sur des chemins indépendants sans connexion (sans contrôle de flux).
- Le service est non fiable et sans garantie: des paquets peuvent être perdus, dupliqués, retardés ou remis dans le désordre. La fiabilisation du transfert de même que la gestion de la connexion sont à la charge de la couche transport.
- Depuis le milieu des années 80, on utilise la version 4 du protocole IP.
- Depuis le milieu des années 90, la version IPv6, presque pas utilisée

IP



Paquet - Adresse – Routage
Un réseau physique = Un réseau IP



Le Paquet IP

32 Bits / 4 octets			
N° Version	Longueur entete	Type de service	Longueur totale du datagramme
Identificateur (Recopiée dans chaque segment)			Drapeaux + place du segment
Durée de vie		Protocole couche 4	Checksum Entete
Adresse IP Source			
Adresse IP Destination			
Options			
Données			

Binaire / Décimal

Conversion binaire décimal

Puissance de 2 de la position	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valeur décimale de la position	128	64	32	16	8	4	2	1
Exemple de calcul								
Valeur binaire	1	0	1	0	1	0	1	0
Valeur décimale	128	0	32	0	8	0	2	0
Valeur décimale de l'octet	170							

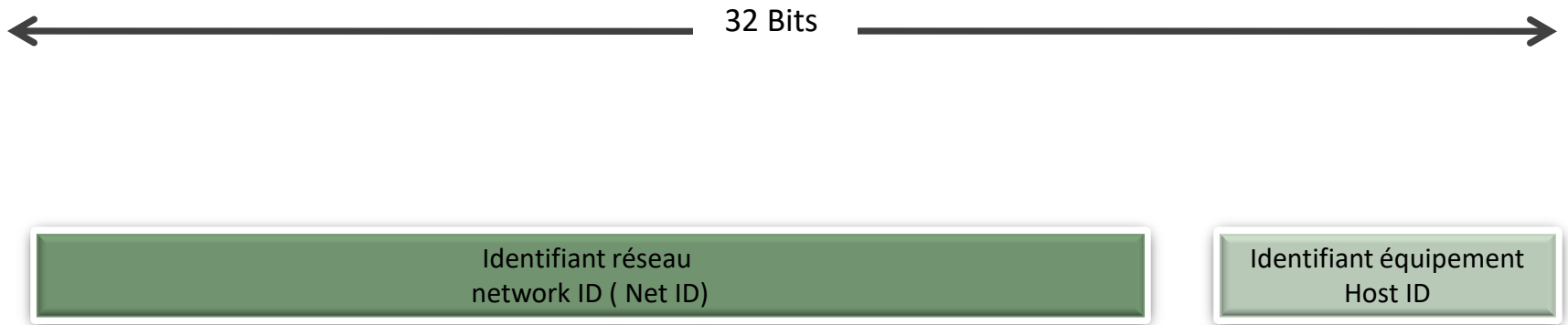
OCTET

Binaire/Décimal/Hexadécimal

0 0 0 0	0	0
0 0 0 1	1	1
0 0 1 0	2	2
0 0 1 1	3	3
0 1 0 0	4	4
0 1 0 1	5	5
0 1 1 0	6	6
0 1 1 1	7	7
1 0 0 0	8	8
1 0 0 1	9	9
1 0 1 0	10	A
1 0 1 1	11	B
1 1 0 0	12	C
1 1 0 1	13	D
1 1 1 0	14	E
1 1 1 1	15	F

0	0 0 0 0	0 0 0 0	0 0
1	0 0 0 0	0 0 0 1	0 1
2	0 0 0 0	0 0 1 0	0 2
3	0 0 0 0	0 0 1 1	0 3
4	0 0 0 0	0 1 0 0	0 4
5	0 0 0 0	0 1 0 1	0 5
6	0 0 0 0	0 1 1 0	0 6
7	0 0 0 0	0 1 1 1	0 7
8	0 0 0 0	1 0 0 0	0 8
10	0 0 0 0	1 0 1 0	0 A
15	0 0 0 0	1 1 1 1	0 F
16	0 0 0 1	0 0 0 0	1 0
32	0 0 1 0	0 0 0 0	2 0
64	0 1 0 0	0 0 0 0	4 0
128	1 0 0 0	0 0 0 0	8 0
192	1 1 0 0	0 0 0 0	C 0
202	1 1 0 0	1 0 1 0	C A
240	1 1 1 1	0 0 0 0	F 0
241	1 1 1 1	0 0 0 1	F 1
255	1 1 1 1	1 1 1 1	F F

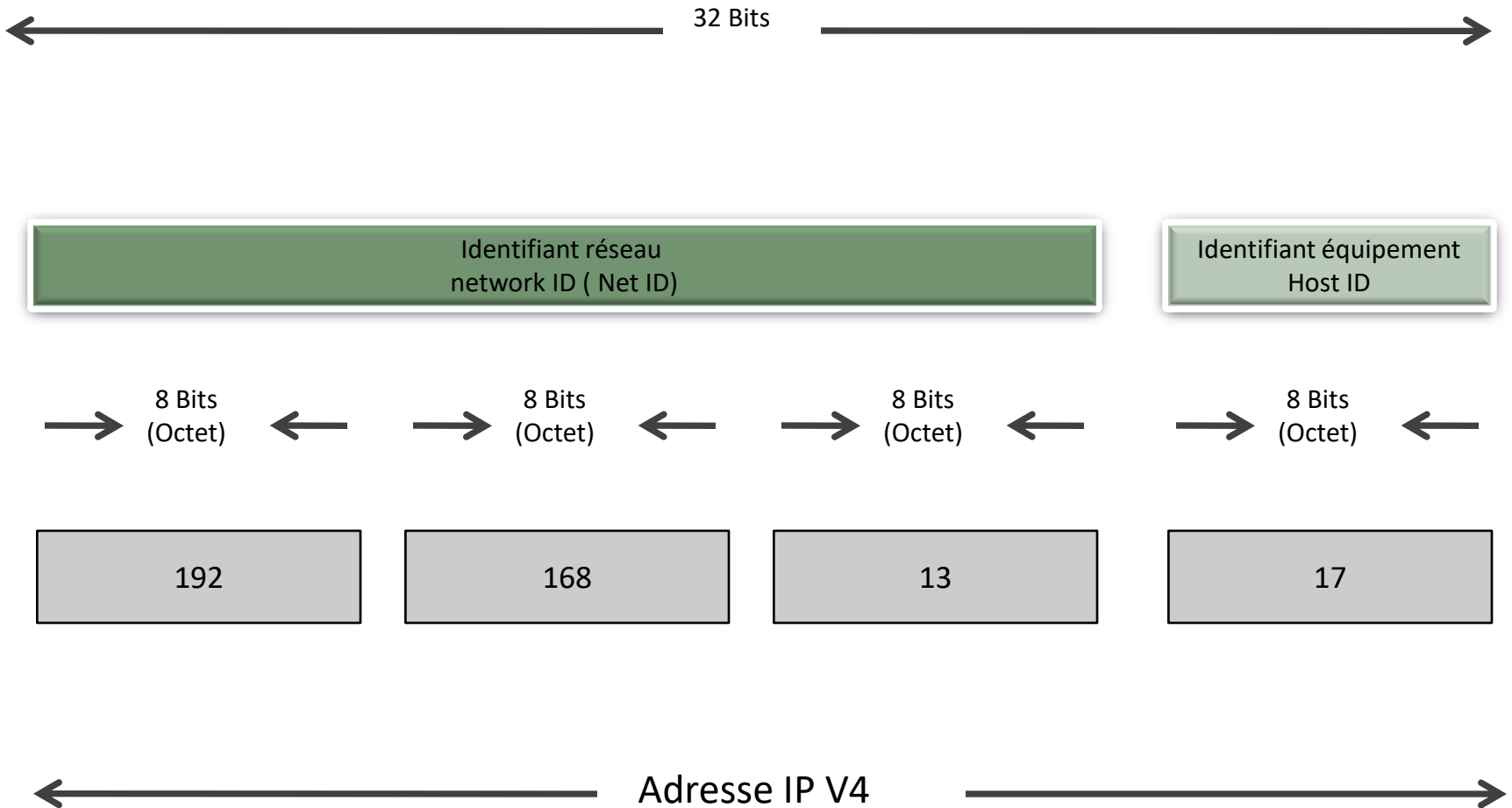
Format des adresses Internet



L'adresse Internet (adresse IP) d'un équipement, codée sur 4 octets, contient à la fois un identifiant du réseau et identifiant de l'équipement connecté au réseau.

L'identifiant réseau" peut être codé sur 1, 2 ou 3 octets, ce qui correspond à trois grandes catégories de réseaux: A, B et C.

