
INF3405

Réseaux informatiques

Architecture technologique TCP/IP

Partie 1 : Protocoles IP

Contenu du module, partie 1

Ce module traite des protocoles de la couche 3 de l'architecture technologique TCP/IP.

- Caractéristiques de la technologie IP
- Standards
- Routeurs
- Adressage IP et sous-réseautage
- Routage avec les adresses IP
- Format du paquet IP
- *Internet Control Message Protocol* (ICMP)
- *Address Resolution Protocol* (ARP)
- *Network Address Translation* (NAT)

Contenu du module , partie 1 (suite)

- Routage dynamique dans les réseaux IP
- *Domain Name Server* (DNS)
- *Dynamic Host Configuration Protocol* (DHCP)
- *IP next generation* (IPng) ou IP version 6 (IPv6).

Caractéristiques de la technologie IP

- Technologie de commutation de paquets.
- Utilisation de paquets de longueur variable.
- Service sans connexion.
- Supporte les communications à débit variable.
- Offre de la bande passante sur demande.
- Utilisation de liens à hauts débits.
- Pas de qualité de service garantie.

Architecture des Réseaux

Échanges d'informations

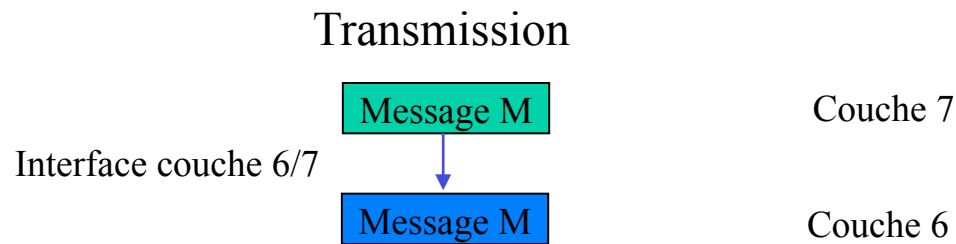
Transmission

Message M

Couche 7

Architecture des Réseaux

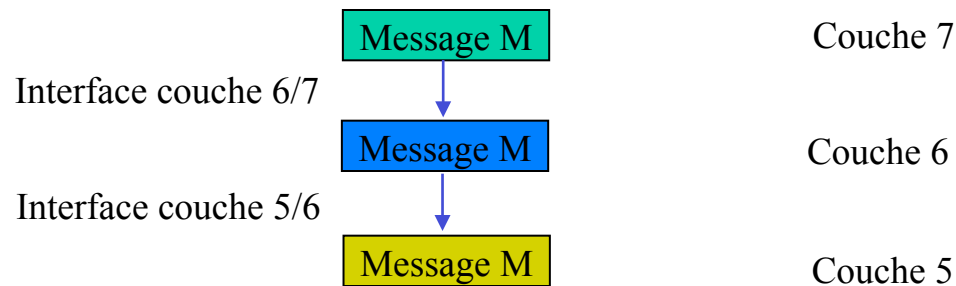
Échanges d'informations



Architecture des Réseaux

Échanges d'informations

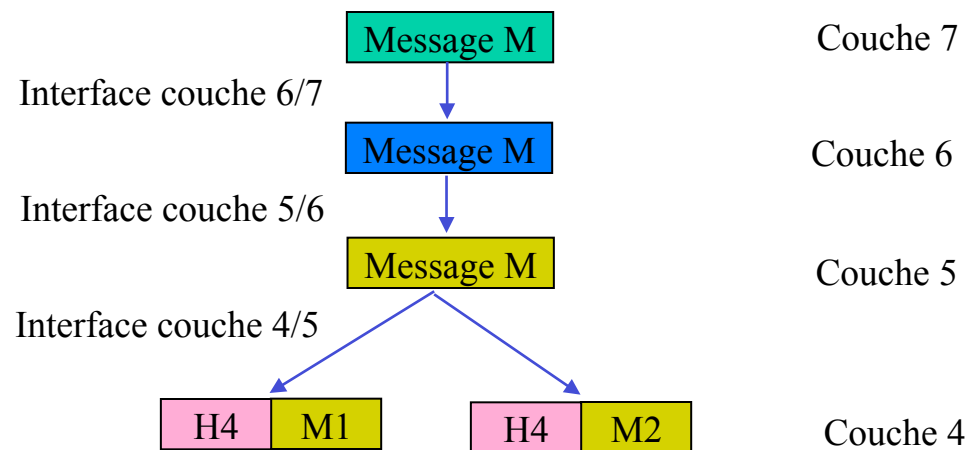
Transmission



Architecture des Réseaux

Échanges d'informations

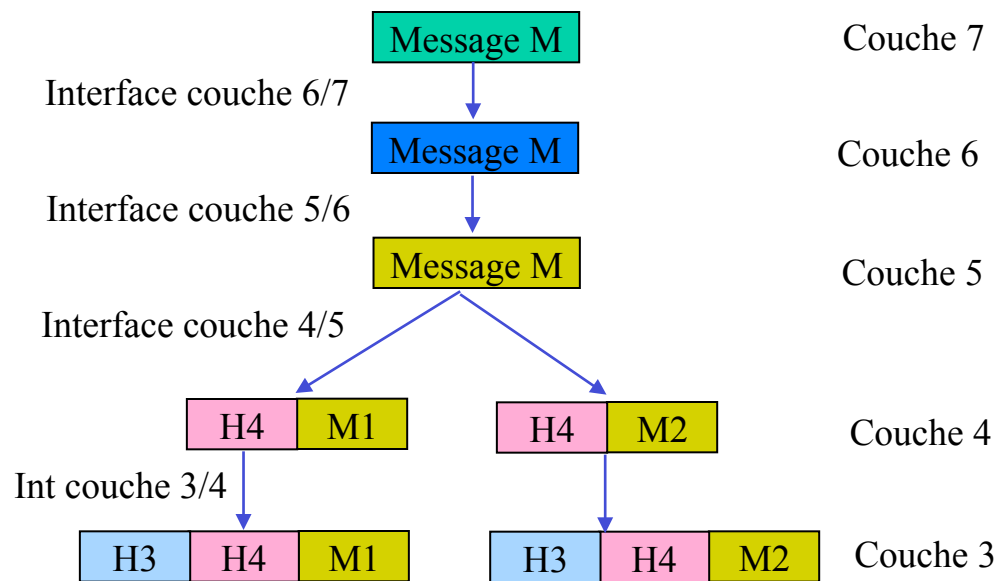
Transmission



Architecture des Réseaux

Échanges d'informations

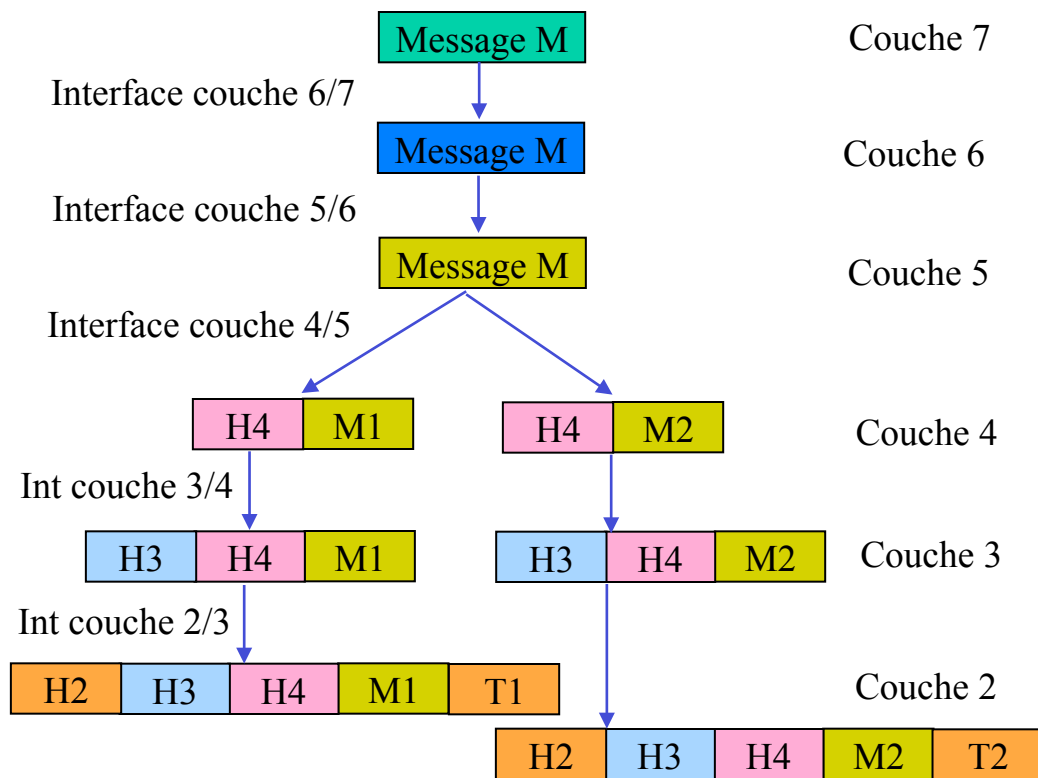
Transmission



Architecture des Réseaux

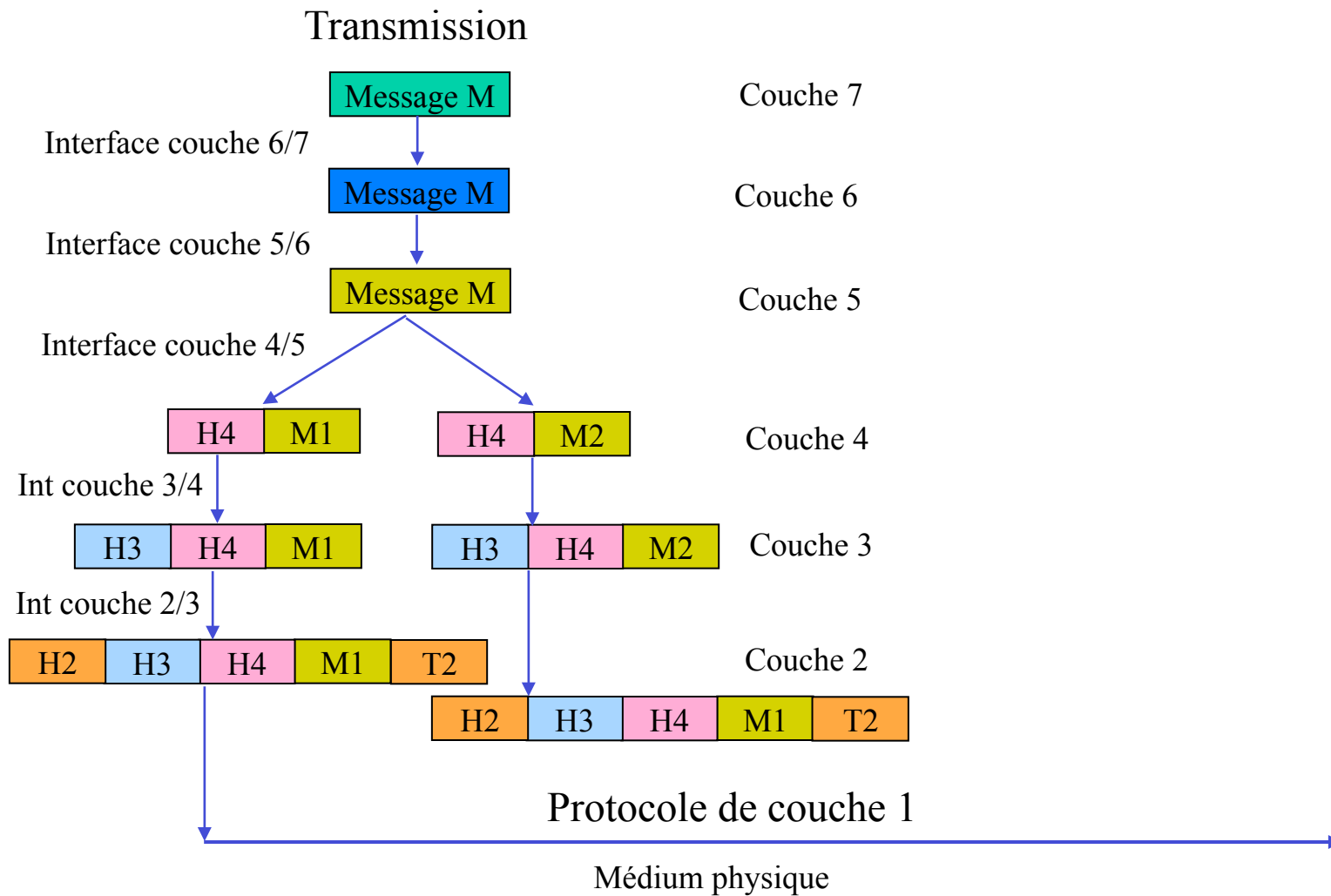
Échanges d'informations

Transmission



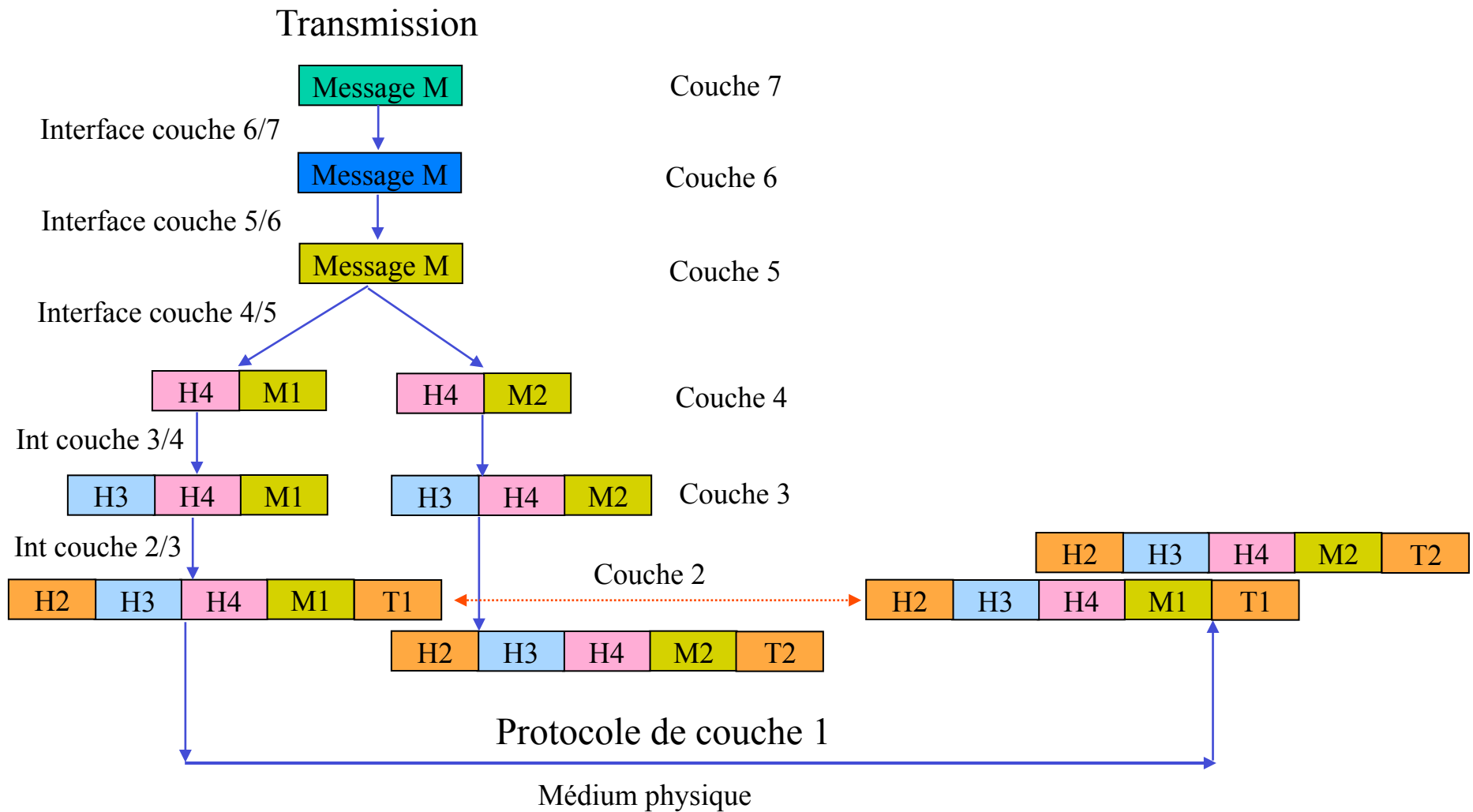
Architecture des Réseaux