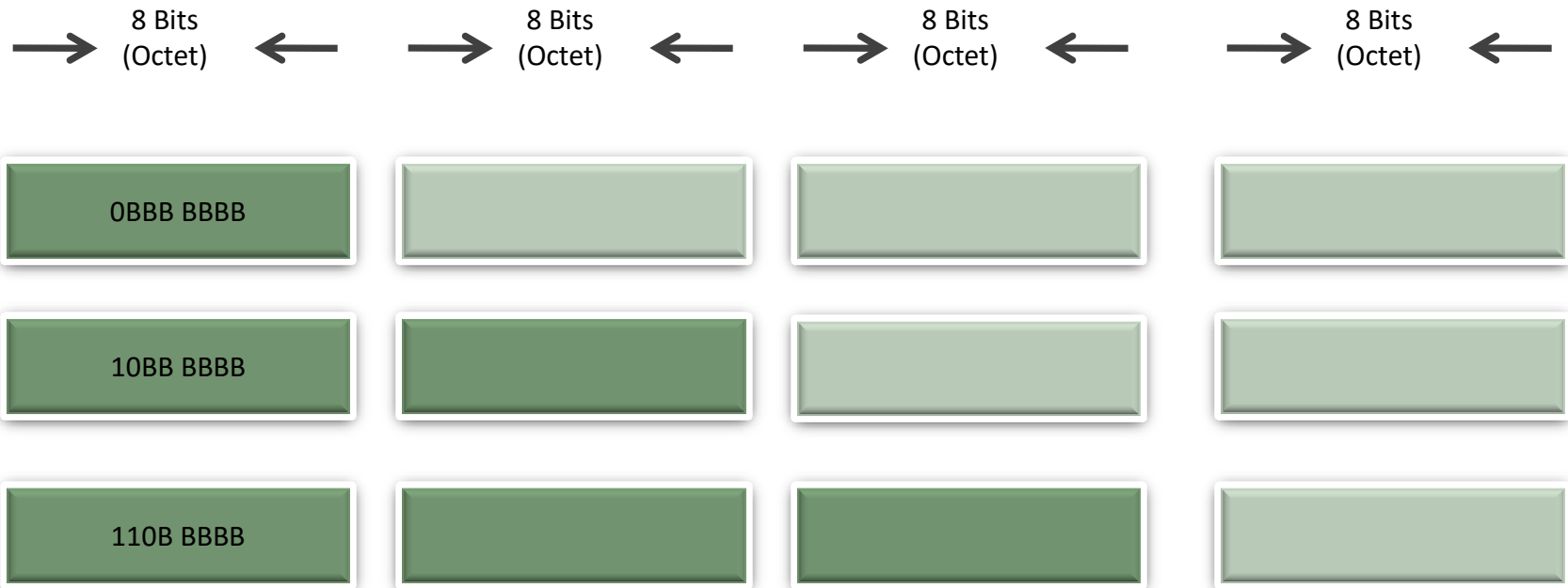
Composant adresse IP



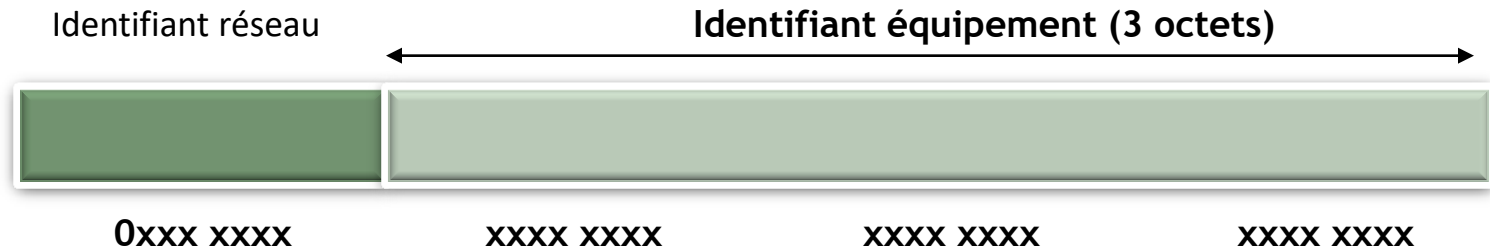
Format des adresses Internet

L'identifiant réseau peut être codé sur 1, 2 ou 3 octets, ce qui correspond à trois grandes catégories de réseaux: A, B et C.

Les trois bits de poids fort du premier octet déterminent la classe de l'adresse et définissent ainsi implicitement le nombre d'octets utilisés pour le codage de l'identifiant du réseau



Adresse classe A



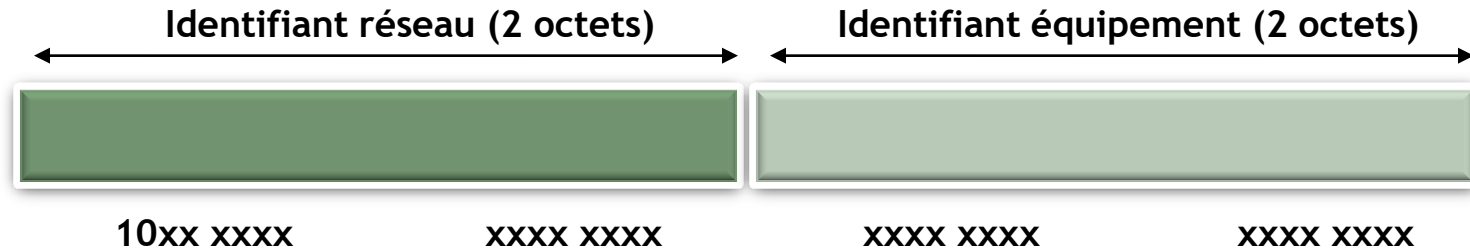
7 bits pour l'ID Réseau - 24 bits pour l'ID Equipement

La plage d'adresses utilisable est la suivante: de 1.0.0.1 à 126.255.255.254

La classe A permet donc de coder 126 très grands réseaux.

Pour chacun $2^{24} - 2$ c'est-à-dire 16 777 214 équipements.

Adresse classe B



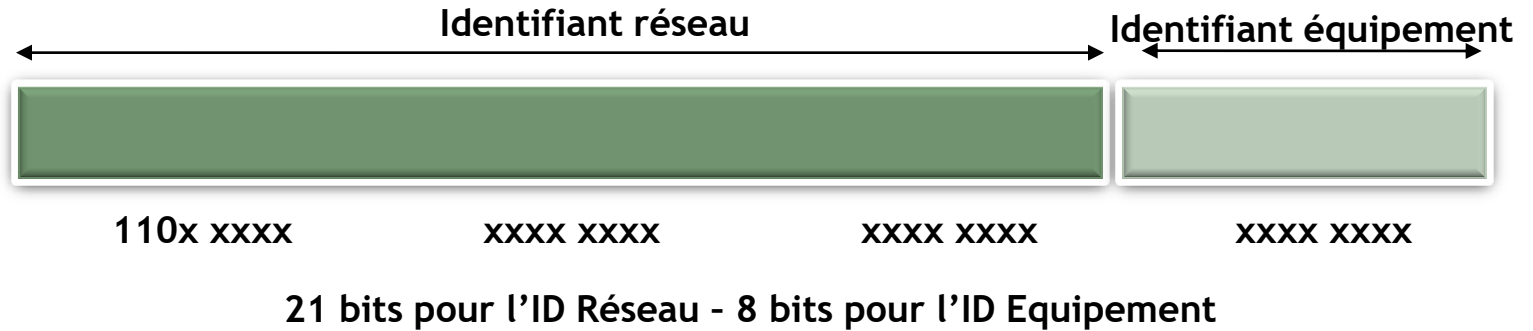
14 bits pour l'ID Réseau - 16 bits pour l'ID Equipement

La plage d'adresses utilisable est la suivante: de **128.0.0.1** à **191.255.255.254**

La classe B permet donc de coder 16384 grands réseaux
Pour chacun $2^{16} - 2$ c'est-à-dire 65534 équipements.

Exemple: 134.157.0.0 (Jussieu).

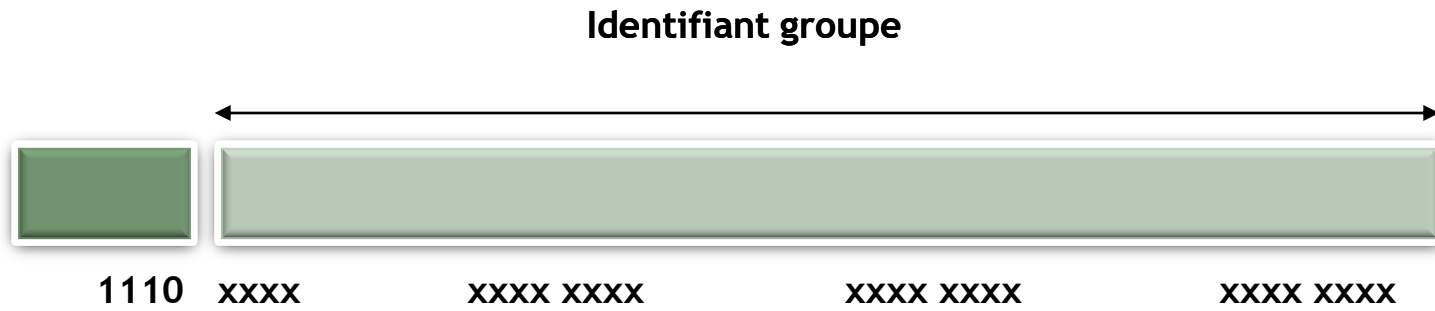
Adresse classe C



La plage d'adresses utilisables est la suivante: de **192.0.0.1** à **223.255.255.254**

La classe C permet donc de coder 8 millions de petits réseaux comprenant moins de 254 équipements

Adresse classe D



28 bits pour l'ID groupe

La classe D permet donc de coder des adresses de groupes regroupement plusieurs équipements (ce qui correspond à une adresse multicast).

Exemples:

224.0.0.9 pour RIP, 239.255.255.250 pour UpNp, 239.192.0.1 pour TF1 bouquet orange

En fait à partir de 240.0.0.0 on parle de classe E à ce jour pour des utilisations expérimentales.