Échanges d'informations



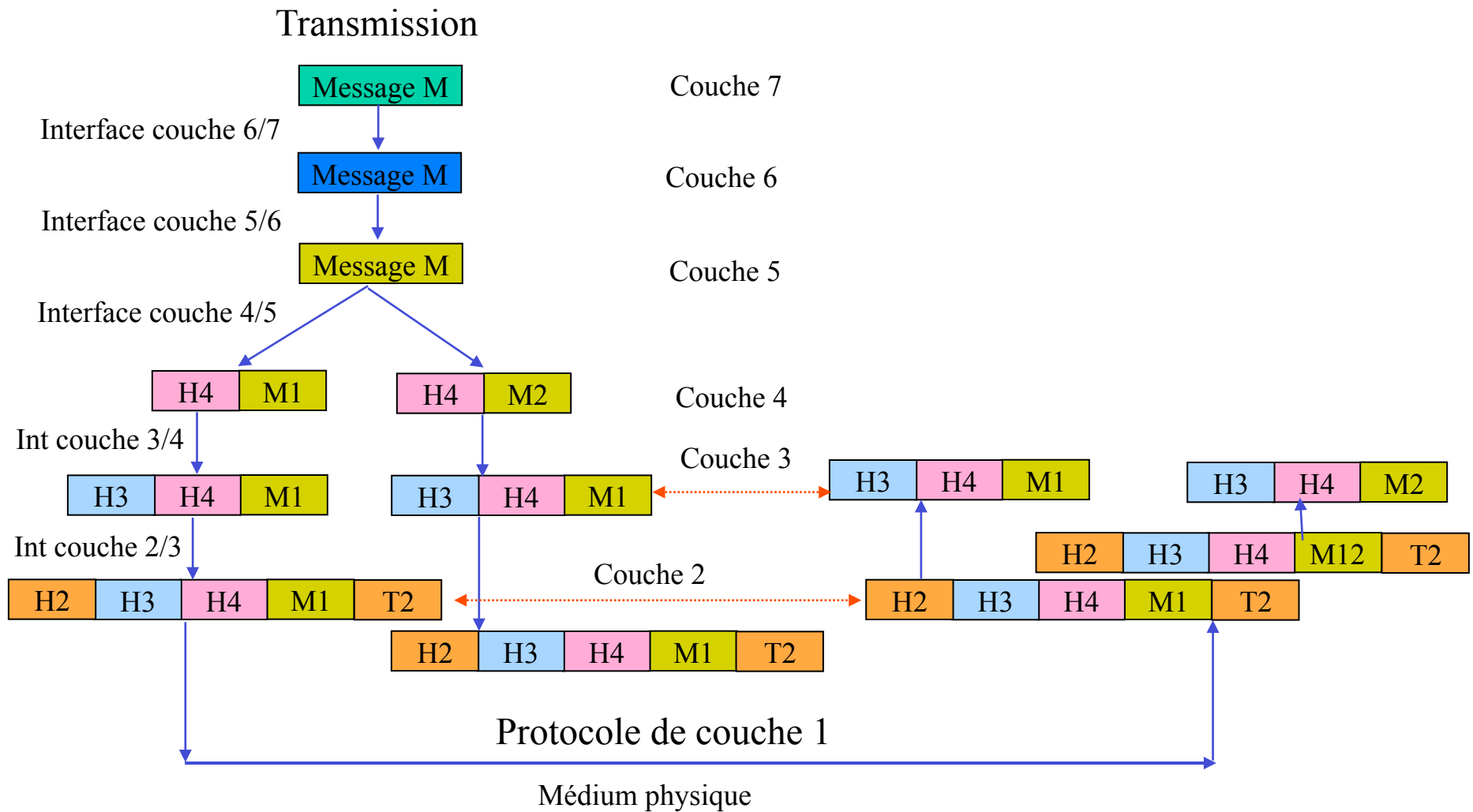
Architecture des Réseaux

Échanges d'informations



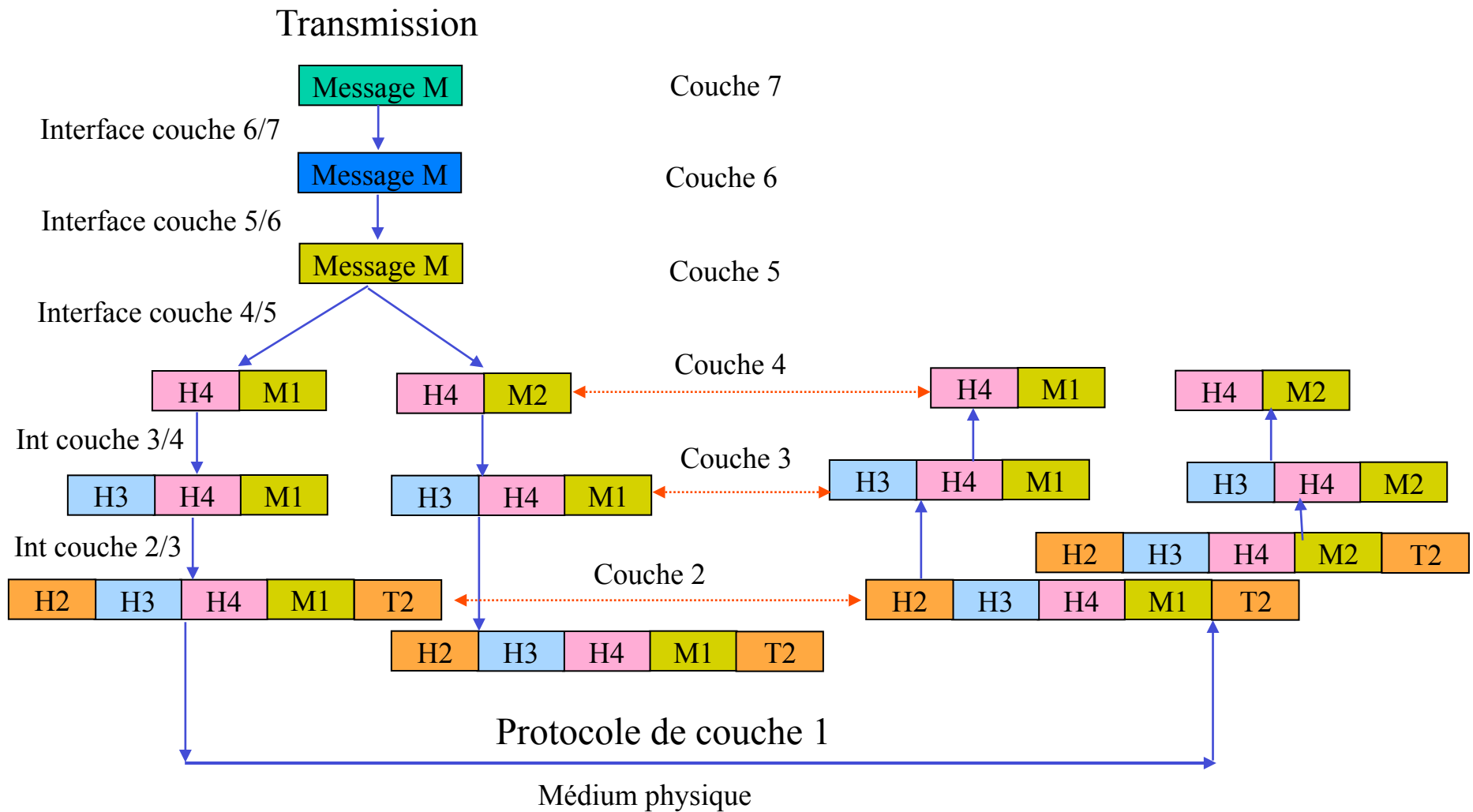
Architecture des Réseaux

Échanges d'informations



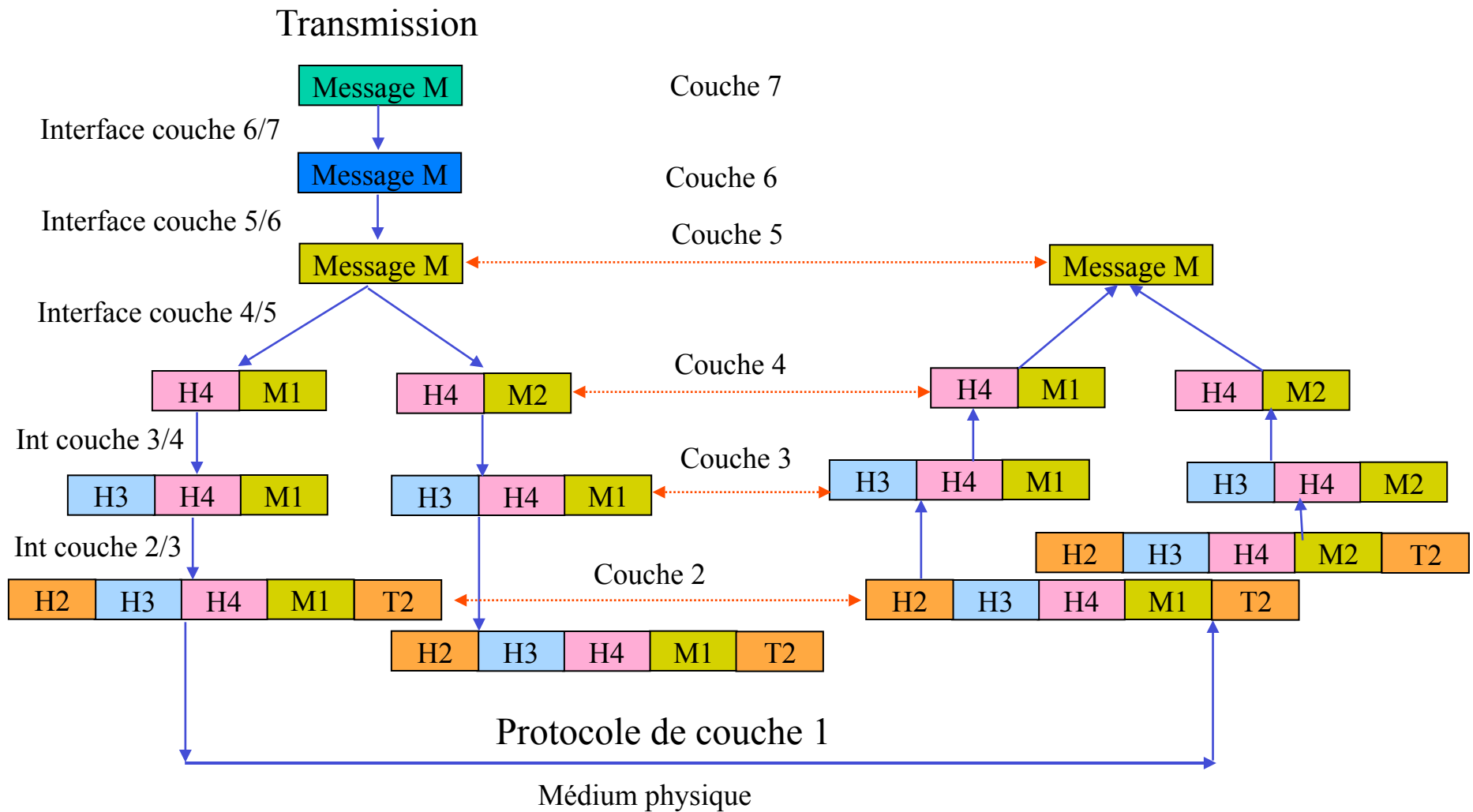
Architecture des Réseaux

Échanges d'informations



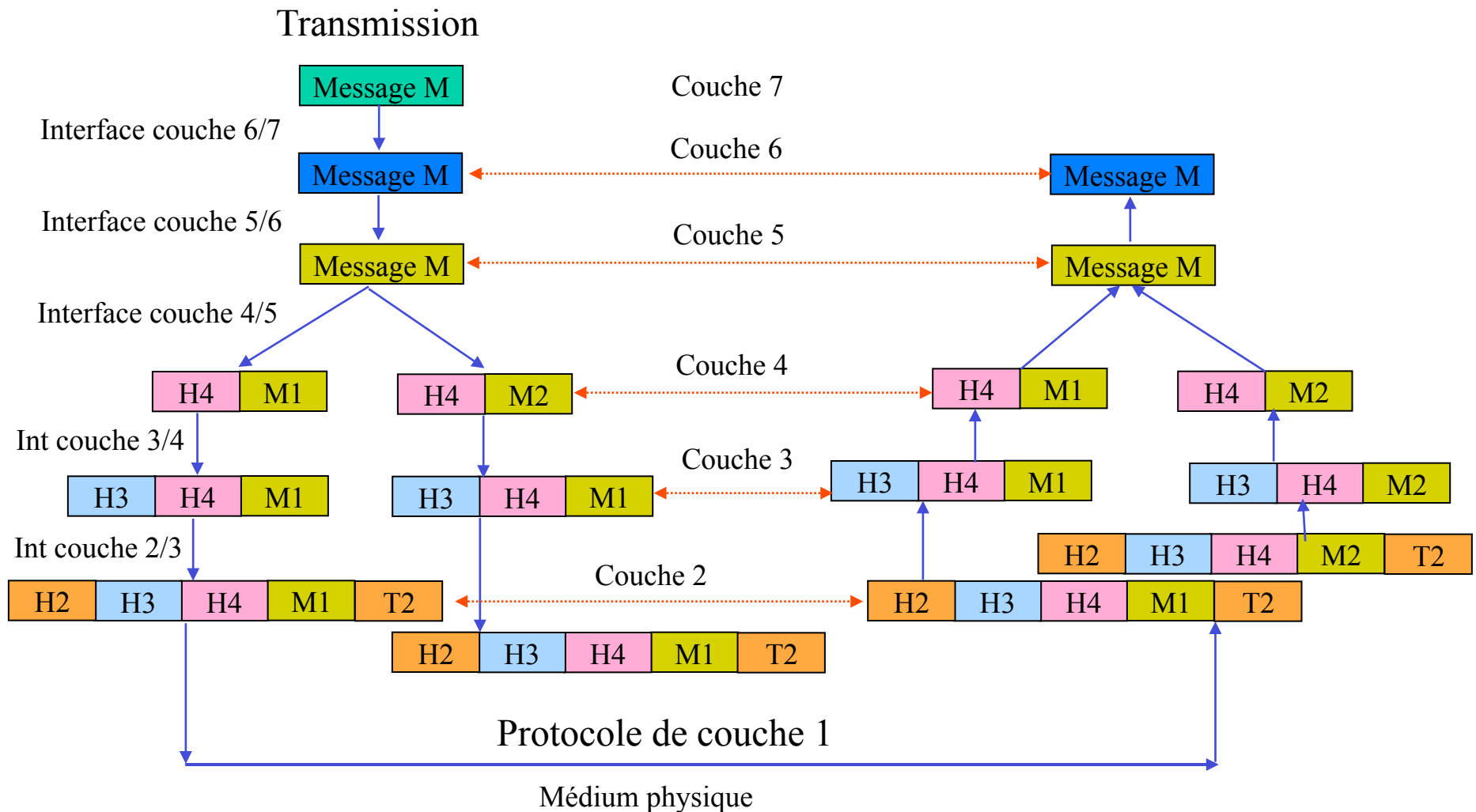
Architecture des Réseaux

Échanges d'informations



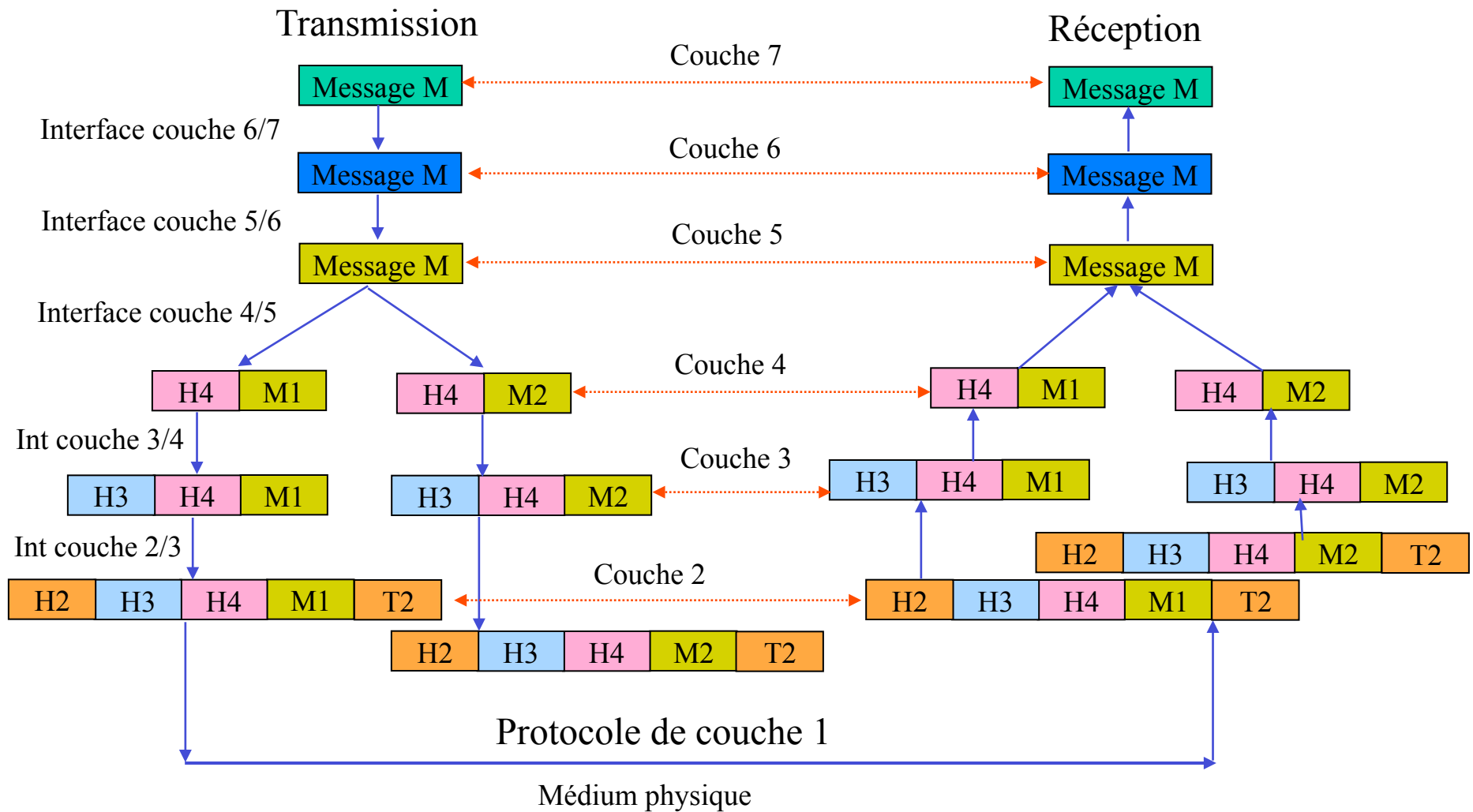
Architecture des Réseaux

Échanges d'informations



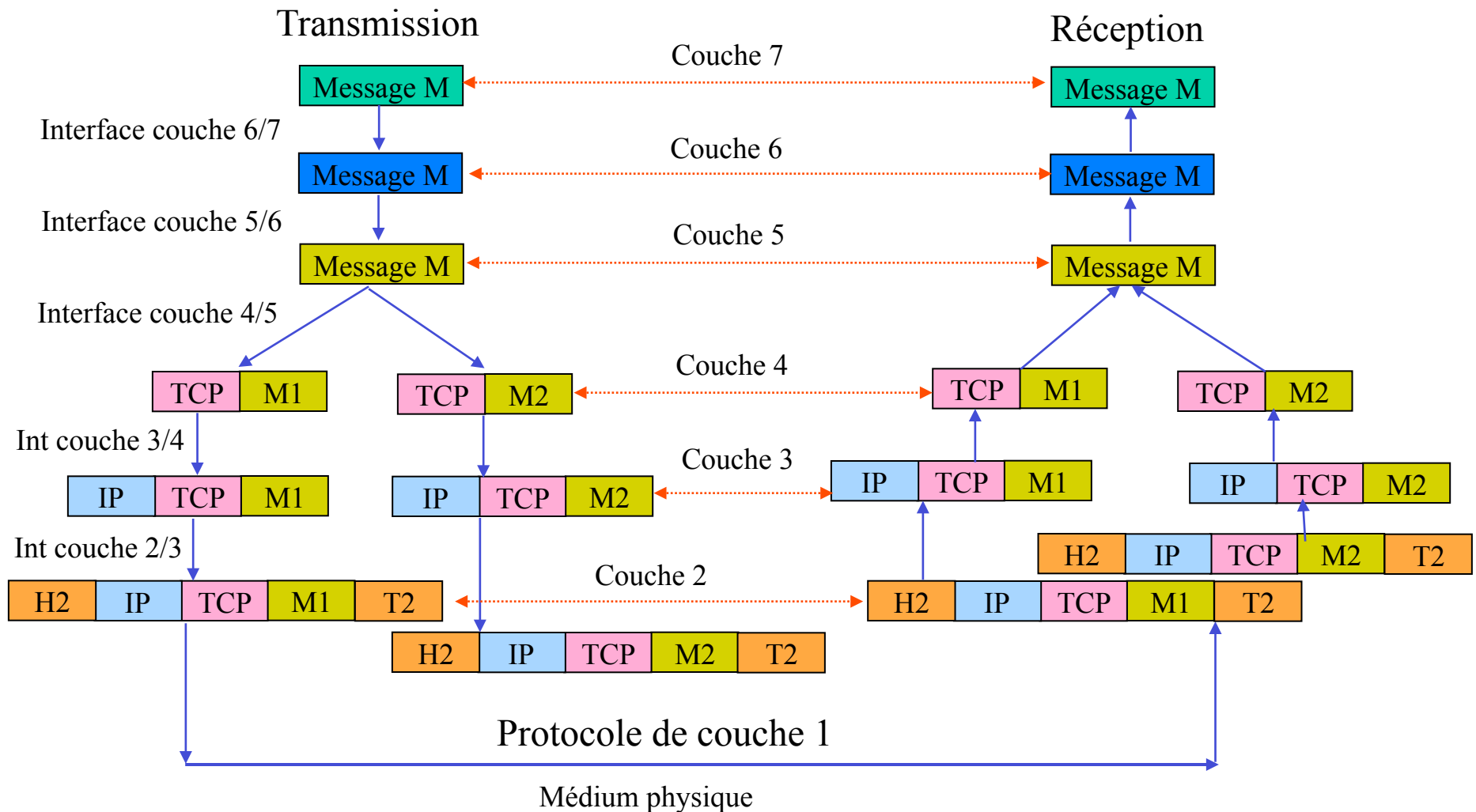
Architecture des Réseaux

Échanges d'informations



Architecture des Réseaux

Échanges d'informations avec TCP/IP



Standards

- L'organisme de standardisation de la technologie IP (*Internet Protocol*) est l'IETF (*Internet Engineering Task Force*, www.ietf.org).
- Fondée en 1986, l'IETF regroupe des manufacturiers (e.g., Nortel Networks, Alcatel, Cisco Systems, Juniper Networks, Lucent Technologies, etc.), des transporteurs (e.g., AT&T, UUNET, etc.) et des universités.
- L'IETF compte 8 sections (*Areas*).
- Chaque section comporte différents groupes de travail (*Working Groups*).

Standards (suite)

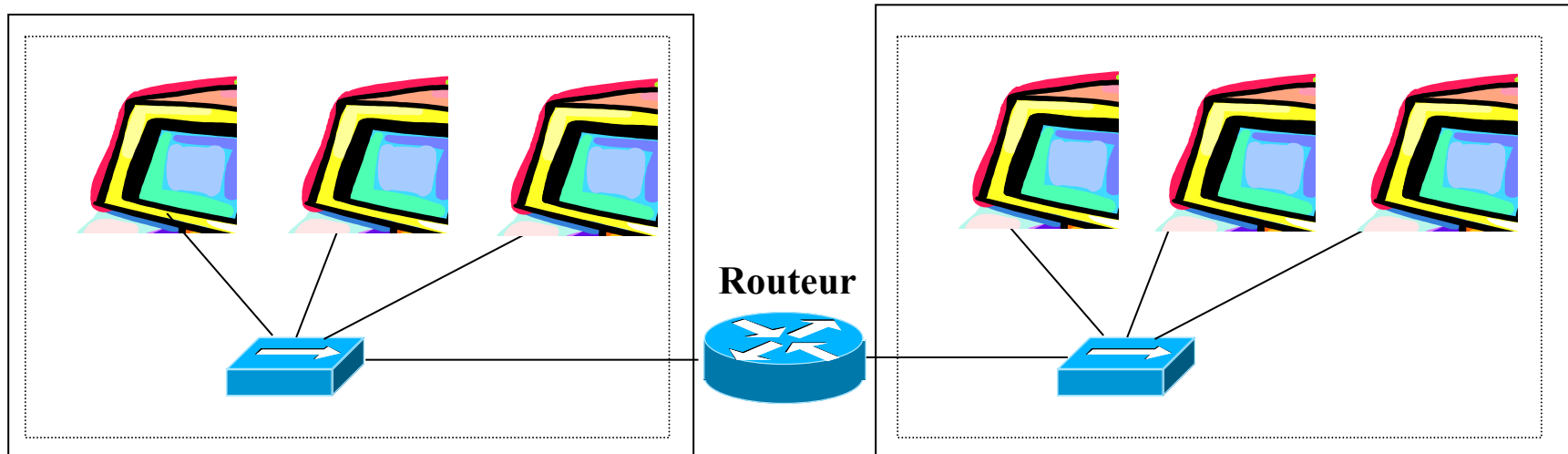
- Les sections de l'IETF
 - *Applications* : Extensions to FTP (File Transfer Protocol), Telnet Enhancements, etc.
 - *General* : Internet Traffic Engineering, IP over Optical, etc.
 - *Internet* : DHC (Dynamic Host Configuration), PPP (Point to Point Protocol) Extensions, etc.
 - *Operations and Management* : SNMP (Simple Network Management Protocol) Version 3, RMON (Remote Monitoring), etc.
 - *Routing* : Multicast Extensions to OSPF (Open Shortest Path First), BGMP (Border Gateway Multicast Protocol), etc.

Standards (suite)