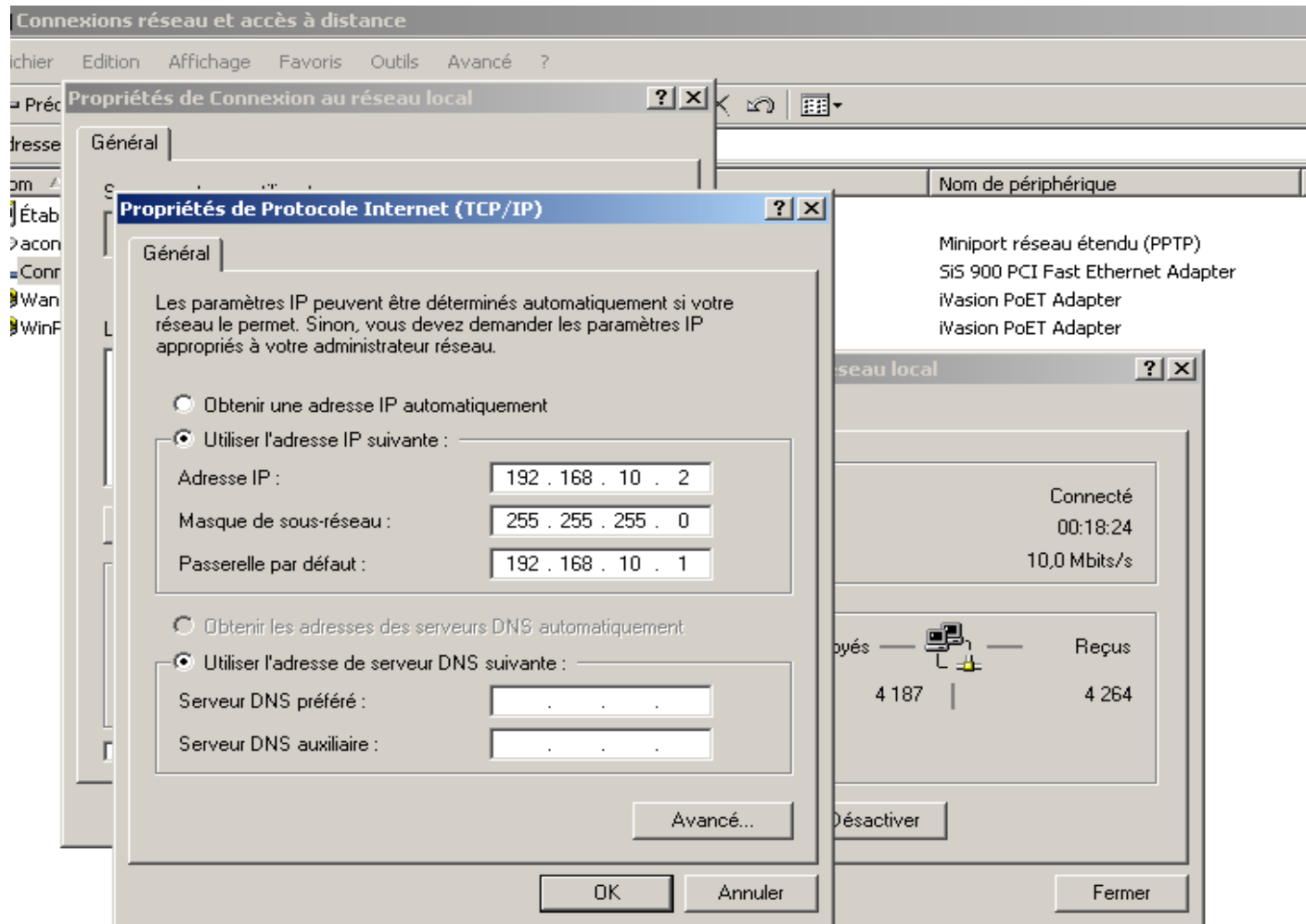
Les adresses

- Adresse réseau:
Lorsque tous les bits de l'ID-équipement sont à 0, l'adresse IP désigne le réseau.
Exemple: 130.90.0.0 désigne le réseau de classe B.
- Les adresses unicast identifiant un équipement de TCP/IP
une adresse réseau plus un identifiant
Exemple: 130.90.89.23
- Les adresses multicast identifient un groupe d'équipement TCP/IP
- Adresse de diffusion (broadcast):
Lorsque tous les bits de l'ID-équipement sont à 1, l'adresse IP indique une diffusion sur le réseau d'adresse ID-réseau
Exemple: 130.90.255.255
- Test en local:
L'adresse 127.0.0.1 (en fait 127.x.x.x) est une adresse IP de test des communications en local (sans sortir de la machine) dite loopback localhost.
- Adresse inconnue:
L'adresse 0.0.0.0 est réservée au cas de résolution d'adresse par le protocole RARP lorsque la machine ne connaît pas sa propre adresse IP et la route par défaut

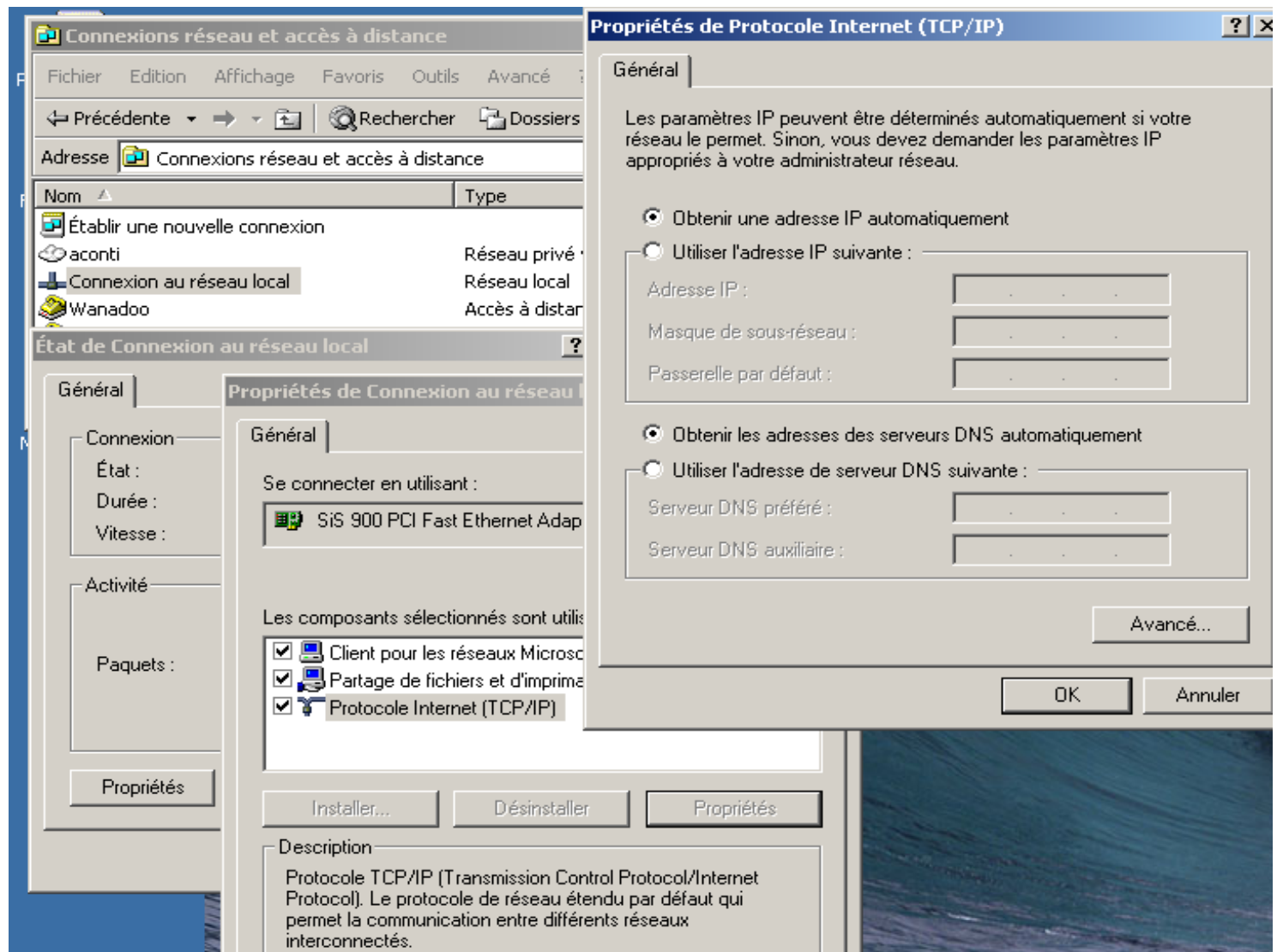
Unicité, privées, publiques

- **L'adresse IP d'un réseau doit être unique à partir du moment où le réseau est connecté à Internet.**
- Les adresses IP d'internet sont attribuées par l'**I.A.N.A** (Internet Assigned Numbers Authority).
- La croissance d'internet entraînant le manque d'adresse IP a nécessité l'introduction de la notion d'adresses publiques et privées
- Les adresses privées sont utilisées en interne par les entreprises et ne sont pas connues de l'internet Public, une passerelle/routeur se trouve à la liaison entreprise/ISP pour résoudre cette problématique
- Les plages d'adresses privées:
 - de 10.0.0.0 à 10.255.255.255 pour la classe A
 - de 172.16.0.0 à 172.31.255.255 pour la classe B
 - de 192.168.0.0 à 192.168.255.255 pour la classe C

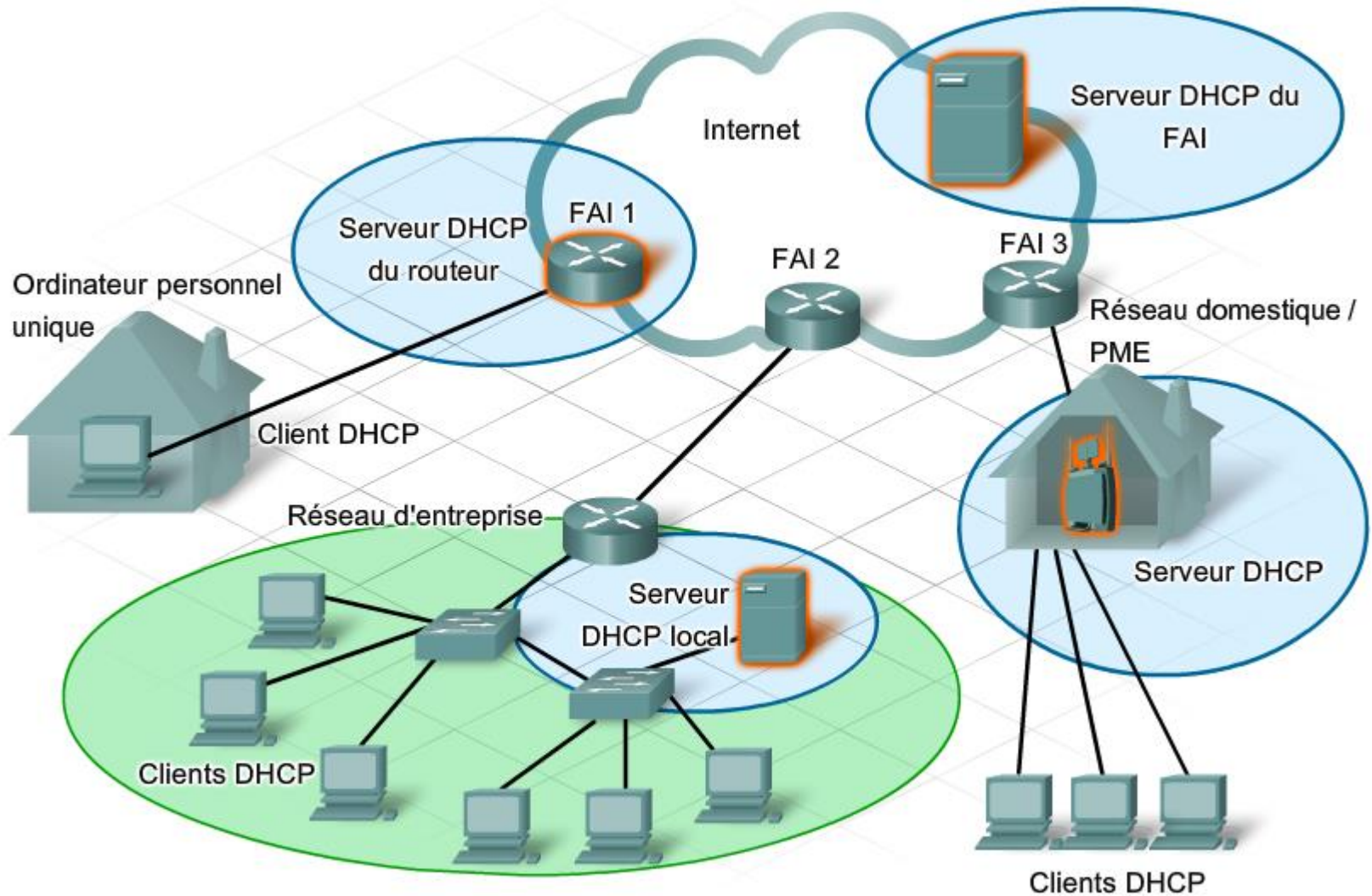
Configuration windows



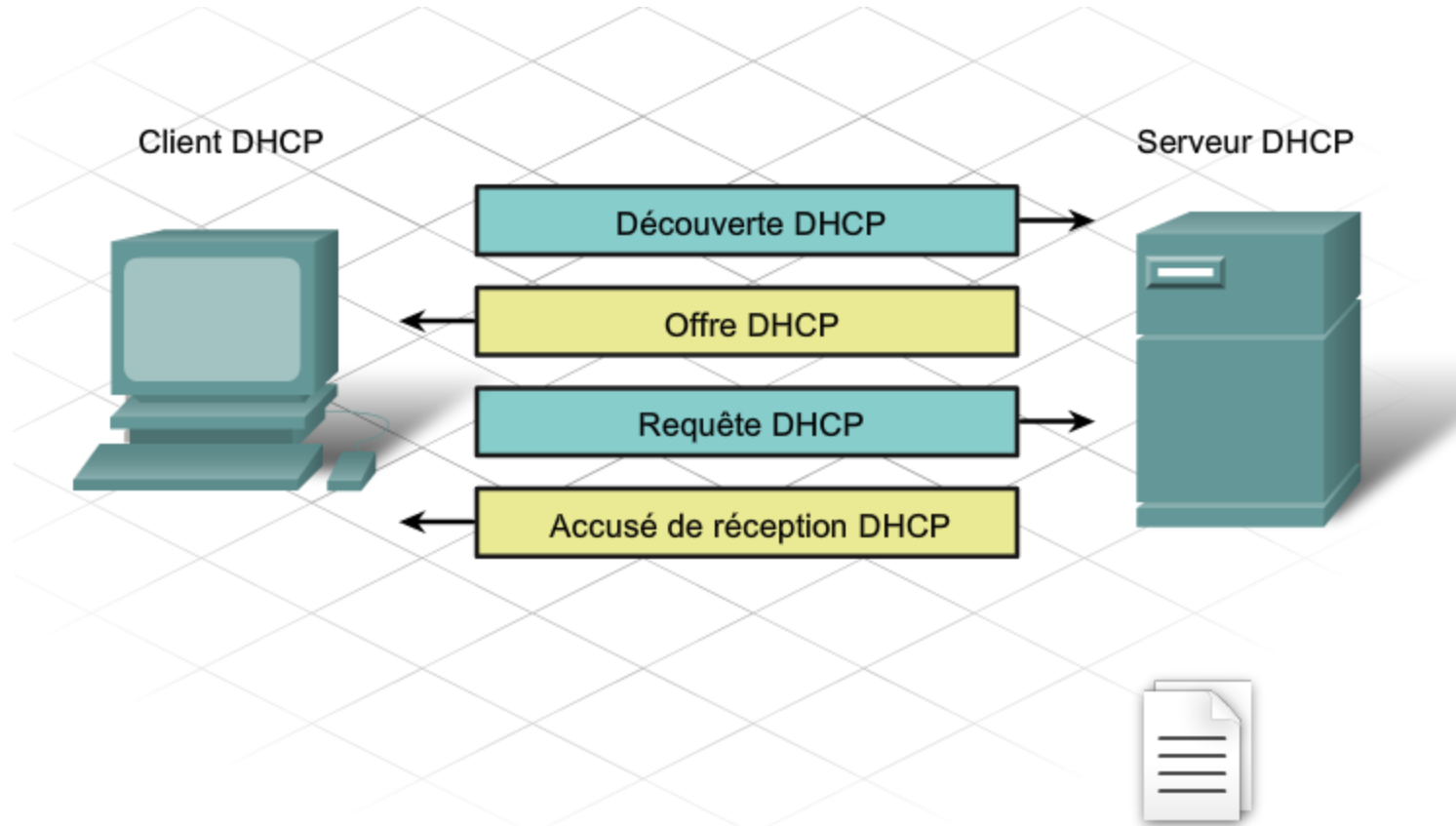
Configuration windows



Dhcp



Dhcp



Dhcp

Automatic Configuration - DHCP

Host Name:

Domain Name:

MTU: Size:

IP Address: . . .

Subnet Mask:

DHCP Server: ☒ Enabled ☐ Disabled DHCP Reservation

Start IP Address: 192 . 168 . 1 .

Maximum Number of Users:

IP Address Range: 192.168.1.100 ~ 149

Client Lease Time: minutes (0 means one day)

Static DNS 1: . . .

Static DNS 2: . . .

Static DNS 3: . . .

WINS: . . .

Cisco conf une interface

Configuration fast ethernet

```
R2(config)#interf fa0/0
```

```
R2(config-if)#ip address 10.2.1.1 255.255.255.0
```

```
R2(config-if)#interf fa0/1
```

```
R2(config-if)#ip address 10.2.2.1 255.255.255.0
```

Configuration ligne série

```
R2(config-if)#interf s0/0/0
```

```
R2(config-if)#ip add 192.168.10.1 255.255.255.0
```

```
R2(config-if)#clock rate 2000000
```

```
R2(config-if)#no shut
```

Visualisation

```
#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.2.1.1	YES	manual	up	up
FastEthernet0/1	10.2.2.1	YES	manual	up	up
FastEthernet0/1/0	unassigned	YES	unset	up	down
FastEthernet0/1/1	unassigned	YES	unset	up	down
FastEthernet0/1/2	unassigned	YES	unset	up	down
FastEthernet0/1/3	unassigned	YES	unset	up	down
Serial0/0/0	192.168.1.1	YES	manual	up	up
Serial0/0/1	192.168.10.1	YES	manual	up	up
Vlan1	unassigned	YES	unset	up	down

Cisco

```
Router>ena
Router#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0090.2165.3d94 (bia 0090.2165.3d94)
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    956 packets input, 193351 bytes, 0 no buffer
    Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    2357 packets output, 263570 bytes, 0 underruns
    0 output errors, 0 collisions, 10 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