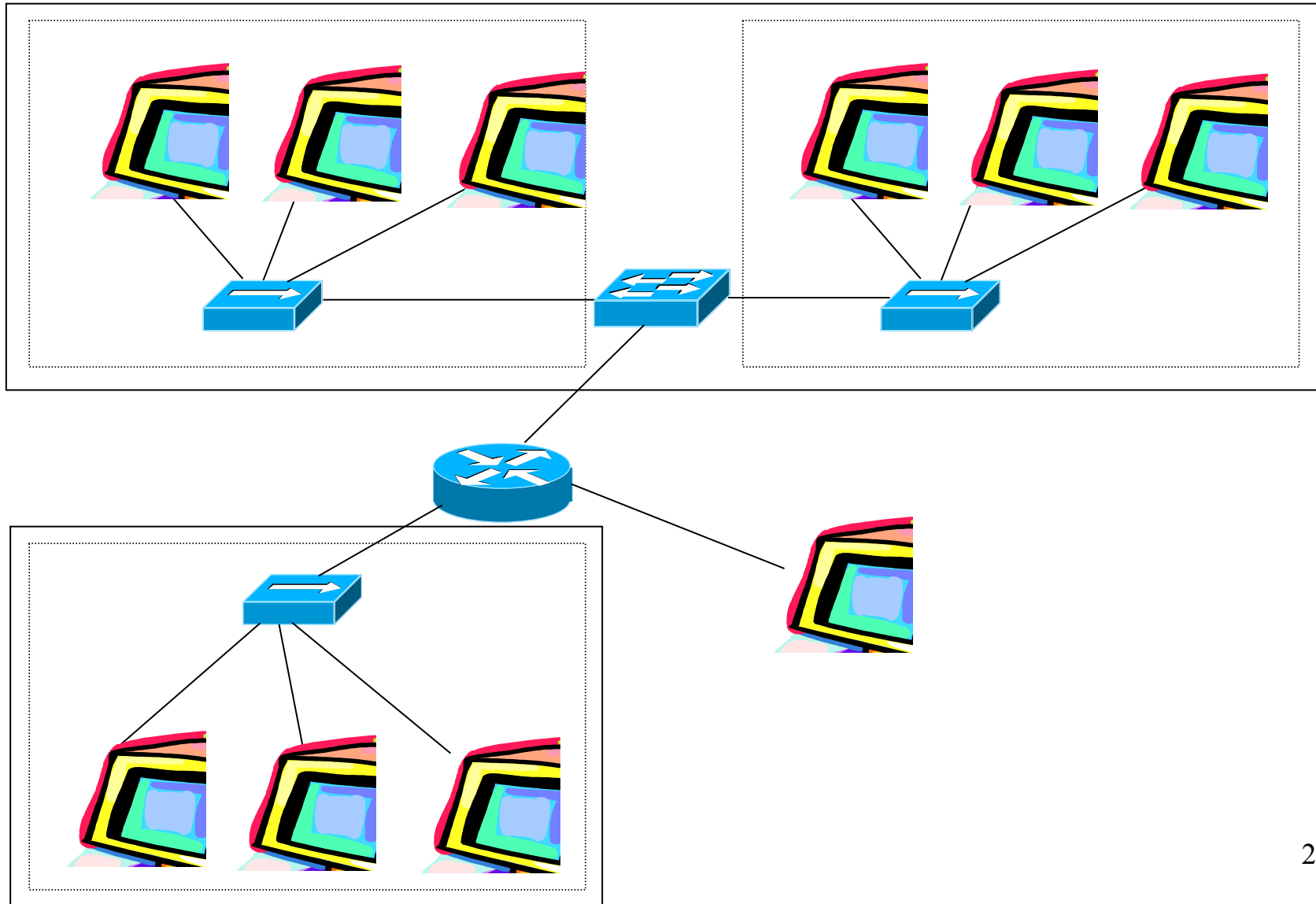
- Les sections de l'IETF (suite)
 - *Security* : IPSec (IP Security Protocol), Web Transactions Security, etc.
 - *Transport* : IP Telephony, RSVP (Resource Reservation Protocol), etc.
 - *User services* : Responsible Use of the Network, User Services.
- Autres organismes:
 - IAB (Internet Architecture Board, www.iab.org)
 - IANA (Internet Assigned Numbers Authority, www.iana.org).

Routeur

- Un routeur est un équipement qui sert à relier des réseaux locaux indépendamment des protocoles de niveau 2 utilisés.
- Un routeur fonctionne au niveau 3 du modèle OSI.
- Le routeur a pour fonction d'aiguiller les paquets provenant d'un réseau IP vers leur destination.
- Le routeur permet de séparer les domaines de *Broadcast*.

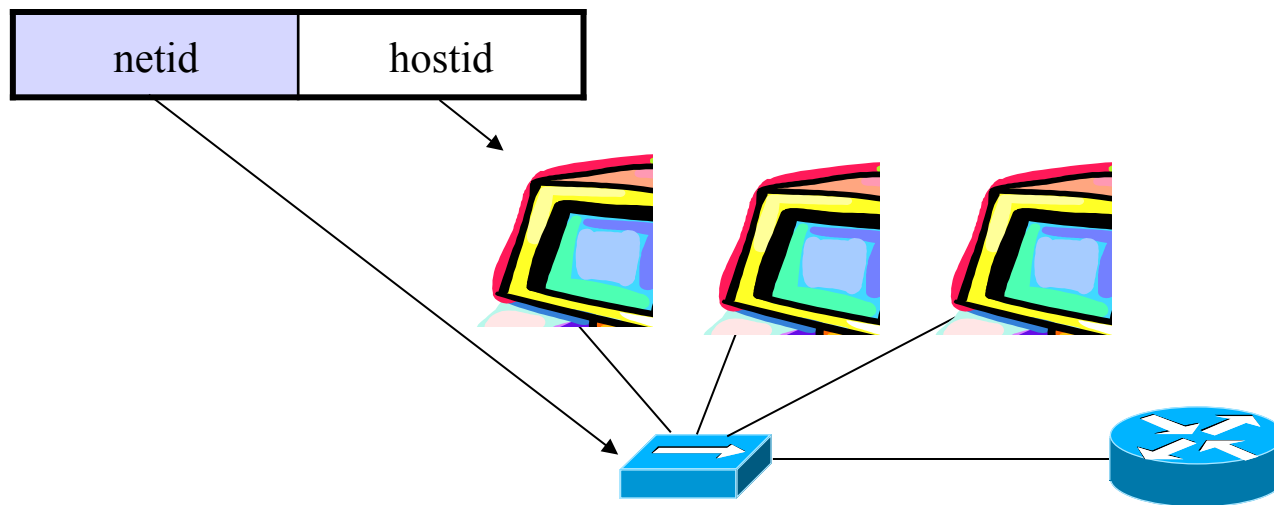


Routeur (suite)



Adressage IP

- L'adressage IP (de niveau 3) permet d'identifier les équipements (cartes réseaux, interfaces des routeurs) communiquant avec le protocole IP.
- Une adresse IP comporte 2 parties:
 - *netid* : identifie l'adresse du réseau
 - *hostid* : identifie l'équipement sur le réseau.



Adressage IP (suite)

- Une adresse IP comporte 4 octets.
- Chaque octet est séparé par un point, par exemple, 191.138.2.1.
- Chaque adresse IP comporte deux parties
 - La première représente le numéro du réseau.
 - La seconde représente le numéro d'un équipement particulier.
- Valeurs associées
 - Masque de réseau.
 - Passerelle par défaut.

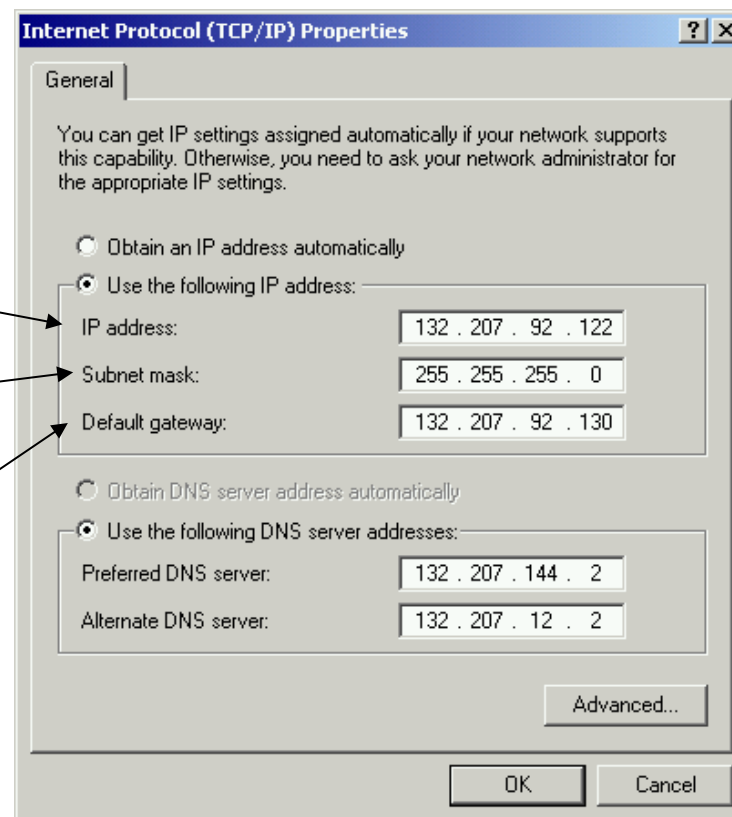
Adressage IP (suite)

- Configuration dans Windows

Adresse IP

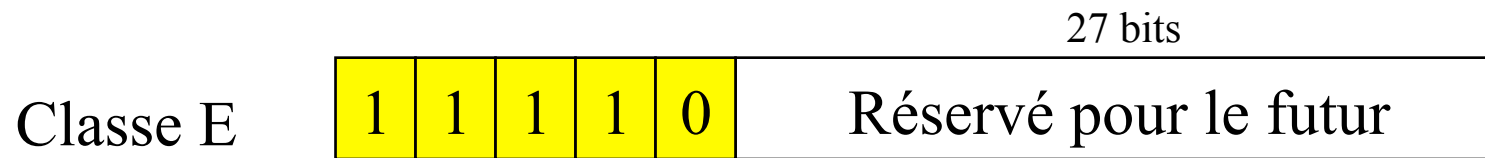
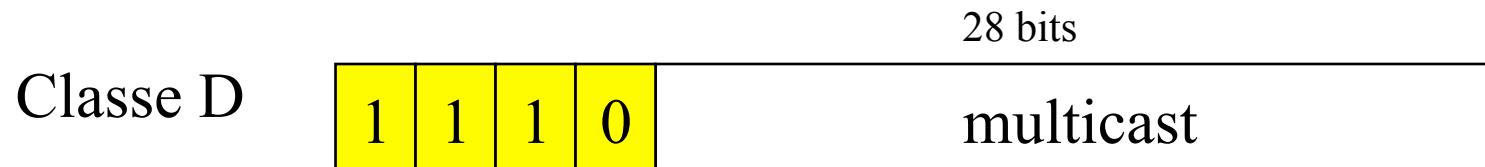
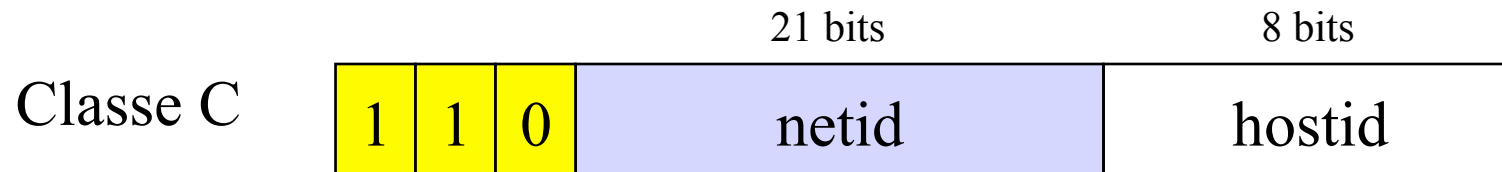
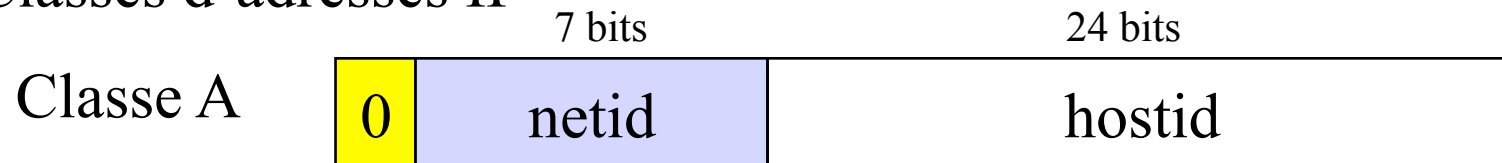
Masque de réseau