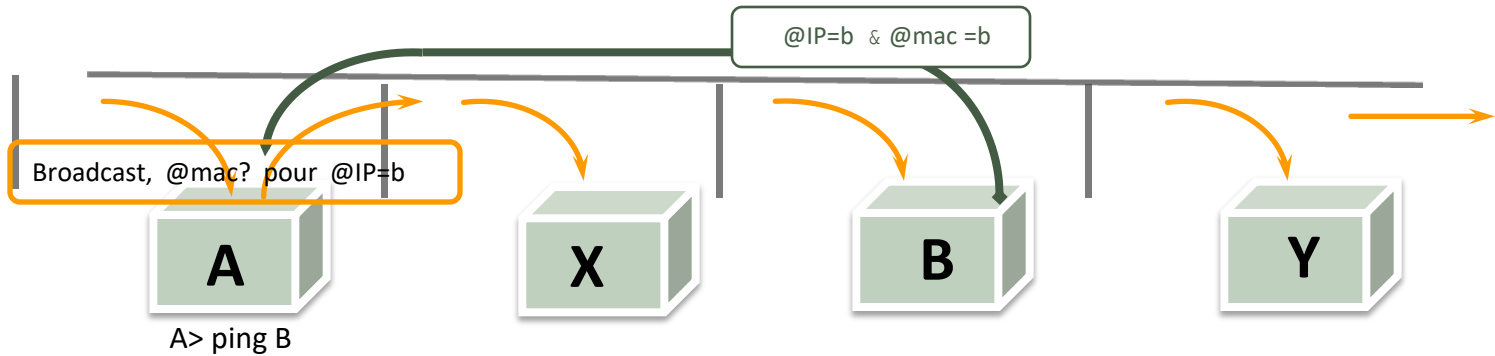
Etude trame (CaptureIP.cap)

Voir TrameADecoderTP142143 n° 50

Mapping adresse MAC, adresse IP

- Considérons la transmission d'un datagramme IP sur un réseau Ethernet: le datagramme est encapsulé dans une trame Ethernet.
- Toute trame Ethernet code l'adresse Ethernet de l'émetteur et l'adresse Ethernet du destinataire (adresse physique du coupleur codée sur 48 bits fixés à la fabrication par le constructeur du coupleur) et **il n'y a pas de correspondance directe entre l'adresse IP d'une station et son adresse MAC** (pas de loi mathématique pour trouver l'adresse MAC à partir de l'adresse IP)
- Nécessité de gérer (en local sur chaque station) une table de correspondance des adresses MAC/IP, appelé table ARP.
La gestion et la mise à jour de cette table est dynamique
- ARP: Address Resolution Protocol
L'utilisation du protocole ARP (Address Resolution Protocol) apporte une solution à cette nécessité de résolution dynamique d'adresse.

Le process ARP

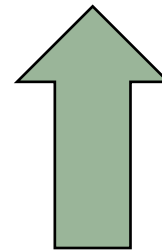
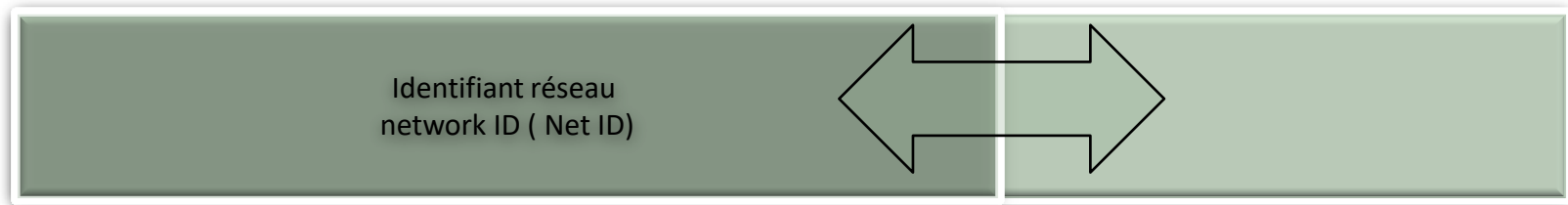


1. La couche IP élabore le paquet ICMP pour B
2. La couche IP détermine que B est sur le même réseau IP, donc même réseau physique.
3. Passe la main à la couche liaison



La notion de masque

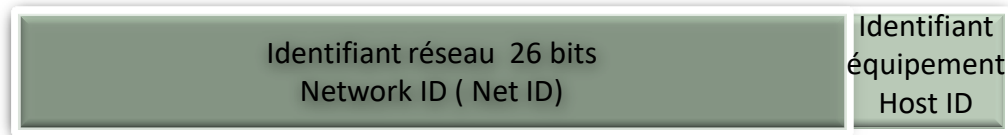
- Début 90 manque d'adresse réseau. Pour palier mise en place de la technique du sous-adressage
- L'identifiant réseau n'est plus fixe en fonction des premiers bits mais variable en fonction d'un masque (vlsm: Variable Length Subnet Masking)
- Permet de définir plusieurs adresses de réseau à partir d'une adresse réseau de classe donnée.



	0	1
0	0	0
1	0	1

Variable en fonction du besoin
/nb de bit du Net ID
Masque

Exemple 1



192 . 168 . 10 . 65

Valeur binaire

1100 0000 . 1010 1000 . 0000 1010 . 0100 0001

Masque

1111 1111 . 1111 1111 . 1111 1111 . 1100 0000

Après application
masque

1100 0000 . 1010 1000 . 0000 1010 . 0100 0000

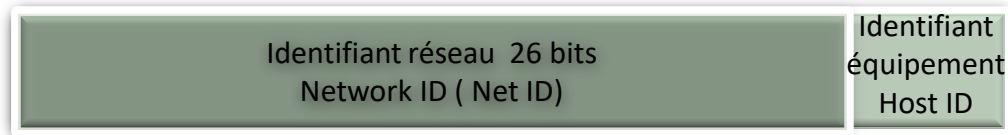
192 . 168 . 10 . 64

Masque

1111 1111 . 1111 1111 . 1111 1111 . 1100 0000

255 . 255 . 255 . 192

Exemple 2



Valeur binaire

192	.	168	.	10	.	190
1100 0000	.	1010 1000	.	0000 1010	.	1011 1110

Masque

1111 1111	.	1111 1111	.	1111 1111	.	1100 0000
-----------	---	-----------	---	-----------	---	-----------

Après application masque

1100 0000	.	1010 1000	.	0000 1010	.	1000 0000
-----------	---	-----------	---	-----------	---	-----------

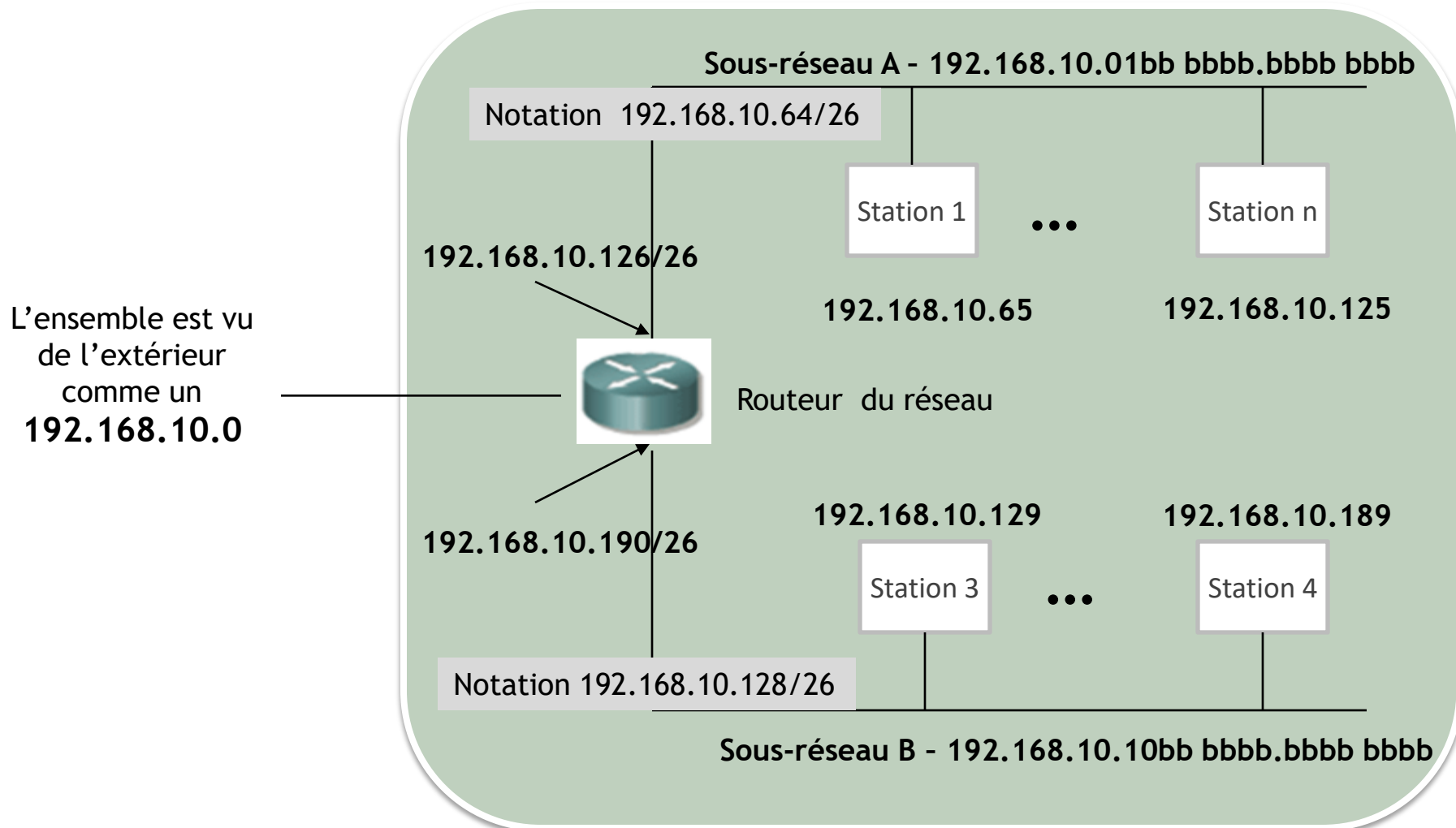
192	.	168	.	10	.	128
-----	---	-----	---	----	---	-----

Masque

1111 1111	.	1111 1111	.	1111 1111	.	1100 0000
-----------	---	-----------	---	-----------	---	-----------

255	.	255	.	255	.	192
-----	---	-----	---	-----	---	-----

Exemple



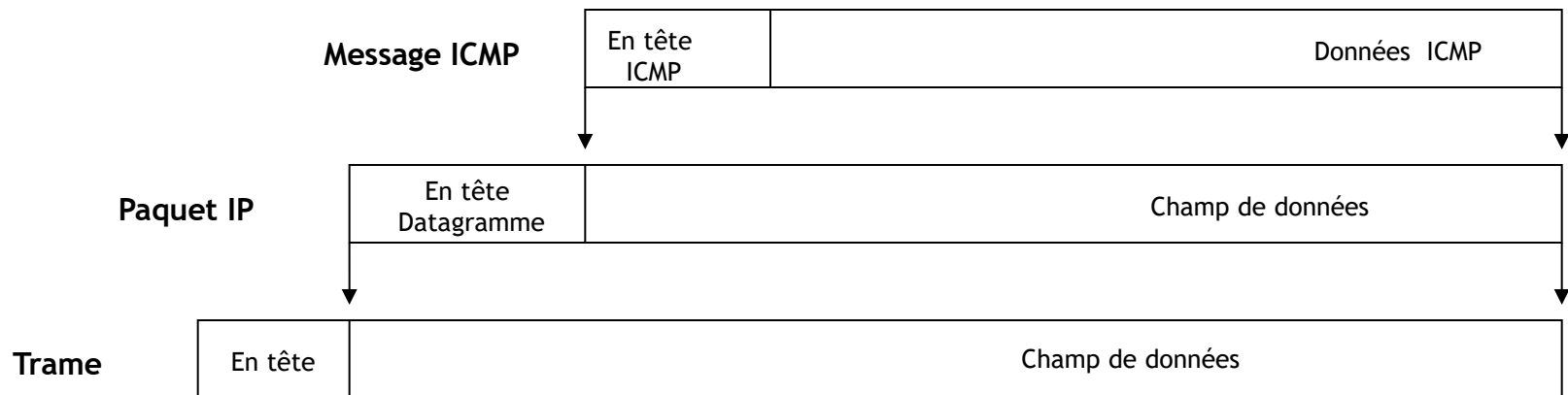
ICMP

Internet Control Message Protocol

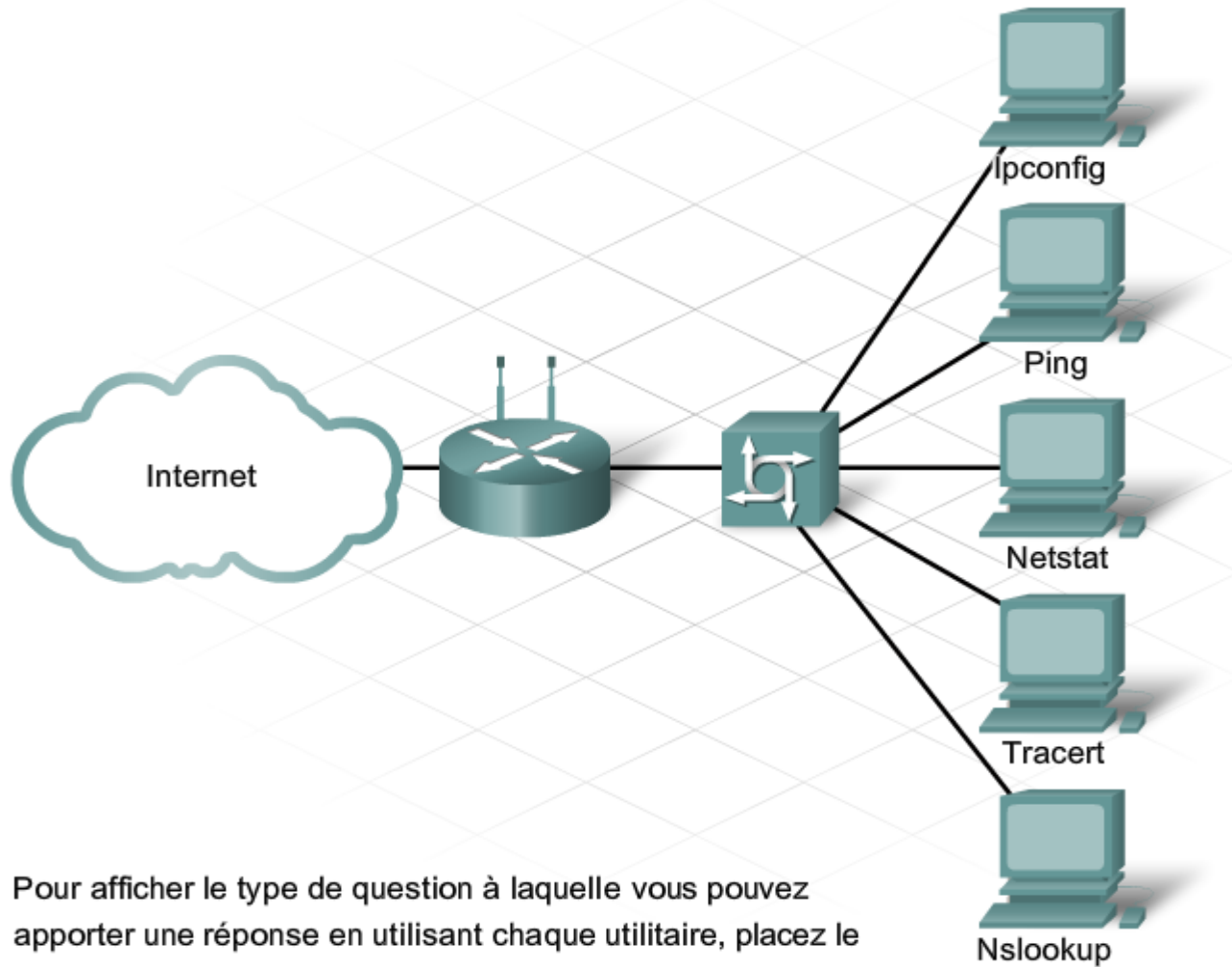
Principes

- Le protocole IP n'étant pas, dans sa définition, absolument fiable, le but de la mise en place du protocole ICMP (Internet Control Message Protocol) est de pouvoir transmettre des messages de contrôle pour signaler l'apparition de cas d'erreur dans l'environnement IP (exemple: lorsqu'un datagramme ne peut pas atteindre sa destination, lorsque le routeur manque de réserve de mémoire pour retransmettre correctement le datagramme,...)
- Le but de ICMP n'est pas de rendre IP fiable
- Le message ICMP est encapsulé dans un datagramme IP à destination de l'émetteur du datagramme d'origine.
- De même qu'il n'y a aucune garantie que le datagramme IP d'origine soit acheminé, il n'y a aucune garantie que le message de contrôle soit retourné

ICMP



Dépannage Connectivité



Pour afficher le type de question à laquelle vous pouvez apporter une réponse en utilisant chaque utilitaire, placez le pointeur de la souris sur chaque commande.

Ipconfig

```
C:\>ipconfig/all

Configuration IP de Windows

    Nom de l'hôte . . . . . : bobfre
    Suffixe DNS principal . . . . . :
    Type de noud . . . . . : Hybride
    Routage IP activ   . . . . . : Non
    Proxy WINS activ   . . . . . : Non

Carte Ethernet Connexion au r  seau local:

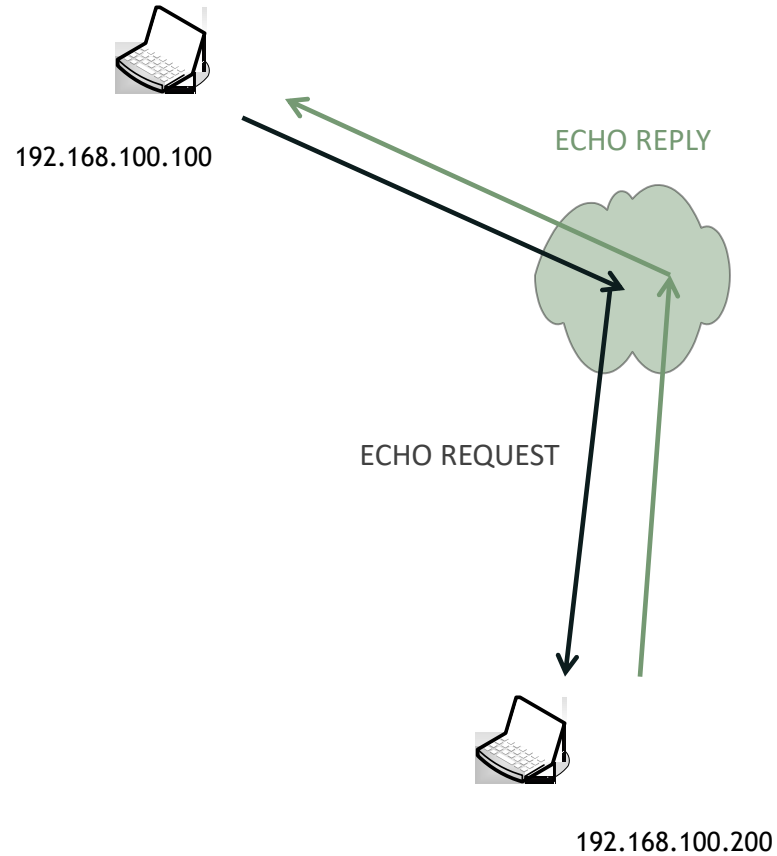
    Suffixe DNS propre    la connexion :
    Description . . . . . : Broadcom NetXtreme Gigabit Ethernet

    Adresse physique . . . . . : 00-0C-29-65-FD-80
    DHCP activ   . . . . . : Oui
    Configuration automatique activ  e : Oui
    Adresse IP. . . . . : 192.168.2.105
    Masque de sous-r  seau . . . . . : 255.255.255.0
    Passerelle par d  faut . . . . . : 192.168.2.1
    Serveur DHCP. . . . . : 192.168.2.1
    Serveurs DNS . . . . . : 68.230.197.234
                           67.69.184.139
    Serveur WINS principal. . . . . : 171.69.2.87
    Bail obtenu . . . . . : mardi 11 d  cembre 2007 16:36:50
    Bail expirant . . . . . : mercredi 19 d  cembre 2007 16:36:50

C:\>_
```