Passerelle par défaut



Adressage IP (suite)

- Classes d'adresses IP



Adressage IP (suite)

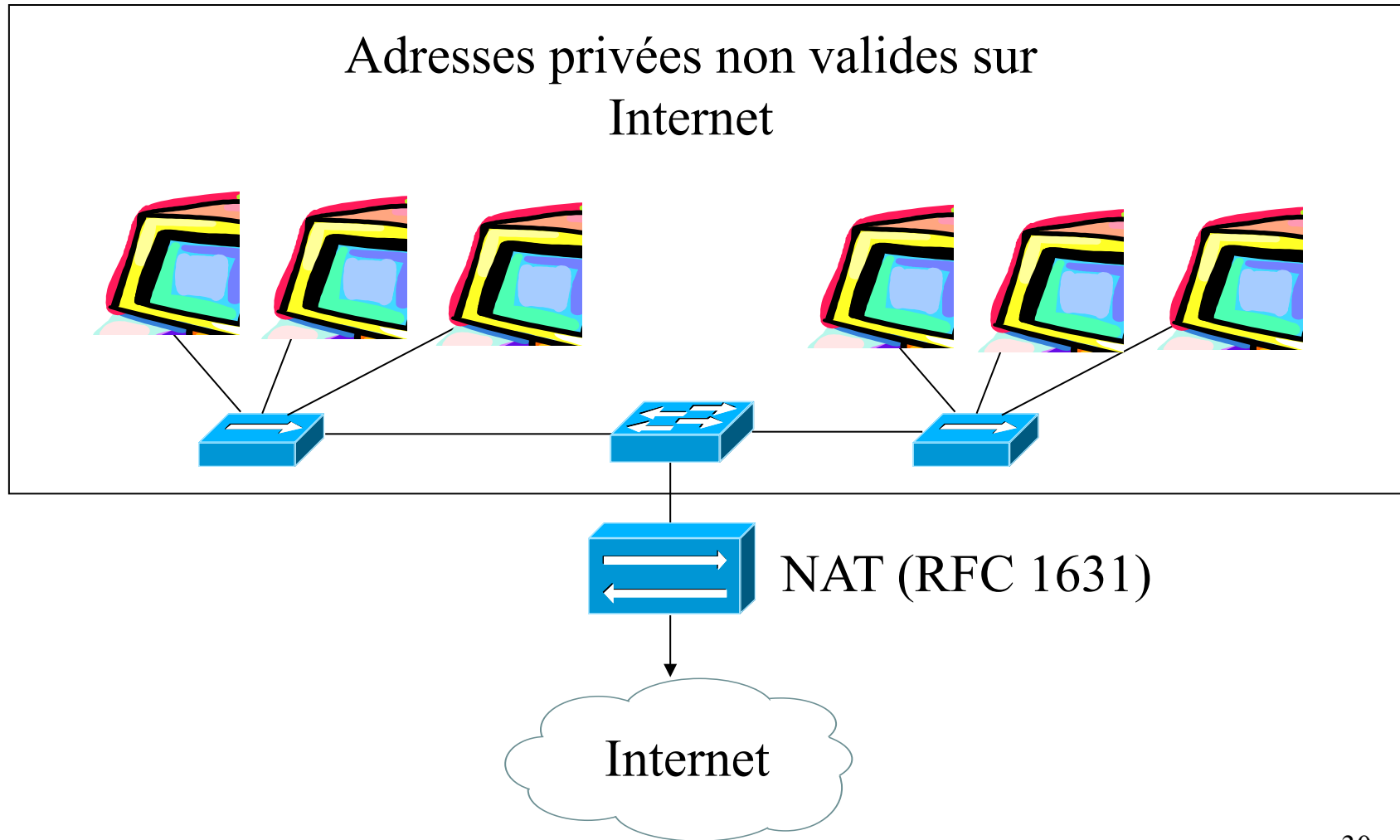
- Classes d'adresses IP (suite)
 - Classe A
 - Deux adresses réservées 0.0.0.0 et 127.0.0.0.
 - 126 réseaux disponibles 1.0.0.0 à 126.0.0.0.
 - 16 777 214 adresses hôtes par réseau.
 - Classe B
 - 16 382 réseaux disponibles, de 128.0.0.0 à 191.255.0.0.
 - 65 534 adresses hôtes par réseau.
 - Classe C
 - 2 097 150 réseaux disponibles de 192.0.0.0 à 223.255.255.0.
 - 254 adresses hôtes par réseau.
 - Classe D
 - 268 435 456 groupes multicast.

Adressage IP (suite)

- Classes d'adresses IP (suite)
 - Classe d'adresses privées (RFC 1597)
 - Une classe A: 10.0.0.0.
 - 16 classes B: 172.16.0.0 à 172.31.0.0.
 - 256 classes C: 192.168.0.0 à 192.168.255.0.
 - Les classes d'adresses privées doivent être utilisé à l'interne (non valide sur l'Internet).
 - La traduction peut être faite avec, par exemple, la fonction NAT (*Network Address Translation*).

Adressage IP (suite)

- Classes d'adresses IP (suite)



Adressage IP (suite)

- Le sous-réseautage
 - Le sous-réseautage consiste à utiliser des bits du champ *hostid* pour définir des sous-réseaux.
 - Le *hostid* est alors divisé en 2 :
 - subnetid ;
 - hostid.
- Exemple

136.183.XXX.SSS/24

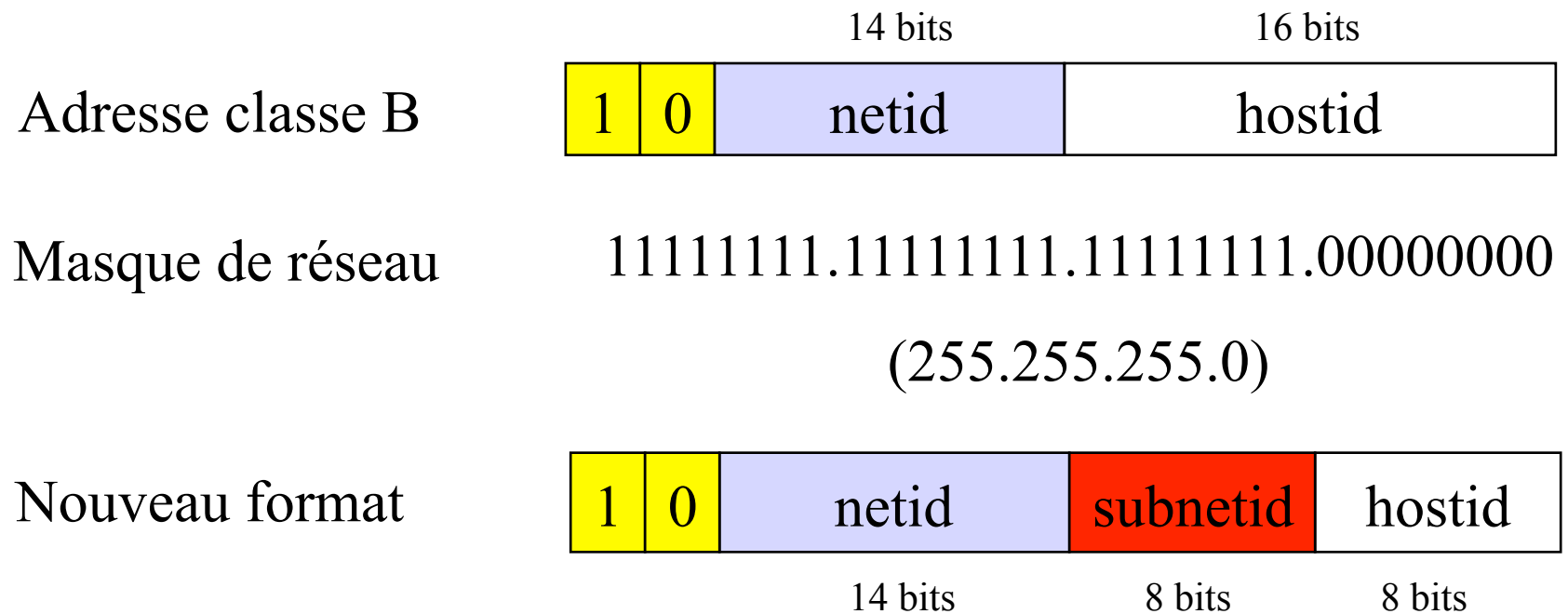
XXX = désigne le numéro du sous-réseau

SSS = désigne le numéro de station

/24 = désigne un masque de 24 bits (255.255.255.0).

Adressage IP (suite)

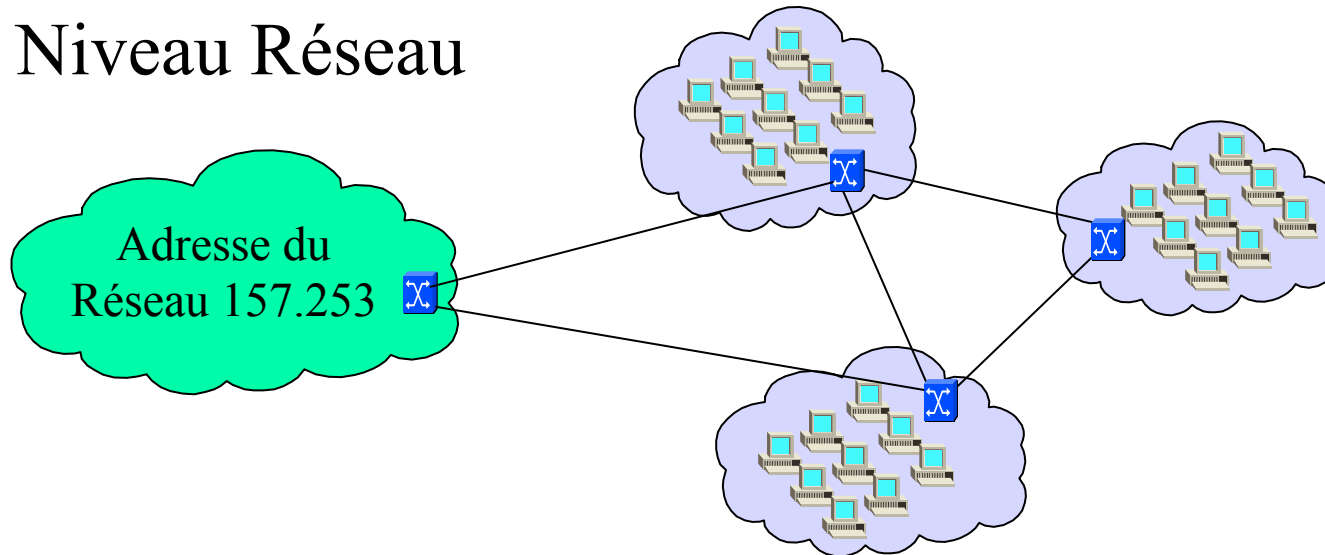
- Le sous-réseautage (suite)



La couche Réseau – Protocole IP

Sous-réseaux

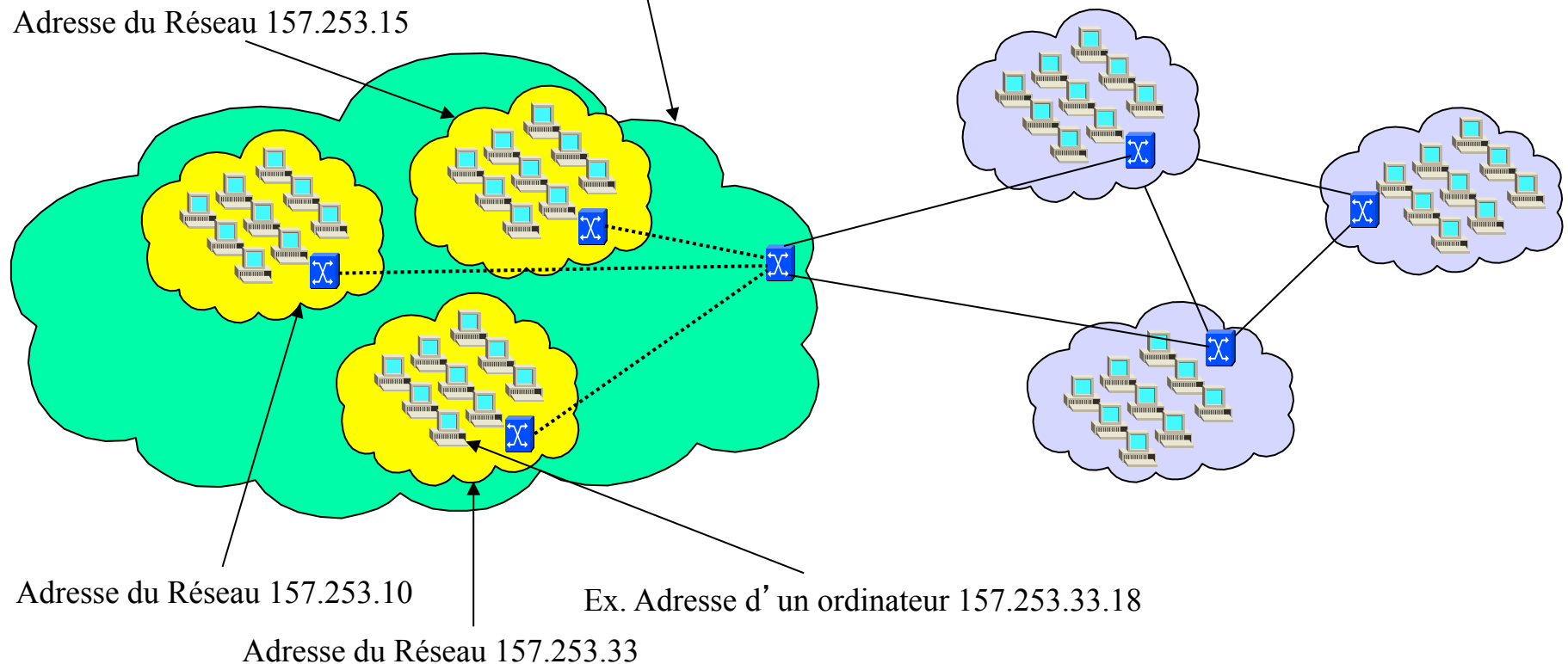
Niveau Réseau



La couche Réseau – Protocole IP

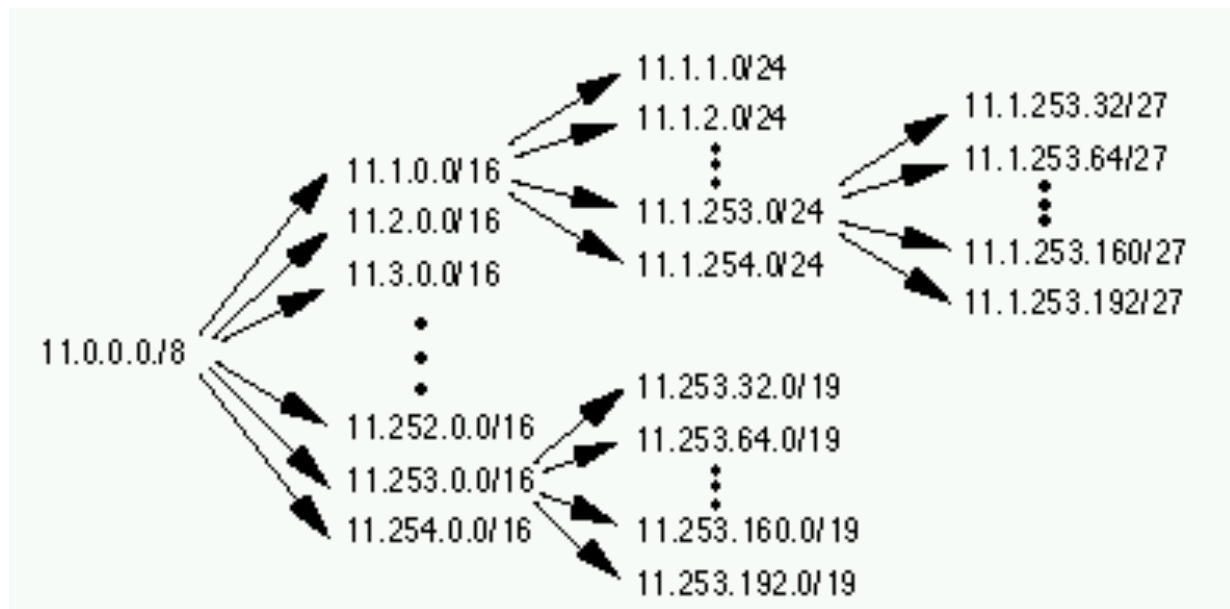
Sous-réseaux

Niveau Sous-Réseau
Adresse du Réseau 157.253



Adressage IP (suite)