PING

```
C:>ping 192.168.100.200
```



Ping

```
C:\>ping 128.107.229.50
```

```
Envoi d'une requête 'ping' sur 128.107.229.50 avec 32 octets de données :
```

```
Réponse de 128.107.229.50 : octets=32 temps=160 ms TTL=102  
Réponse de 128.107.229.50 : octets=32 temps=161 ms TTL=102  
Réponse de 128.107.229.50 : octets=32 temps=159 ms TTL=102  
Réponse de 128.107.229.50 : octets=32 temps=160 ms TTL=102
```

```
Statistiques Ping pour 128.107.229.50:
```

```
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),  
Durée approximative des boucles en millisecondes :  
Minimum = 159ms, Maximum = 161ms, Moyenne = 160ms
```

```
C:\>ping cisco.netacad.net
```

```
Envoi d'une requête 'ping' sur cisco.netacad.net [128.107.229.50] avec 32 octets  
de données :
```

```
Réponse de 128.107.229.50 : octets=32 temps=160 ms TTL=102  
Réponse de 128.107.229.50 : octets=32 temps=161 ms TTL=102  
Réponse de 128.107.229.50 : octets=32 temps=160 ms TTL=102  
Réponse de 128.107.229.50 : octets=32 temps=159 ms TTL=102
```

```
Statistiques Ping pour 128.107.229.50:
```

```
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),  
Durée approximative des boucles en millisecondes :  
Minimum = 159ms, Maximum = 161ms, Moyenne = 160ms
```

```
C:\>_
```

PING

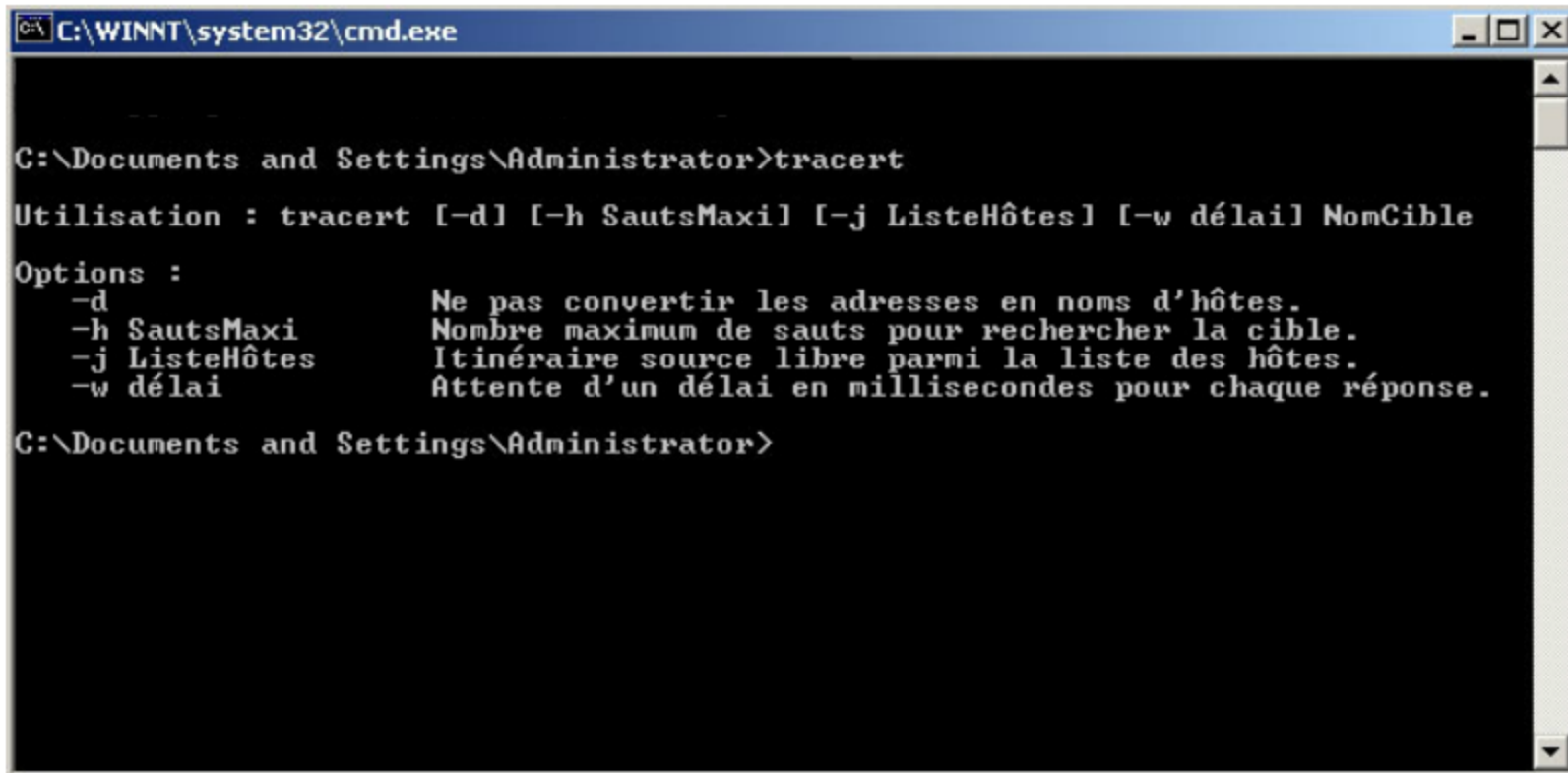
```
C:\>ping
```

```
Utilisation : ping [-t] [-a] [-n échos] [-l taille] [-f] [-i vie] [-v TypServ]
               [-r NbSauts] [-s NbSauts] [[-j ListeHôtes] : [-k ListeHôtes]]
               [-w Délai] NonCible
```

Options :

-t	Envoie la requête ping sur l'hôte spécifié jusqu'à interruption. Entrez Ctrl-Attn pour afficher les statistiques et continuer, Ctrl-C pour arrêter.
-a	Recherche les noms d'hôte à partir des adresses.
-n échos	Nombre de requêtes d'écho à envoyer.
-l taille	Envoie la taille du tampon.
-f	Active l'indicateur Ne pas fragmenter dans le paquet.
-i vie	Durée de vie.
-v TypServ	Type de service.
-r NbSauts	Enregistre l'itinéraire pour le nombre de sauts.
-s NbSauts	Dateur pour le nombre de sauts.
-j ListeHôtes	Itinéraire source libre parmi la liste d'hôtes.
-k ListeHôtes	Itinéraire source strict parmi la liste d'hôtes.
-w Délai	Délai d'attente pour chaque réponse, en millisecondes.