- VLSM (*Variable Length Subnet Mask*)

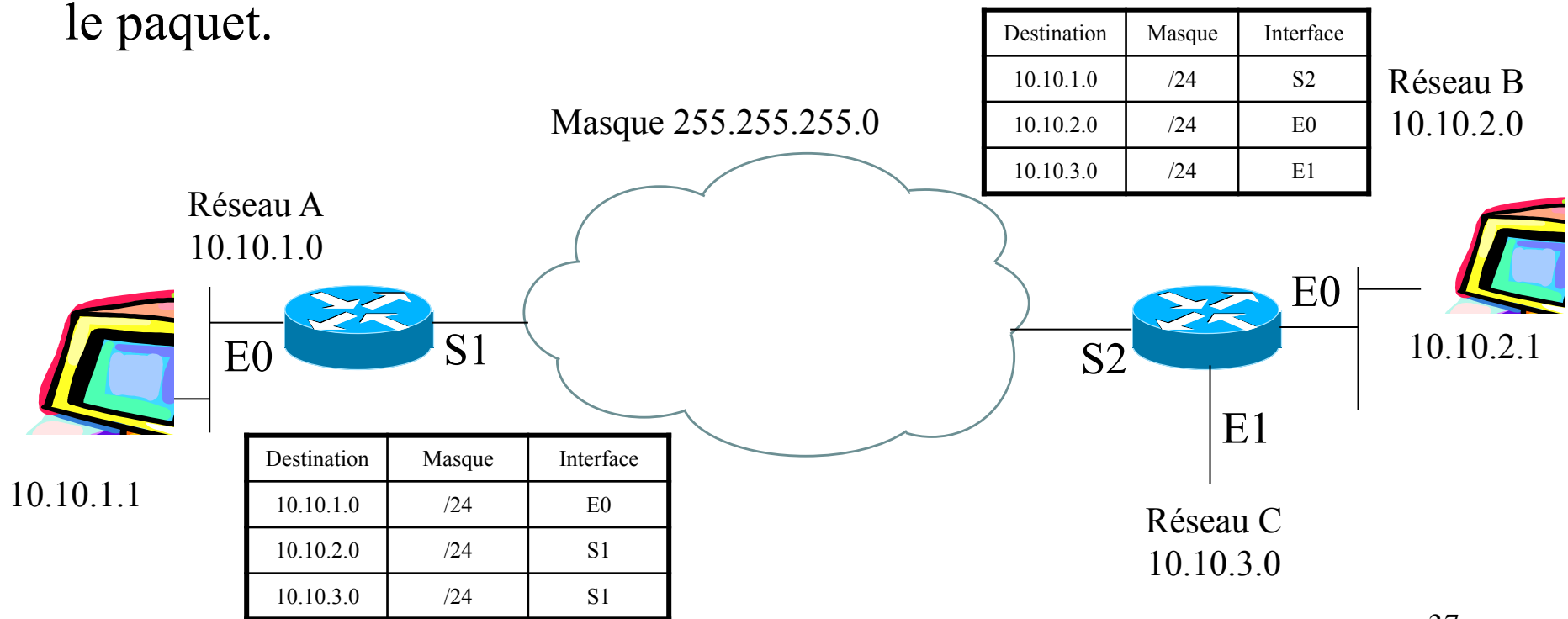


Adressage IP (suite)

- CIDR (*Classless Interdomain Routing*)
 - CIDR supprime l'usage des classes A, B et C pour généraliser celui du préfixe réseau étendu. Les classes A, B ou C n'existent plus; toutes les adresses de réseaux sont annoncées avec leur préfixe qui peut être de taille arbitraire : /9, /10, /11, /12 ...
 - Les routeurs ne se basent plus sur les 3 premiers bits de chaque adresse pour déterminer la classe du réseau : seul le préfixe fait loi.
 - Les adresses annoncées de cette manière peuvent être d'anciennes adresses de classe A, B ou C. Par exemple, et respectivement, 10.45.63.0/20, 130.5.0.0/20 et 192.56.32.0/20.

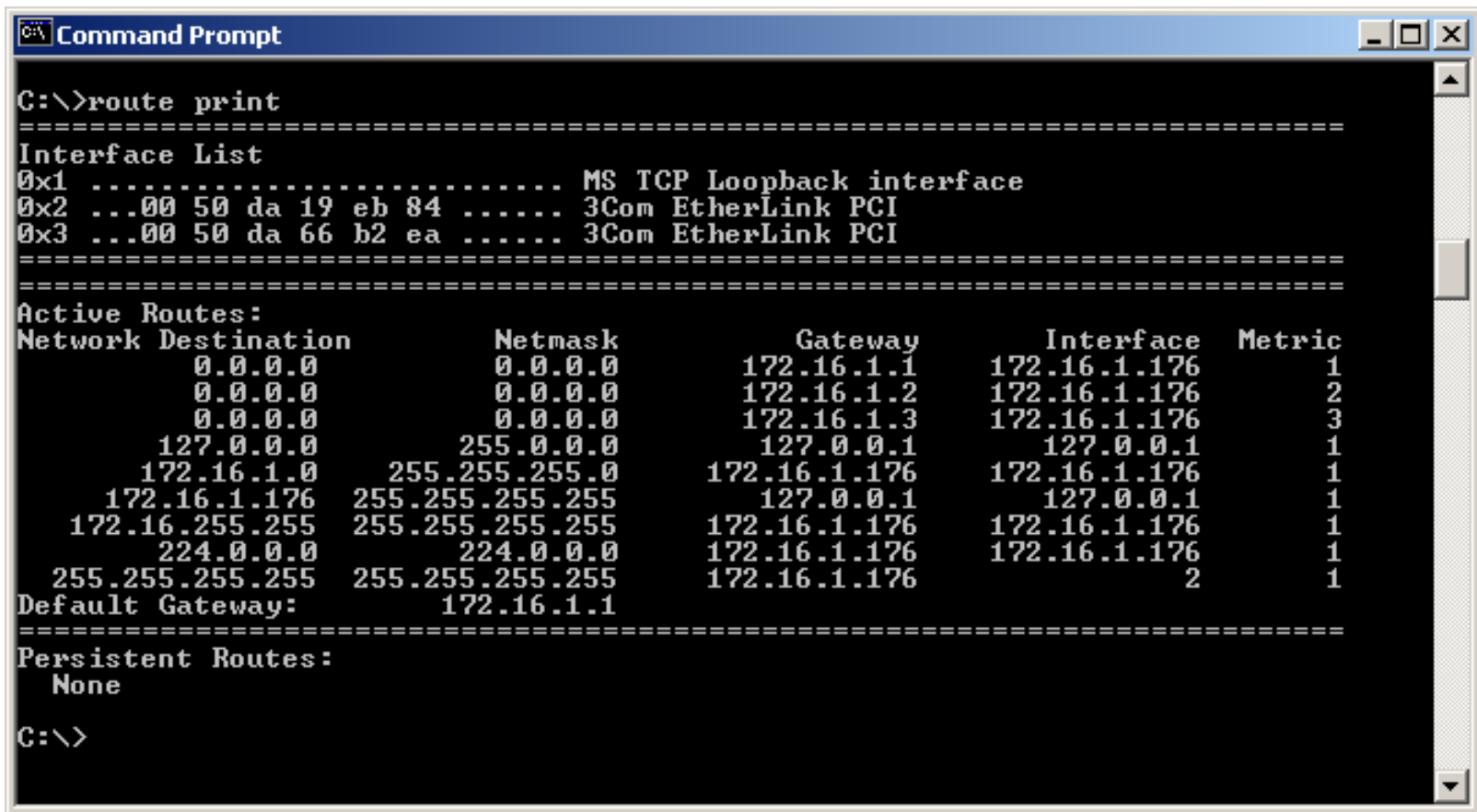
Routage avec les adresses IP

- Chaque routeur utilise les adresses IP pour aiguiller l'information (les paquets).
- Le routeur regarde l'adresse IP de destination dans chaque paquet IP et détermine l'interface de sortie sur lequel il transmettra le paquet.



Routage avec les adresses IP (suite)

- Table de routage d'un PC (route print)



```
C:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 50 da 19 eb 84 ..... 3Com EtherLink PCI
0x3 ...00 50 da 66 b2 ea ..... 3Com EtherLink PCI
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface         Metric
0.0.0.0                    0.0.0.0          172.16.1.1        172.16.1.176      1
0.0.0.0                    0.0.0.0          172.16.1.2        172.16.1.176      2
0.0.0.0                    0.0.0.0          172.16.1.3        172.16.1.176      3
127.0.0.0                  255.0.0.0        127.0.0.1         127.0.0.1         1
172.16.1.0                 255.255.255.0    172.16.1.176      172.16.1.176      1
172.16.1.176              255.255.255.255  127.0.0.1         127.0.0.1         1
172.16.255.255            255.255.255.255  172.16.1.176      172.16.1.176      1
224.0.0.0                  224.0.0.0        172.16.1.176      172.16.1.176      1
255.255.255.255          255.255.255.255  172.16.1.176      2                 1
Default Gateway:          172.16.1.1
=====
Persistent Routes:
None
C:\>
```

Routage avec les adresses IP (suite)

- Table de routage d'un routeur Cisco (sh ip route)

```
Command Prompt - telnet 172.24.0.1

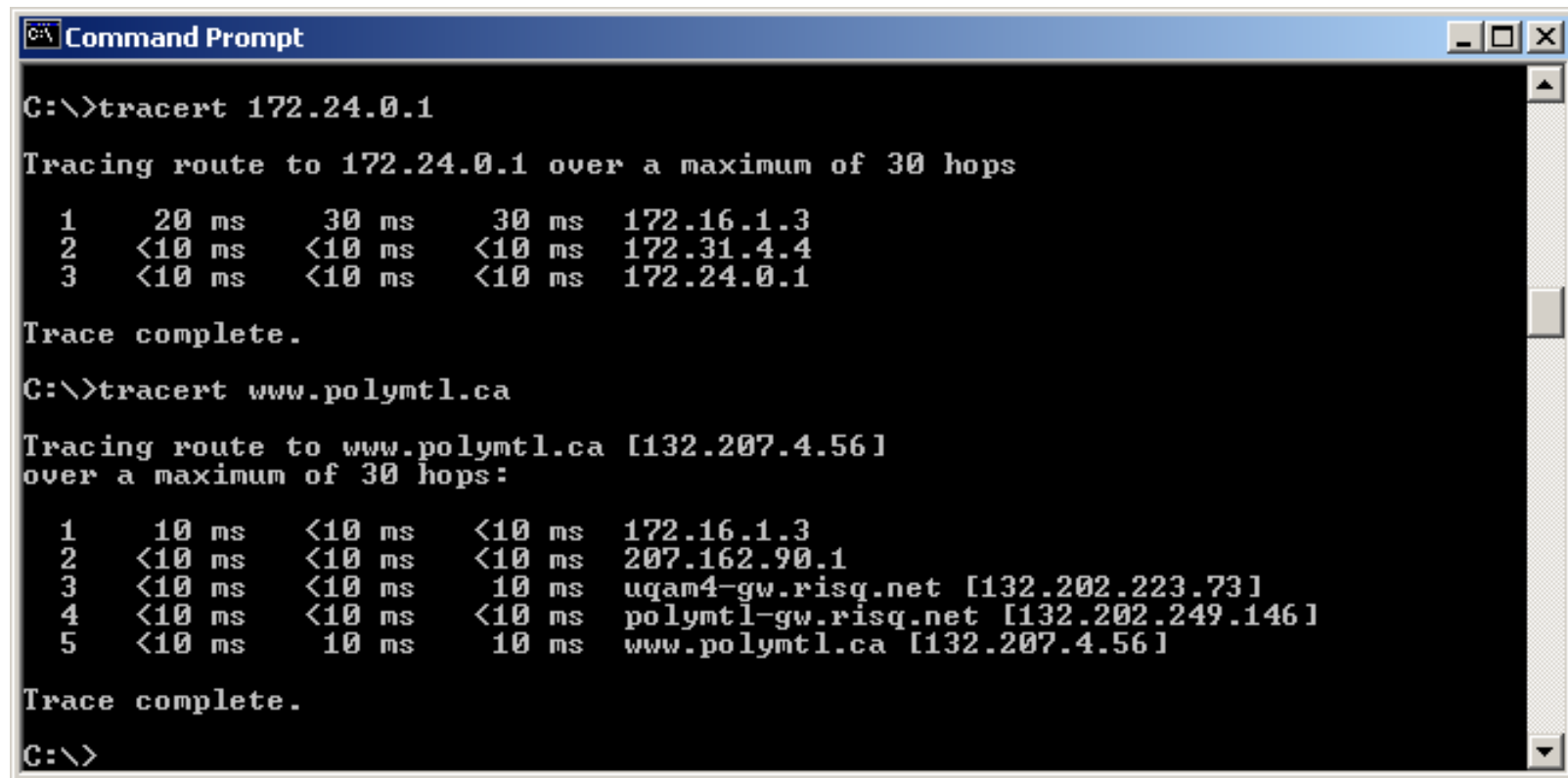
Chicago-ISP-1# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.24.2.6 to network 0.0.0.0

B    172.16.0.0/16 [20/0] via 172.24.2.6, 4d16h
B    172.25.0.0/16 [200/100] via 172.24.2.2, 03:37:34
     172.24.0.0/16 is variably subnetted, 16 subnets, 3 masks
C    172.24.1.200/30 is directly connected, ATM3/0.10
O    172.24.1.52/30 [110/2] via 172.24.1.17, 03:37:55, BUI1
C    172.24.1.48/30 is directly connected, Serial5/0.1
C    172.24.32.0/24 is directly connected, FastEthernet1/0
C    172.24.33.0/24 is directly connected, BUI2
O    172.24.1.44/30 [110/98] via 172.24.1.17, 03:37:55, BUI1
C    172.24.1.40/30 is directly connected, Serial5/0.2
C    172.24.1.16/30 is directly connected, BUI1
C    172.24.2.4/30 is directly connected, ATM3/0.3
C    172.24.1.0/30 is directly connected, ATM3/0.1
C    172.24.0.1/32 is directly connected, Loopback0
O    172.24.2.0/30 [110/196] via 172.24.1.1, 03:37:55, ATM3/0.1
O    172.24.0.2/32 [110/2] via 172.24.1.1, 03:37:55, ATM3/0.1
O    172.24.0.3/32 [110/2] via 172.24.1.17, 03:37:55, BUI1
O    172.24.1.8/30 [110/2] via 172.24.1.17, 03:37:55, BUI1
     [110/2] via 172.24.1.1, 03:37:55, ATM3/0.1
O IA 172.24.97.0/24 [110/11] via 172.24.1.17, 03:37:55, BUI1
B    172.31.0.0/16 [20/0] via 172.24.2.6, 4d16h
S*   0.0.0.0/0 [1/0] via 172.24.2.6
Chicago-ISP-1#
```

Routage avec les adresses IP (suite)

- Route à partir d'un PC (tracert)



```
C:\>tracert 172.24.0.1

Tracing route to 172.24.0.1 over a maximum of 30 hops

  1    20 ms    30 ms    30 ms    172.16.1.3
  2   <10 ms   <10 ms   <10 ms   172.31.4.4
  3   <10 ms   <10 ms   <10 ms   172.24.0.1

Trace complete.

C:\>tracert www.polymtl.ca

Tracing route to www.polymtl.ca [132.207.4.56]
over a maximum of 30 hops:

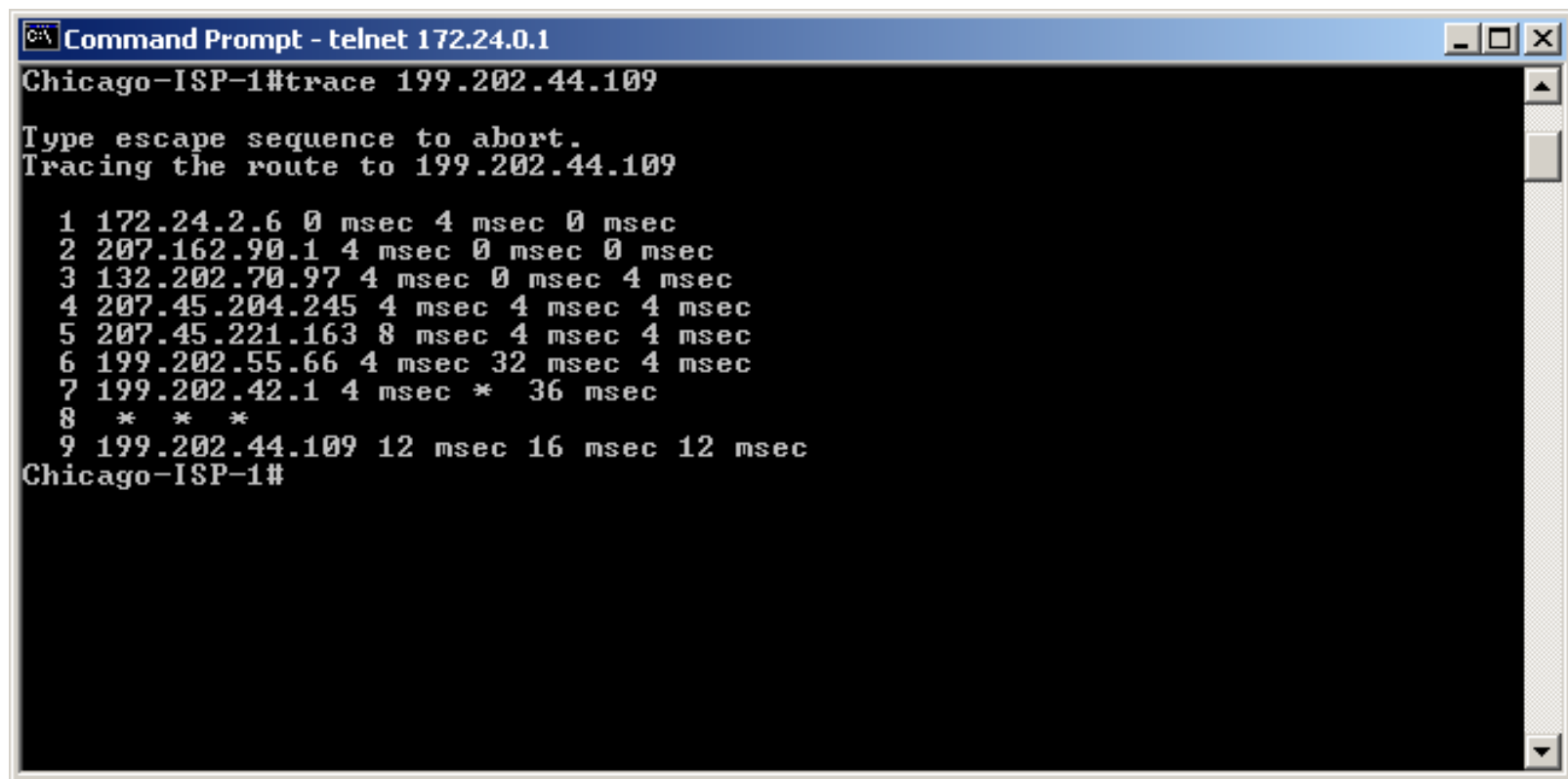
  1    10 ms    <10 ms    <10 ms    172.16.1.3
  2   <10 ms    <10 ms    <10 ms    207.162.90.1
  3   <10 ms    <10 ms    10 ms     uqam4-gw.risq.net [132.202.223.73]
  4   <10 ms    <10 ms    <10 ms    polymtl-gw.risq.net [132.202.249.146]
  5   <10 ms    10 ms     10 ms     www.polymtl.ca [132.207.4.56]

Trace complete.

C:\>
```


Routage avec les adresses IP (suite)

- Route à partir d'un routeur Cisco (trace)



```
Command Prompt - telnet 172.24.0.1
Chicago-ISP-1#trace 199.202.44.109
Type escape sequence to abort.
Tracing the route to 199.202.44.109

 0 172.24.2.6 0 msec 4 msec 0 msec
 1 207.162.90.1 4 msec 0 msec 0 msec
 2 132.202.70.97 4 msec 0 msec 4 msec
 3 207.45.204.245 4 msec 4 msec 4 msec
 4 207.45.221.163 8 msec 4 msec 4 msec
 5 199.202.55.66 4 msec 32 msec 4 msec
 6 199.202.42.1 4 msec * 36 msec
 7 * * *
 8 199.202.44.109 12 msec 16 msec 12 msec
Chicago-ISP-1#
```

Format du paquet IP

- L'entête du paquet IP se retrouve au début de chaque paquet IP.
- L'entête contient des champs de longueur fixe et variable.
- Chaque champ à un rôle bien spécifique à jouer.

0	3 4	7 8	1 1 5 6	1 9	2 2 2 3	3 1
VERS	IHL	TOS	TOTAL LENGTH			
IDENTIFICATION			FLAGS	FRAGMENT OFFSET		
TTL		PROTOCOL	HEADER CHECKSUM			
Adresse IP d'origine						
Adresse IP de destination						
OPTION					Remplissage	
Données						
...						

Format du paquet IP (suite)

- Les champs du IP PDU sont
 - VERS (*Version*) : indique la version du paquet IP. Chaque routeur doit vérifier la version avant de traiter le paquet. Actuellement $VERS = 4$.
 - IHL (*IP Header Length*) : indique la longueur de l'entête en mots de 32 bits. La longueur la plus fréquente est $IHL = 5$. En fait $IHL = 5 + N$ où N est le nombre de mots utilisés par le champ OPTION.

Format du paquet IP (suite)

- Les champs du IP PDU (suite)

- TOS (*Type of Service*) : Ce champ caractérise le mode de transport du paquet selon une série de variables.

Le champ TOS contient trois sous-champs: PRECEDENCE (3 bits), TOS (4 bits) et MBZ (1 bit). MBZ signifie *Must Be Zero*.



Format du paquet IP (suite)

- Les champs du IP PDU (suite)
 - TOS (suite):

PRECEDENCE			Signification
1	1	1	Network Control
1	1	0	Internetwork Control
1	0	1	Critical
1	0	0	Flash override
0	1	1	Flash
0	1	0	Immediate
0	0	1	Priority
0	0	0	Routine

TOS				Signification
0	0	0	0	Normal
0	0	0	1	Minimize cost
0	0	1	0	Maximize reliability
0	1	0	0	Maximize throughput
1	0	0	0	Minimize delay

Le champ MBZ = 0

Format du paquet IP (suite)

- Les champs du IP PDU (suite)

- TOTAL LENGTH : indique la longueur totale du paquet IP en octets. Cela comprend l'entête et les données.

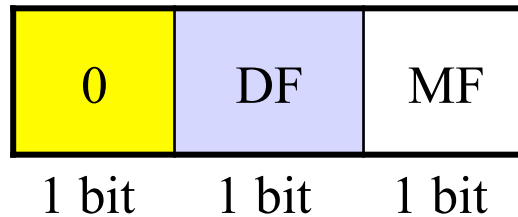
Ainsi la longueur maximale d'un paquet IP est de 65 535 octets.

- IDENTIFICATION : Ce champ est utilisé par la destination pour reconstituer le message au niveau supérieur.

Chaque paquet comporte un numéro d'identification spécifique. Dans le cas d'une fragmentation, le numéro du paquet est copié dans chaque fragment.

Format du paquet IP (suite)

- Les champs du IP PDU (suite)
 - **FLAGS** : Champ utilisé pour insérer de l'information quant à la fragmentation du paquet (datagramme) au niveau de la couche 2.



DF = *Don't Fragment*

MF = *More Fragment*

DF = 1 indique que le paquet ne doit pas être fragmenté.

MF = 1 indique d'autres fragments à venir.

Format du paquet IP (suite)

- Les champs du IP PDU (suite)

- **FRAGMENT OFFSET** : ce champ indique la position du fragment dans le datagramme IP. Il est utilisé pour réassembler le paquet et pour détecter les fragments manquants.

La valeur du champ correspond au décalage (dans le datagramme assemblé) du premier octet de données à partir du champ de données de ce fragment.

La valeur de ce décalage est exprimée en unité de 8 octets.

Tous les fragment, sauf le dernier, ont un drapeau MF = 1.

Format du paquet IP (suite)

- Les champs du IP PDU (suite)

- TTL (*Time to Live*) : ce champ indique la durée maximale de transit d'un paquet IP dans le réseau.

La durée de vie est représentée par un compteur qui est décrémenté de un à chaque routeur (la plupart des routeurs ne supportent pas la décrémentation en secondes).

Par exemple, pour Windows 95 le champ TTL est de 32, 128 pour NT4.0 et Windows 7, ainsi que 255 pour XP.

Format du paquet IP (suite)

- Les champs du IP PDU (suite)
 - **PROTOCOL** : ce champ indique le type de protocole qui est encapsulé dans le paquet IP.

Valeur du champ PROTOCOL (décimal)	Acronyme	Protocole
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
6	TCP	Transport Control
17	UDP	User Datagram

Format du paquet IP (suite)

- Les champs du IP PDU (suite)

- **HEADER CHECKSUM** : Code pour faire la détection d'erreur dans l'entête du paquet IP.

La réception d'un paquet avec un mauvais CHECKSUM entraîne sa destruction.

- **Adresse IP d'origine/destination** : ce champ spécifie l'adresse IP source (d'où provient le paquet) et l'adresse IP de destination (où va le paquet).
- **OPTION** : le champ des option peut être omis. En général, il est utilisé pour des besoins de vérification et de déverminage.

Format du paquet IP (suite)

- Exemple : champs d'un IP PDU

Flags: 0x00
Status: 0x00
Packet Length: 340
Timestamp: 16:09:33.582686 02/27/2002

Ethernet Header

Destination: 00:90:6D:F2:C8:00
Source: 00:50:BA:79:0F:EB
Protocol Type: 0x0800 IP

IP Header - Internet Protocol Datagram

Version: 4
Header Length: 5 (20 bytes)
Type of Service: %00000000
Precedence: Routine, Normal Delay, Normal Throughput, Normal Reliability
Total Length: 322
Identifier: 4631
Fragmentation Flags: %010 *Do Not Fragment Last Fragment*
Fragment Offset: 0 (0 bytes)
Time To Live: 128
Protocol: 6 TCP
Header Checksum: 0x13A1
Source IP Address: 132.207.92.122
Dest. IP Address: 208.48.34.132
No IP Options

TCP - Transport Control Protocol

Source Port: 1384
Destination Port: 80 *World Wide Web HTTP*
Sequence Number: 831861752
Ack Number: 1883895931
Offset: 5
Reserved: %000000
Code: %011000
*Ack is valid
Push Request*

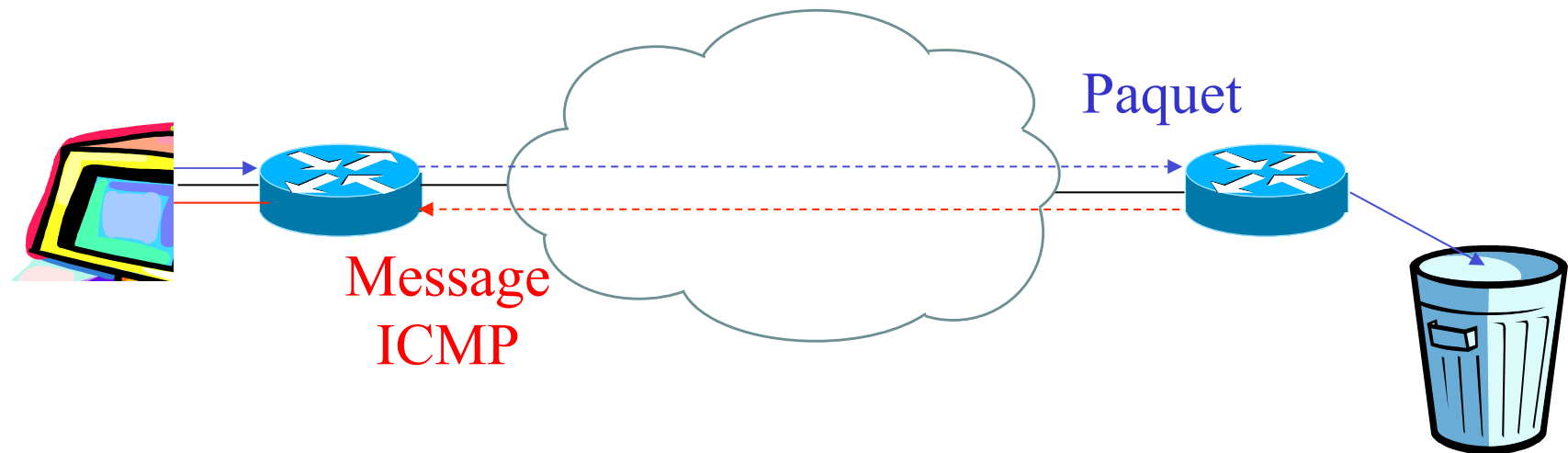
Window: 17143
Checksum: 0xB800
Urgent Pointer: 0
No TCP Options

HTTP - HyperText Transfer Protocol

GET /images/logo 47 45 54 20 2F 69 6D 61 67 65 73 2F 6C 6F 67 6F
.jpg HTTP/1.1.. 2E 6A 70 67 20 48 54 54 50 2F 31 2E 31 0D 0A
Accept: */*.. 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A
Referer: http:// 52 65 66 65 72 65 72 3A 20 68 74 74 70 3A 2F 2F
www.test.com/.. 77 77 77 2E 74 65 73 74 2E 63 6F 6D 2F 0D 0A
Accept-Language: 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A
en-ca.. 20 65 6E 2D 63 61 0D 0A
Accept-Encoding: 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A
gzip, deflate.. 20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 0D 0A
User-Agent: Mozi 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69
lla/4.0 (compati 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 61 74 69
ble; MSIE 5.01; 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 31 3B 20
Windows NT 5.0). 57 69 6E 64 6F 77 73 20 4E 54 20 35 2E 30 29 0D
. 0A
Host: www.test.c 48 6F 73 74 3A 20 77 77 77 2E 74 65 73 74 2E 63
om.. 6F 6D 0D 0A
Connection: Keep 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70
-Alive.. 2D 41 6C 69 76 65 0D 0A
Cookie: jsession 43 6F 6F 6B 69 65 3A 20 6A 73 65 73 73 69 6F 6E
id=1880481014844 69 64 3D 31 38 38 30 34 38 31 30 31 34 38 34 34
393765.. 33 39 33 37 36 35 0D 0A
.. 0D 0A
Frame Check Sequence: 0x00000000

ICMP

- Comme le protocole IP ne garantit pas la livraison des paquets, cette responsabilité est laissée aux couches supérieures.
- Cependant, le protocole IP fournit un moyen d'envoyer des alertes et des messages de diagnostic en utilisant le protocole ICMP (*Internet Control Message Protocol*).
- ICMP est définie dans le RFC 792.

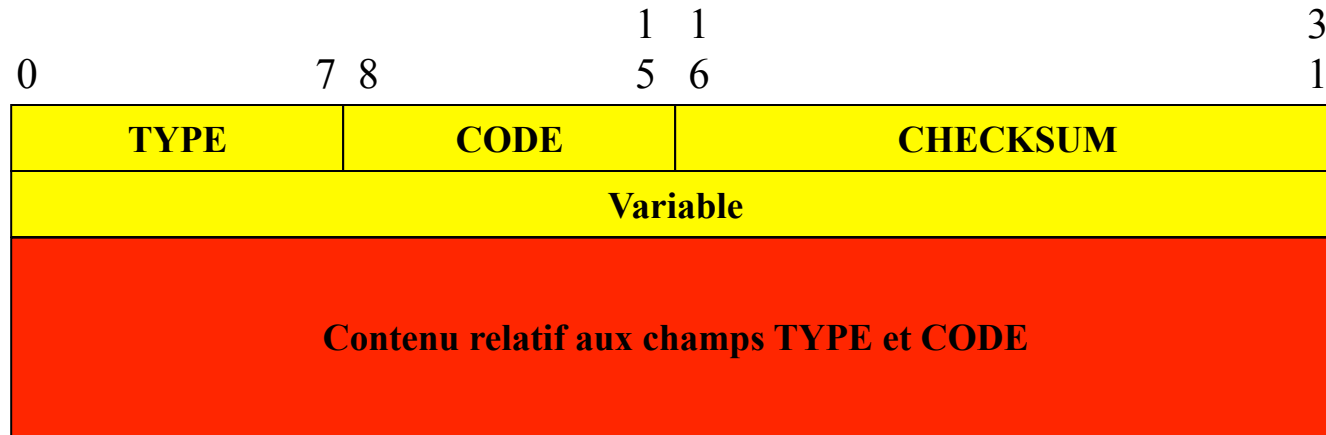


ICMP (suite)

- Les messages ICMP sont divisés en deux catégories :
 - messages d'erreurs
 - messages de requêtes/réponses.
- Un message d'erreur ICMP n'est pas envoyé en réponse à :
 - un message d'erreur ICMP; il est toutefois envoyé dans le cas d'un message de requête/réponse ;
 - un datagramme destiné à une adresse « broadcast » ou « multicast » ;
 - un fragment IP autre que le premier.

ICMP (suite)

- La structure d'un message ICMP



- Lorsque ICMP est utilisé, le champ PROTOCOL dans l'entête IP est 1.
- Le champ TYPE détermine la fonction du message.
- Le champ CODE dépend du champ type.
- Le champ CHECKSUM est un code de détection d'erreur.

ICMP (suite)

- Valeurs courantes du champ TYPE

TYPE	Fonction
0	Echo reply (réponse d'écho)
3	Destination unreachable (destination inaccessible)
5	Redirect (redirection)
8	Echo request (demande d'écho)
11	Time exceeded (expiration de délai)
12	Parametre problem (problème de paramètre)
13	Timestamp request (demande d'estampille de temps)
14	Timestamp reply (réponse d'estampille de temps)
15	Information request (demande d'informations)
16	Information reply (réponse d'informations)
17	Address mask request (demande de masque)
18	Address mask reply (réponse de masque)

ICMP (suite)

Pour les messages d'erreurs ICMP, le « contenu » du message inclut les éléments suivants :

- l'entête IP (20 octets) ;
- les options IP (0-40 octets) ;
- les huit premiers octets du champ des données.

Parmi les huit premiers octets du champ des données, on retrouve les numéros de ports utilisés pour TCP ou UDP.

Ces ports indiquent à quelle application le paquet appartient.

ICMP (suite)

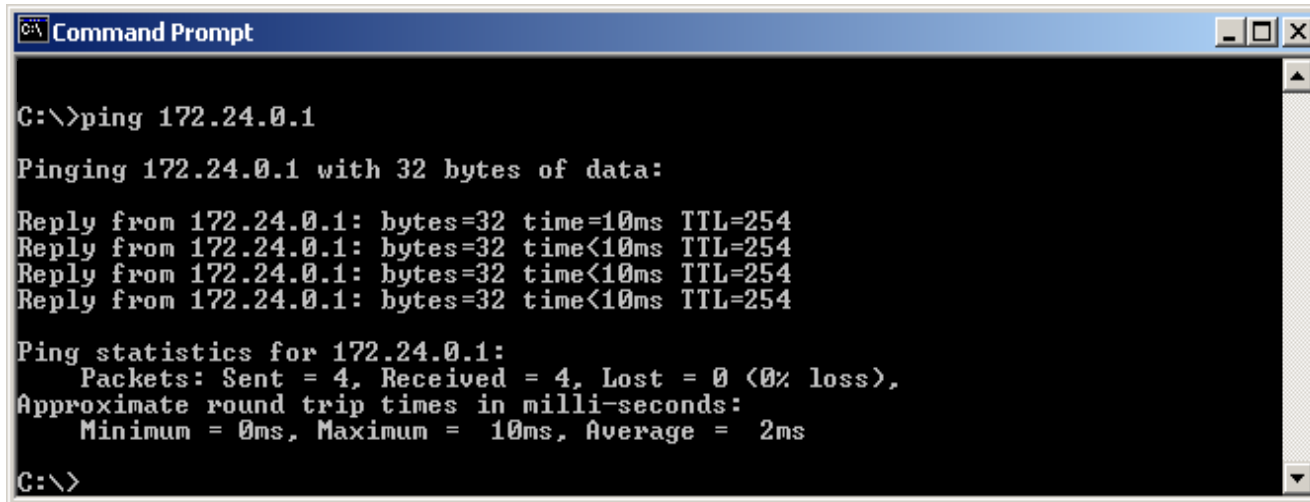
- Exemple: ICMP « Echo request » et « Echo reply »
 - La structure d'un message ICMP « Echo request/reply » est la suivante.