Traceroute/tracert



```
C:\WINNT\system32\cmd.exe

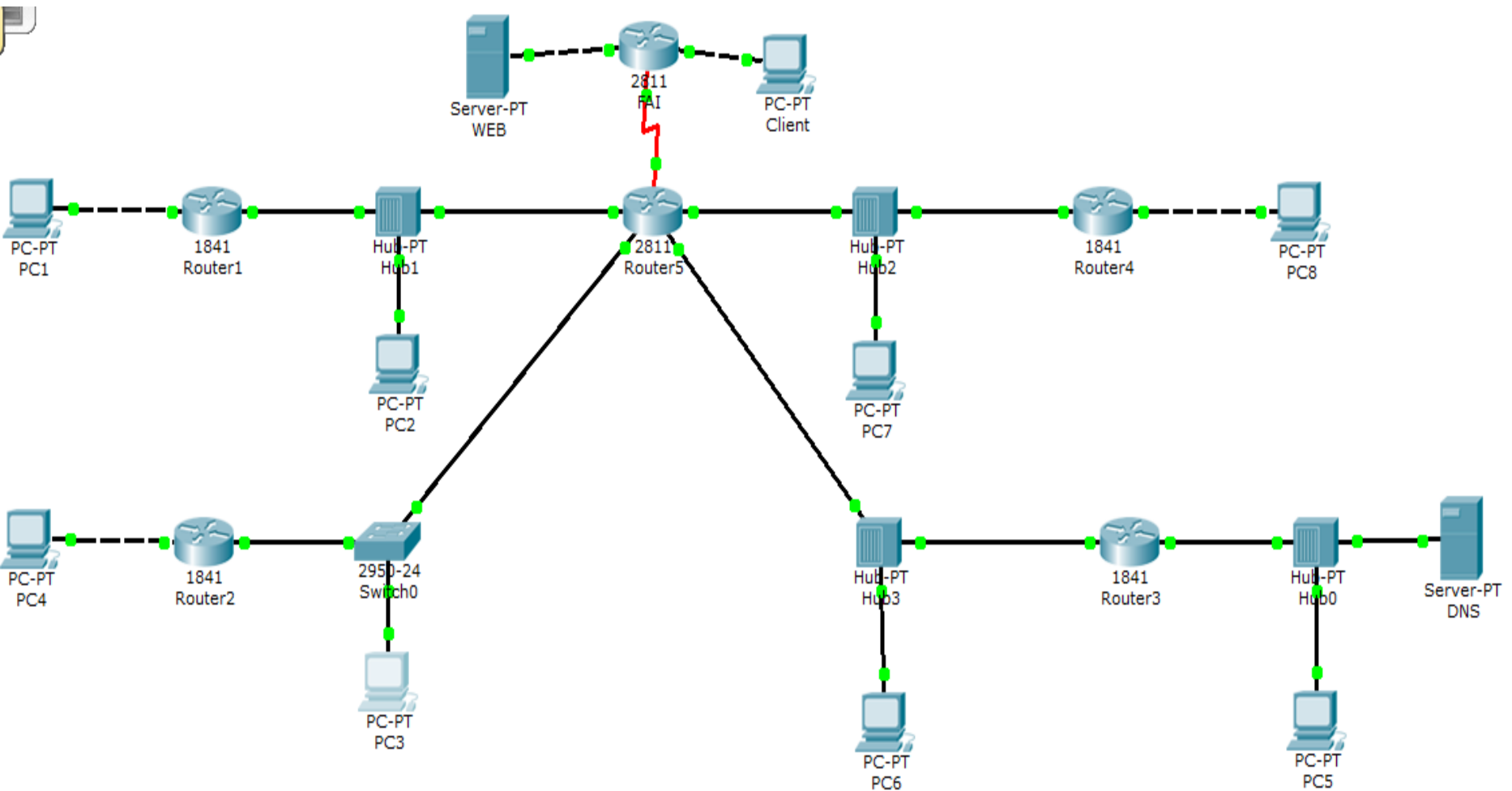
C:\Documents and Settings\Administrator>tracert

Utilisation : tracert [-d] [-h SautsMaxi] [-j ListeHôtes] [-w délai] NomCible

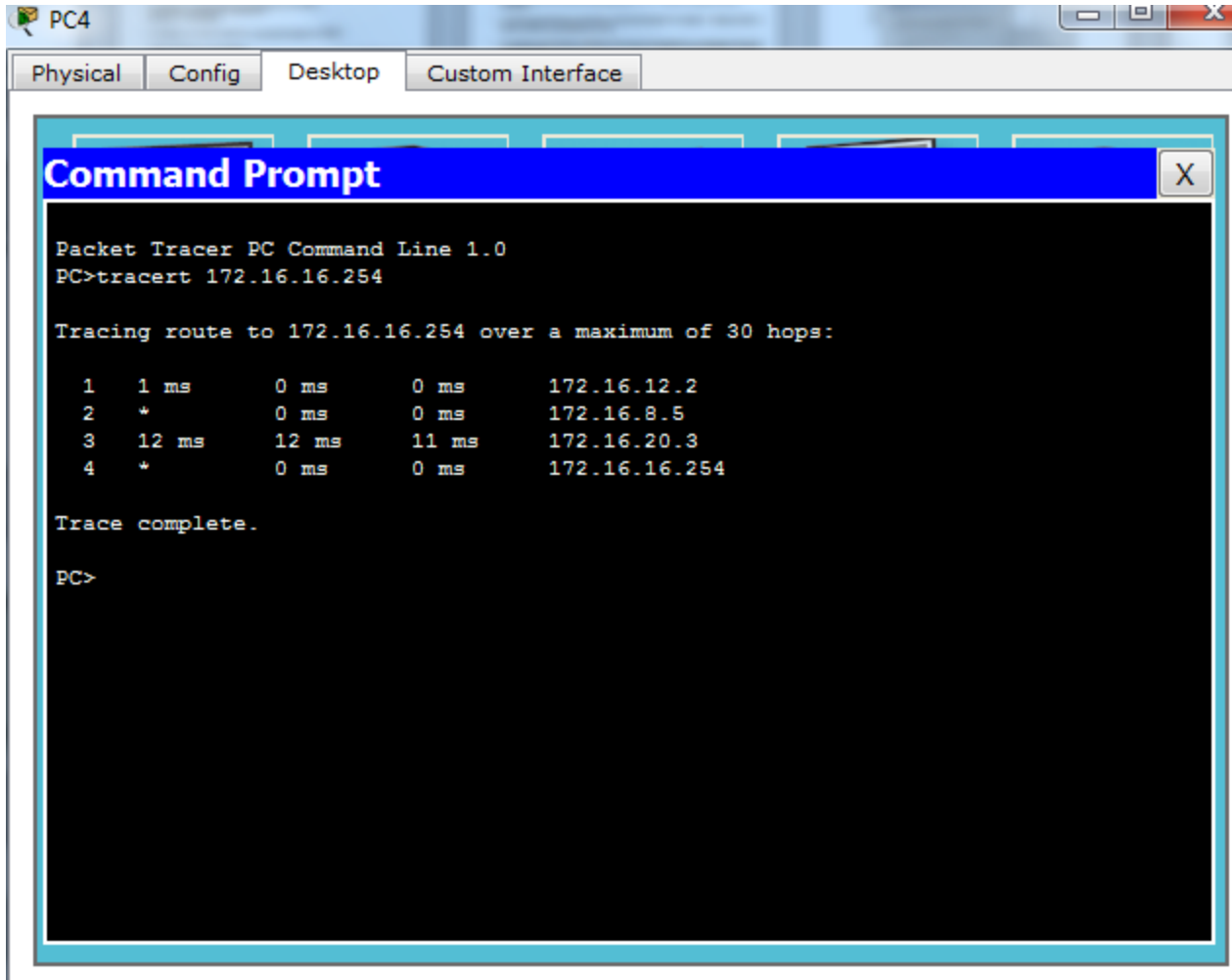
Options :
  -d          Ne pas convertir les adresses en noms d'hôtes.
  -h SautsMaxi Nombre maximum de sauts pour rechercher la cible.
  -j ListeHôtes Itinéraire source libre parmi la liste des hôtes.
  -w délai    Attente d'un délai en millisecondes pour chaque réponse.

C:\Documents and Settings\Administrator>
```

Traceroute



Traceroute



The screenshot shows a Packet Tracer PC window titled "PC4" with tabs for "Physical", "Config", "Desktop", and "Custom Interface". The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of the `tracert` command to reach the destination IP 172.16.16.254. The output displays the path taken by the packets, including the number of hops, round-trip times, and the IP addresses of the intermediate routers.

```
Packet Tracer PC Command Line 1.0
PC>tracert 172.16.16.254

Tracing route to 172.16.16.254 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms   172.16.12.2
  1  *        0 ms    0 ms   172.16.8.5
  2  12 ms   12 ms   11 ms  172.16.20.3
  3  *        0 ms    0 ms   172.16.16.254

Trace complete.

PC>
```

Traceroute



tp2-SyntheseRoutage_V5_M1A.pkt

- Faire tracet sur PC4
- Détailler les divers sauts
- Simuler une panne sur interface fa 0/1 du routeur « router3 »

Traceroute

The screenshot shows a Packet Tracer PC4 interface with a Command Prompt window open. The window has tabs for Physical, Config, Desktop, and Custom Interface. The Command Prompt displays two traceroute results.

First Traceroute (Successful):

```
Tracing route to 172.16.16.254 over a maximum of 30 hops:
```

Hop	RTT1	RTT2	RTT3	Interface
1	1 ms	0 ms	0 ms	172.16.12.2
2	*	0 ms	0 ms	172.16.8.5
3	12 ms	12 ms	11 ms	172.16.20.3
4	*	0 ms	0 ms	172.16.16.254

Trace complete.

PC>tracert 172.16.16.254

Second Traceroute (Failed):

```
Tracing route to 172.16.16.254 over a maximum of 30 hops:
```

Hop	RTT1	RTT2	RTT3	Interface
1	0 ms	0 ms	0 ms	172.16.12.2
2	0 ms	0 ms	3 ms	172.16.8.5
3	*	*	*	Request timed out.
4	*	*	*	Request timed out.
5	*	*	*	Request timed out.
6	*	*	*	Request timed out.
7	*	*	*	Request timed out.
8	*	*	*	Request timed out.
9	*	*	*	Request timed out.
10	*	*	*	Request timed out.
11	*	*	*	Request timed out.
12	*	*	*	Request timed out.
13	*	*	*	Request timed out.
14	*	*	*	Request timed out.
15	*	*	*	Request timed out.

netstat

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\user>netstat -a

Connexions actives

Proto  Adresse locale          Adresse distante        Etat
TCP    beatyou:epmap            beatyou:0                LISTENING
TCP    beatyou:microsoft-ds    beatyou:0                LISTENING
TCP    beatyou:2869            beatyou:0                LISTENING
TCP    beatyou:5190            beatyou:0                LISTENING
TCP    beatyou:5193            beatyou:0                LISTENING
TCP    beatyou:1025            beatyou:0                LISTENING
TCP    beatyou:1213            localhost:1214           ESTABLISHED
TCP    beatyou:1214            localhost:1213           ESTABLISHED
TCP    beatyou:5180            beatyou:0                LISTENING
TCP    beatyou:6999            beatyou:0                LISTENING
TCP    beatyou:nethios-ssn     beatyou:0                LISTENING
UDP    beatyou:microsoft-ds    *:
UDP    beatyou:isakmp          *:
UDP    beatyou:1026            *:
UDP    beatyou:1085            *:
UDP    beatyou:1243            *:
UDP    beatyou:1249            *:
UDP    beatyou:1254            *:
UDP    beatyou:2307            *:
UDP    beatyou:4500            *:
UDP    beatyou:48116           *:
UDP    beatyou:ntp             *:
UDP    beatyou:1031            *:
UDP    beatyou:1120            *:
UDP    beatyou:1900            *:
UDP    beatyou:4421            *:
UDP    beatyou:ntp             *:
UDP    beatyou:nethios-ns      *:
UDP    beatyou:nethios-dgm     *:
UDP    beatyou:1900            *:

C:\Documents and Settings\user>
```

nslookup

```
C:\>nslookup cisco.netcad.net
Server: DNSTEST.svr.example.com
Address: 192.168.254.32

Non-authoritative answer:
Name:   cisco.netcad.net
Address: 209.165.200.224
```