TYPE = 0 ou 8	CODE = 0	CHECKSUM
Identificateur		Numéro de séquence
Données		

- Identificateur : nombre arbitraire permettant d'associer un « request » à un « reply ».
- Numéro de séquence : compteur incrémenté après la réception d'un « reply ».
- Données : utilisé pour faire varier la taille du datagramme.

ICMP (suite)

- Exemple: ICMP « Echo request » et « Echo reply » (suite)
 - Application : la commande PING (ping 172.24.0.1)



```
Command Prompt

C:\>ping 172.24.0.1

Pinging 172.24.0.1 with 32 bytes of data:

Reply from 172.24.0.1: bytes=32 time=10ms TTL=254
Reply from 172.24.0.1: bytes=32 time<10ms TTL=254
Reply from 172.24.0.1: bytes=32 time<10ms TTL=254
Reply from 172.24.0.1: bytes=32 time<10ms TTL=254

Ping statistics for 172.24.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>
```

ICMP (suite)

- Exemple: ICMP « Echo request » et « Echo reply » (suite)
 - Application : la commande PING (ping 132.207.92.177): « Echo request »

```
Flags:      0x00
Status:     0x00
Packet Length: 78
Timestamp:  16:39:31.815894 02/27/2002
Ethernet Header
Destination: 00:50:04:AC:69:69
Source:      00:50:BA:79:0F:EB
Protocol Type: 0x0800  IP
IP Header - Internet Protocol Datagram
Version:     4
Header Length: 5 (20 bytes)
Type of Service: %00000000
Precedence: Routine, Normal Delay, Normal Throughput, Normal Reliability
Total Length: 60
Identifier:  133
Fragmentation Flags: %000 May Fragment Last Fragment
Fragment Offset: 0 (0 bytes)
Time To Live: 128
Protocol:    1  ICMP
Header Checksum: 0x77C4
Source IP Address: 132.207.92.40
Dest. IP Address: 132.207.92.177
No IP Options
ICMP - Internet Control Messages Protocol
ICMP Type:   8  Echo Request
Code:        0
Checksum:    0x495C
Identifier:  0x0200
Sequence Number: 512
ICMP Data Area:
abcdefghijklmnop 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70
qrstuvwxyzab 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69
```

ICMP (suite)

- Exemple: ICMP « Echo request » et « Echo reply » (suite)
 - Application : la commande PING (ping 132.207.92.177): « Echo reply »

```
Flags:          0x00
Status:         0x00
Packet Length: 78
Timestamp:      16:39:31.816586 02/27/2002
Ethernet Header
Destination:    00:50:BA:79:0F:EB
Source:         00:50:04:AC:69:69
Protocol Type:  0x0800  IP
IP Header - Internet Protocol Datagram
Version:        4
Header Length:  5 (20 bytes)
Type of Service: %00000000
Precedence: Routine, Normal Delay, Normal Throughput, Normal Reliability
Total Length:   60
Identifier:     47906
Fragmentation Flags: %000 May Fragment Last Fragment
Fragment Offset: 0 (0 bytes)
Time To Live:   128
Protocol:       1 ICMP
Header Checksum: 0xBD26
Source IP Address: 132.207.92.177
Dest. IP Address: 132.207.92.40
No IP Options
ICMP - Internet Control Messages Protocol
ICMP Type:      0 Echo Reply
Code:           0
Checksum:       0x515C
Identifier:      0x0200
Sequence Number: 512
ICMP Data Area:
abcdefghijklmnop 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70
rstuvwxyzabcdefghi 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69
```

ICMP (suite)

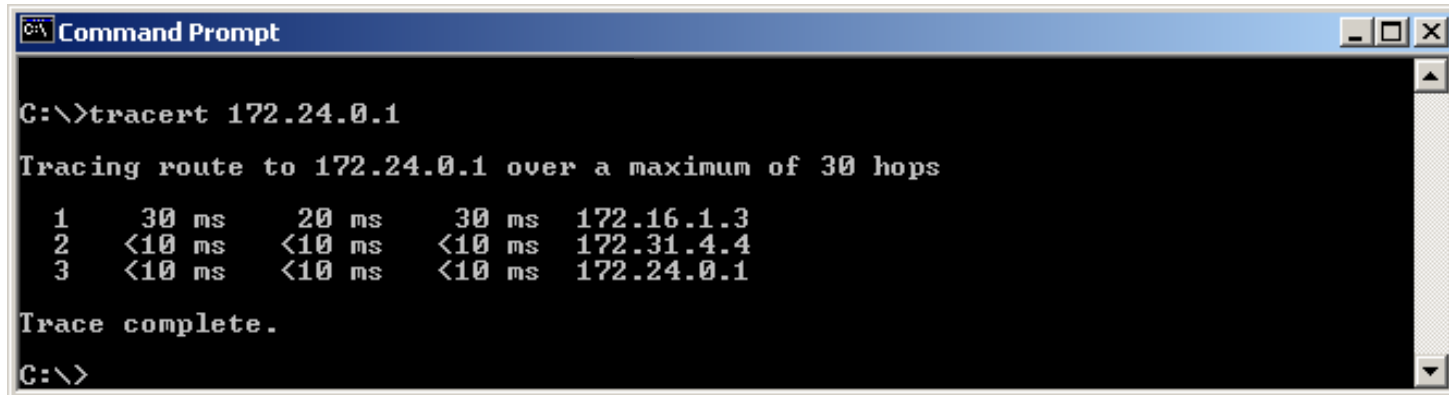
- Exemple: ICMP « Time exceeded »
- La structure d'un message ICMP « Time exceeded » est la suivante.

TYPE = 11	CODE = 0 ou 1	CHECKSUM
0		
Entête IP + 8 octets du champ de données du paquet IP		

- CODE = 0 : la durée de vie du paquet est expirée.
- CODE = 1 : le temps d'attente pour rassembler les fragments est expiré.

ICMP (suite)

- Exemple: ICMP « Time exceeded » (suite)
 - Application : la commande TRACERT (tracert 172.24.0.1)



```
Command Prompt

C:\>tracert 172.24.0.1

Tracing route to 172.24.0.1 over a maximum of 30 hops

  1    30 ms    20 ms    30 ms  172.16.1.3
  2   <10 ms   <10 ms   <10 ms  172.31.4.4
  3   <10 ms   <10 ms   <10 ms  172.24.0.1

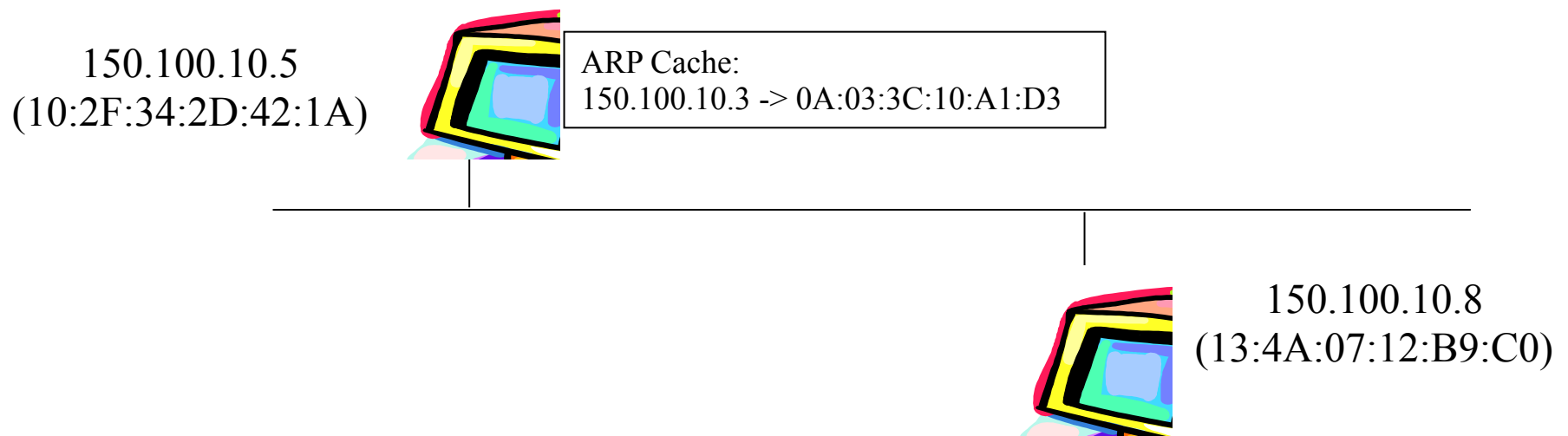
Trace complete.

C:\>
```

Note : tracert (DOS), traceroute (UNIX), trace (Cisco).

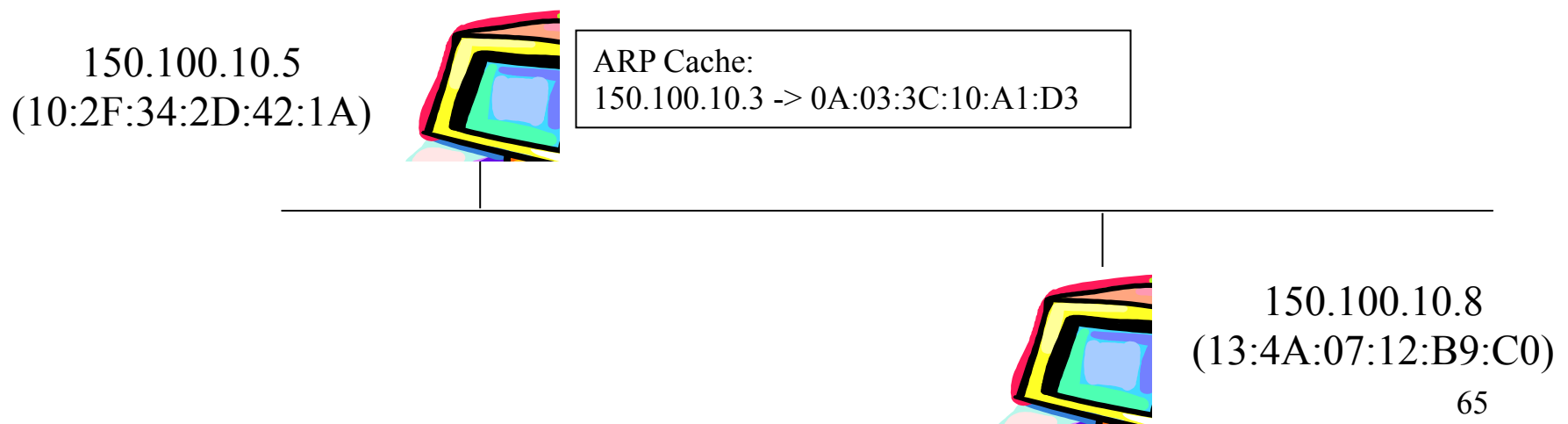
ARP

- Le protocole de résolution d'adresse ARP (*Address Resolution Protocol*) permet d'associer une adresse IP à une adresse de niveau 2, par exemple, une adresse MAC.
- Fonctionnement de l'ARP (RFC 826) par un exemple.
 - L'utilisateur de la station 150.100.10.5 fait un PING pour savoir si la station 150.100.10.8 est dans le réseau.



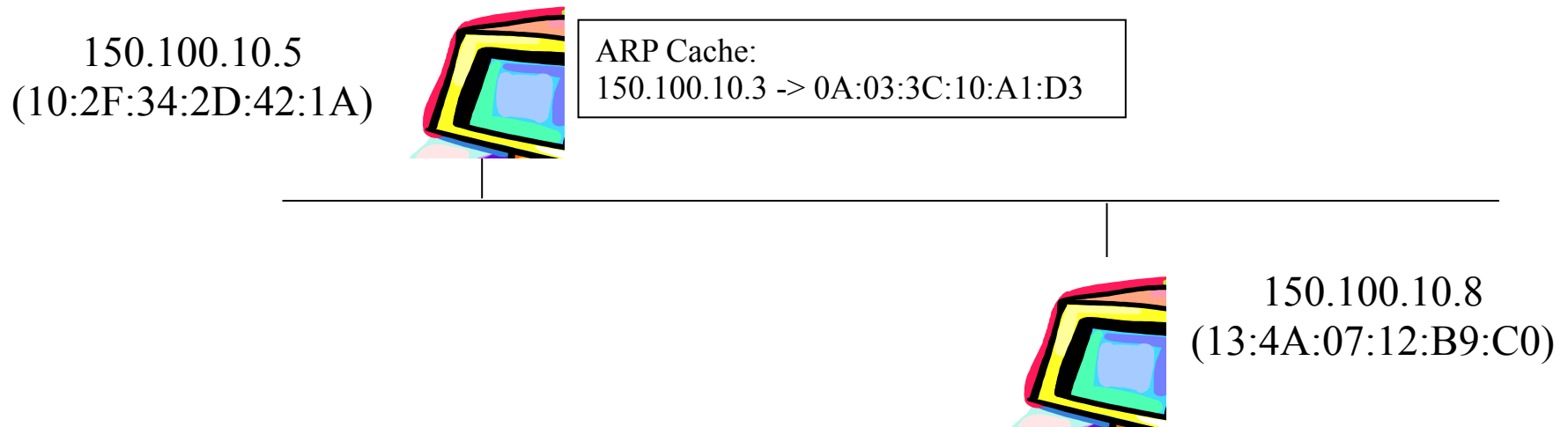
ARP (suite)

- Fonctionnement de l'ARP par un exemple (suite)
 - La commande PING envoie un message ICMP au module IP.
 - Le module IP vérifie si l'adresse IP de destination est dans le même réseau local.
 - Le module IP demande au module ARP l'adresse MAC correspondante à l'adresse IP de destination 150.100.10.8.



ARP (suite)

- Fonctionnement de l'ARP par un exemple (suite)
 - Le module ARP vérifie dans sa table (ARP Cache) s'il connaît l'adresse.
 - La table se bâtit au fur et à mesure que le module IP demande une adresse physique de destination. La durée des entrées dans la table varie en fonction des implantations (quelques minutes).



ARP (suite)

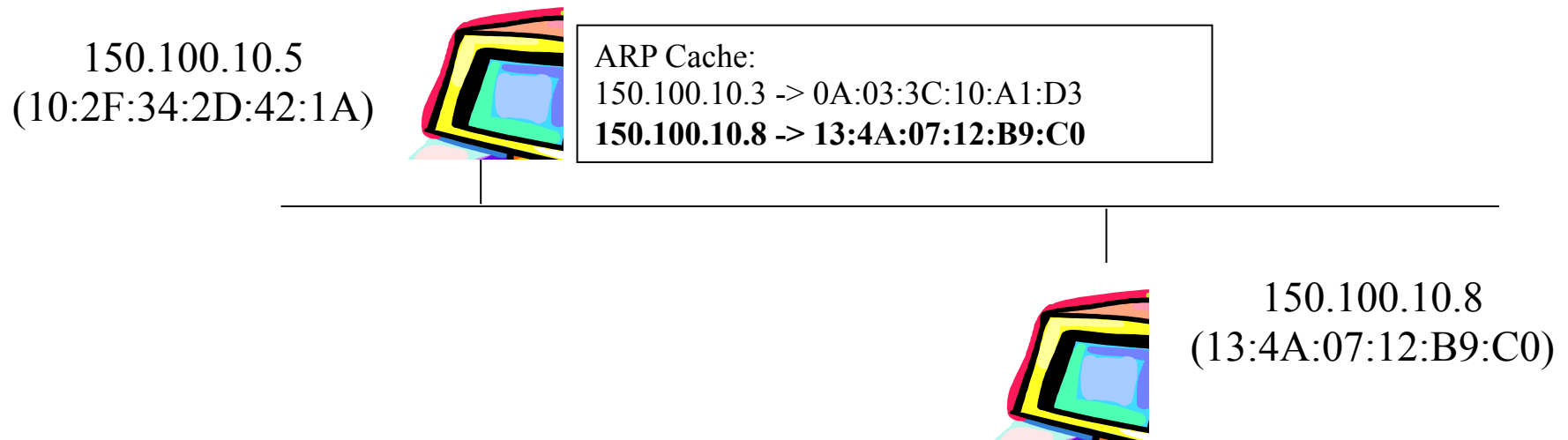
- Fonctionnement de l'ARP par un exemple (suite)
 - Le module ARP constate que l'adresse n'est pas dans sa table. Il envoie un paquet au module Ethernet avec comme information
 - Un ARP « request »
 - L'adresse Ethernet de la source (10:2F:34:2D:42:1A)
 - L'adresse IP de la source (150.100.10.5) et de la cible (150.100.10.8).
 - Le module Ethernet envoie le message à tous les ordinateurs sur le segment local Ethernet (FF:FF:FF:FF:FF:FF qui est l'adresse « broadcast » de Ethernet).
 - Le module Ethernet de la station 150.100.10.8 reçoit le message et le retourne à la couche supérieure.

ARP (suite)

- Fonctionnement de l'ARP par un exemple (suite)
 - Le module ARP récupère le paquet et constate que le message est un ARP « request » qui lui est destiné.
 - Le module ARP envoie un « reply » avec les informations suivantes
 - L'adresse Ethernet (13:4A:07:12:B9:C0) et IP (150.100.10.8) de la source.
 - L'adresse Ethernet (10:2F:34:2D:42:1A) et IP (150.100.10.5) de la destination.
 - Le module Ethernet retourne le paquet au poste 150.100.10.5.
 - Le module Ethernet retourne le paquet à la couche supérieure. Le module ARP constate que le paquet est un « reply » au « request » précédent.

ARP (suite)

- Fonctionnement de l'ARP par un exemple (suite)
 - Le module ARP retourne au module IP l'adresse Ethernet correspondant à l'adresse IP de destination.
 - Le module ARP met sa table à jour.
 - Le message ICMP est envoyé via le module Ethernet.



ARP (suite)

- Description d'un paquet ARP

HARDWARE		PROTOCOL
HLEN	PLEN	OPERATION
Sender hardware address ...		
... Sender hardware address		Sender protocol address ...
... Sender protocol address		... Target hardware address
... Target hardware address		
Target protocol address		

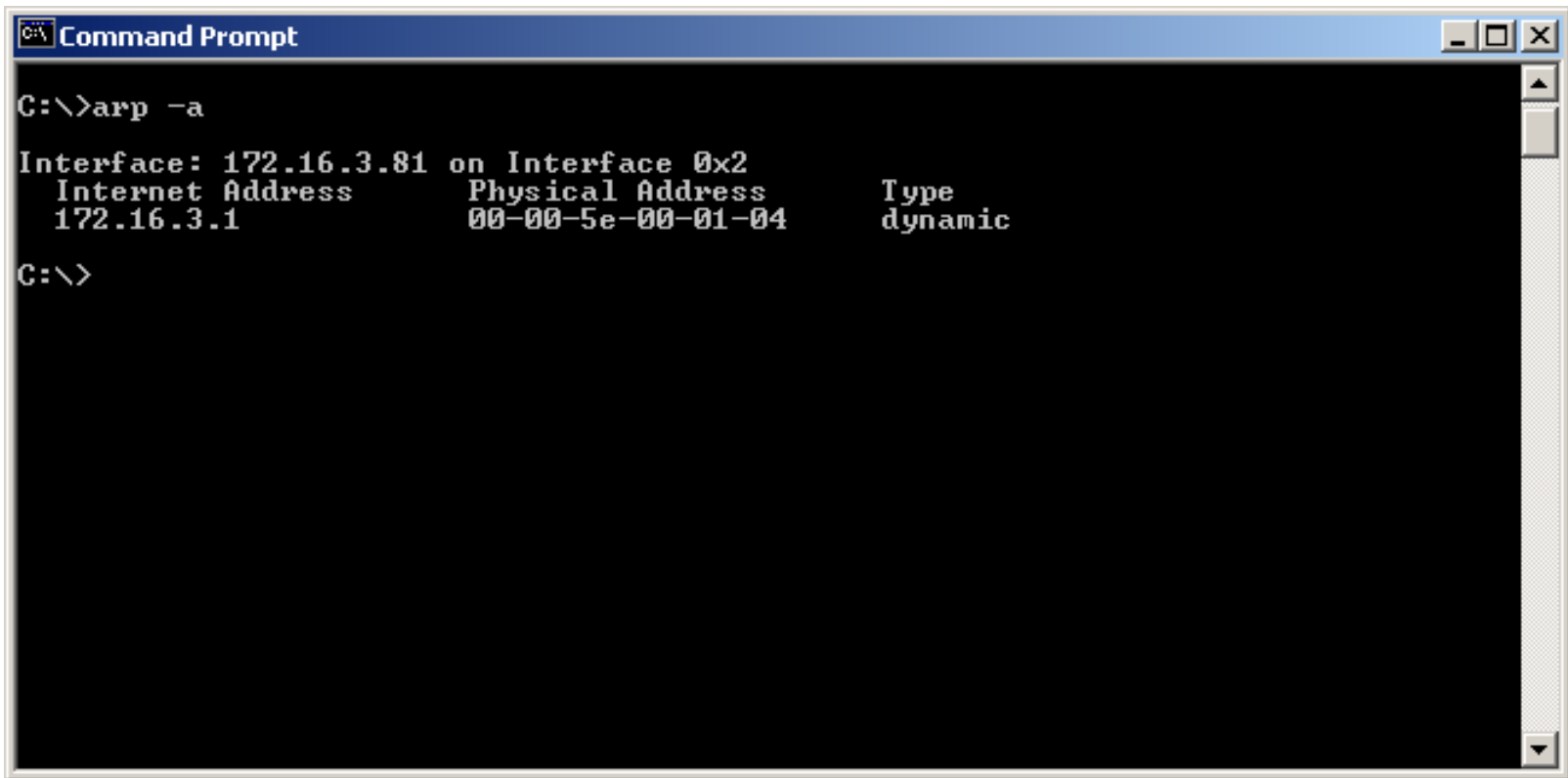
- **HARDWARE** : identifie le type d'interface physique. **HARDWARE** = 1 pour Ethernet.
- **PROTOCOL** : identifie le type d'adresse que le protocole utilise. **PROTOCOL** = 0x0800 pour IP.
- **HLEN** et **PLEN** : indiquent la longueur de l'adresse physique et du protocole respectivement. **HLEN** = 6 pour Ethernet et **PLEN** = 4 pour IP.

ARP (suite)

- Description d'un paquet ARP (suite)
 - OPERATION
 - 1: ARP « request »
 - 2: ARP « reply »
 - 3: RARP « request »
 - 4: RARP « reply ».
 - Les autres champs sont les adresses physique et protocole de la source et la cible.

ARP (suite)

- Commande arp -a (DOS) pour déterminer les adresses dans la liste ARP.



```
C:\>arp -a

Interface: 172.16.3.81 on Interface 0x2
  Internet Address      Physical Address      Type
  172.16.3.1            00-00-5e-00-01-04     dynamic

C:\>
```

The screenshot shows a Windows Command Prompt window with a blue title bar labeled "Command Prompt". The command prompt displays the output of the 'arp -a' command. It shows the interface IP address 172.16.3.81 and the physical address 00-00-5e-00-01-04 for the interface 0x2. The output is formatted as a table with three columns: Internet Address, Physical Address, and Type. The Type is listed as dynamic. The prompt ends with 'C:\>'.

ARP (suite)

- Trame ARP « request »

Flags: 0x00
Status: 0x00
Packet Length: 64
Timestamp: 16:26:09.536295 02/27/2002

Ethernet Header

Destination: FF:FF:FF:FF:FF:FF *Ethernet Broadcast*
Source: 00:04:75:70:D1:25
Protocol Type: 0x0806 *IP ARP*

ARP - Address Resolution Protocol

Hardware: 1 *Ethernet (10Mb)*
Protocol: 0x0800 *IP*
Hardware Address Length: 6
Protocol Address Length: 4
Operation: 1 *ARP Request*
Sender Hardware Address: 00:04:75:70:D1:25
Sender Internet Address: 132.207.92.140
Target Hardware Address: 00:00:00:00:00:00 *(ignored)*
Target Internet Address: 132.207.92.103

Extra bytes (Padding):

..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.. 00 00

Frame Check Sequence: 0x00000000

ARP (suite)

- Trame ARP « response »

Flags: 0x00
Status: 0x00
Packet Length: 64
Timestamp: 16:47:03.191102 02/27/2002

Ethernet Header

Destination: 00:50:BA:79:0F:EB
Source: 00:50:BA:76:DC:B1
Protocol Type: 0x0806 IP ARP

ARP - Address Resolution Protocol

Hardware: 1 Ethernet (10Mb)
Protocol: 0x0800 IP
Hardware Address Length: 6
Protocol Address Length: 4
Operation: 2 ARP Response
Sender Hardware Address: 00:50:BA:76:DC:B1
Sender Internet Address: 132.207.92.103
Target Hardware Address: 00:04:75:70:D1:25
Target Internet Address: 132.207.92.140

Extra bytes (Padding):

20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20

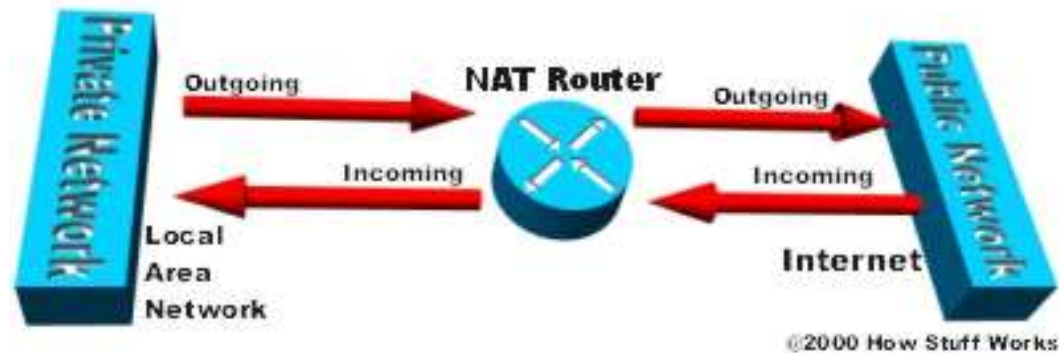
Frame Check Sequence: 0x00000000

NAT

- NAT – Network Address Translation
- Fonction dans routeur d'accès (entre site et Internet)
- Traduit les adresses IP
 - Modifie l'entête des datagrammes IP échangés avec l'extérieur
 - Dans les sens sortant et entrant
- Une station du site
 - Possède une adresse interne 10.1.1.2
 - Elle est configurée avec cette adresse
 - Les machines internes communiquent avec elle avec cette adresse
 - Connue de l'extérieur avec l'adresse 193.96.49.64 (@ externe)
 - Les machines de l'Internet communiquent avec elle avec cette adresse
- Le système est transparent pour les stations
- Le routeur entre le site et l'Internet fait la traduction

NAT

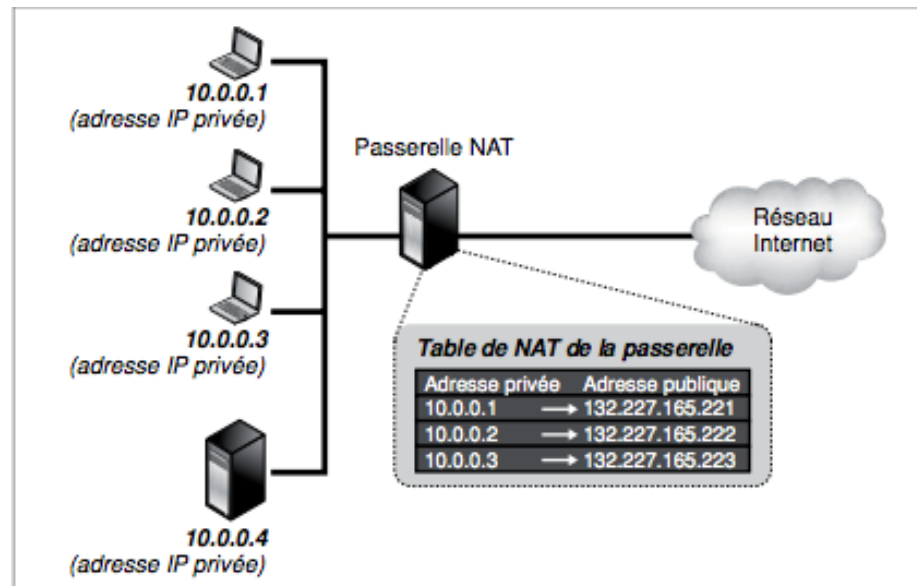
- NAT est définie dans le RFC 1631.
- Par exemple



Source : Cisco

Le NAT statique

Dans le NAT statique, à toute adresse IP privée qui communique avec l'extérieur, une adresse IP publique fixe lui est affectée. Avec ce type de NAT, les utilisateurs du réseau local sont joignables de l'extérieur, car la passerelle réalise la correspondance d'une adresse IP locale en une adresse IP publique dans les deux sens.



Le NAT dynamique

Avec le NAT dynamique, une plage d'adresses IP publiques est disponible et partagée par tous les utilisateurs du réseau local.

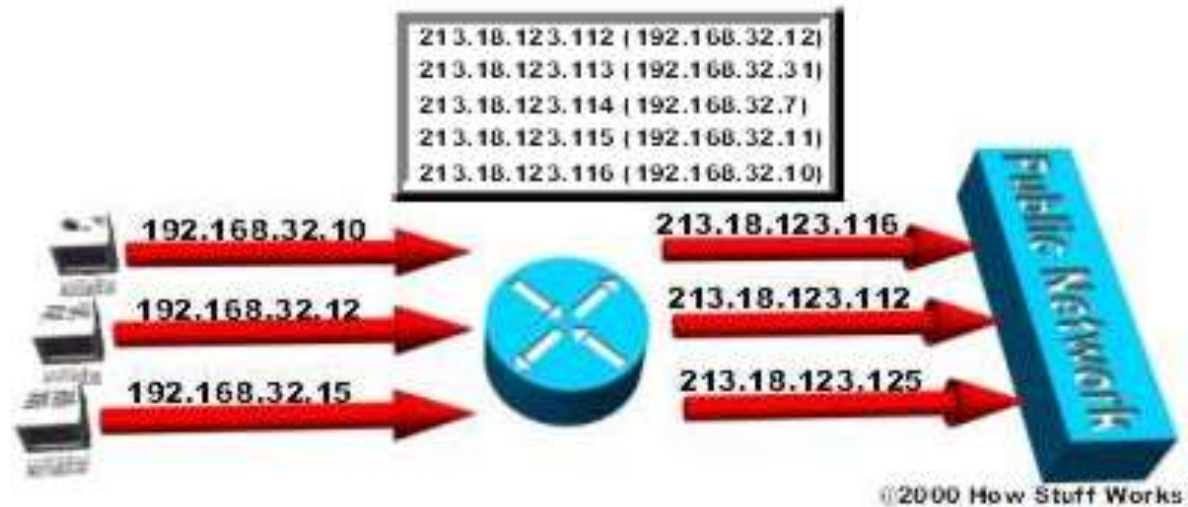
Chaque fois qu'une demande d'un utilisateur local (avec une adresse privée) parvient à la passerelle NAT, celle-ci lui concède dynamiquement une adresse IP publique.

Les utilisateurs locaux ne sont joignables de l'extérieur que s'ils ont une entrée dans la table de la passerelle NAT.

Si une machine interne n'a pas d'activité réseau, aucune entrée ne lui est attribué dans la table de NAT.

L'adresse IP qui leur est affectée est temporaire et peut être différente à la prochaine connexion.

Le NAT dynamique



Le NAPT (Network Address Port Translation)

Il consiste à attribuer une même adresse IP à plusieurs utilisateurs d'un même réseau local.

Pour associer une même adresse IP publique à deux machines ayant une adresse privée distincte, la passerelle NAT joue sur les ports des applications : une requête envoyée à partir du port A d'une source est retransmise avec le port B de la passerelle, tandis qu'une requête émise à partir du port C d'une autre source est retransmise avec le port D de la passerelle.

Seuls les utilisateurs du réseau local peuvent commencer une communication vers l'extérieur.

Le NAPT est la méthode la plus utilisée puisqu'elle permet de masquer tout un réseau local avec une seule adresse IP.

NAT (suite)

- La fonction NAT utilise les ports définis dans TCP et UDP pour associer les paquets entrants dans le réseau local (ayant la même adresse IP publique dans l'entête) vers le bon ordinateur dans le réseau local.
- Dans l'exemple, la passerelle NAT pourrait utiliser les correspondances suivantes.

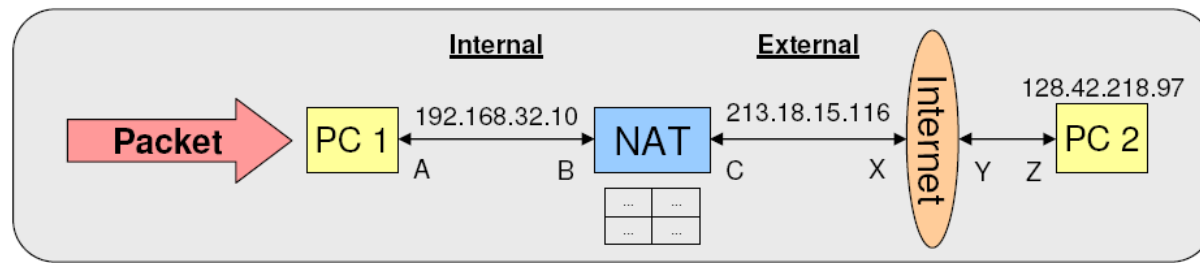
Adresse IP de la source	Port (source et destination)	Nouvelle adresse IP (utilisée dans l'Internet)	Nouveau port (source)
10.0.0.2	80 (HTTP)	157.55.0.1	2000
10.0.0.3	20 (FTP)	157.55.0.1	2001
10.0.0.2	23 (Telnet)	157.55.0.1	2002

NAT : avantages et inconvénients

- Avantages
 - On dispose d'un espace d'adresses énorme en interne
 - Pas de limitation dans l'architecture des sous réseaux
 - Pas de problème quand nouvelles stations à numéroté
 - Les stations clientes ont des @ IP dynamiques
 - Plus difficiles à attaquer : meilleure sécurité
- Désavantages
 - Sécurité : les stations clientes sont « anonymes »
 - Difficile de savoir quelle station interne a attaqué un site externe
 - Coupe le principe IP de connectivité de bout en bout
 - Retarde l'arrivée de IPv6

NAT

NAT Mechanics – Outbound Packet



Ethernet Header				IP Header				Data	
Dst MAC	Src MAC	IP Csum	Src IP	Dst IP	...	Payload	CRC

Before NAT (internal network)

<i>B</i>	<i>A</i>	<i>IP Csum</i>	<i>PC 1</i>	<i>PC 2</i>	...	<i>Payload</i>	<i>CRC</i>
----------	----------	-----	-----	----------------	-------------	-------------	-----	----------------	------------

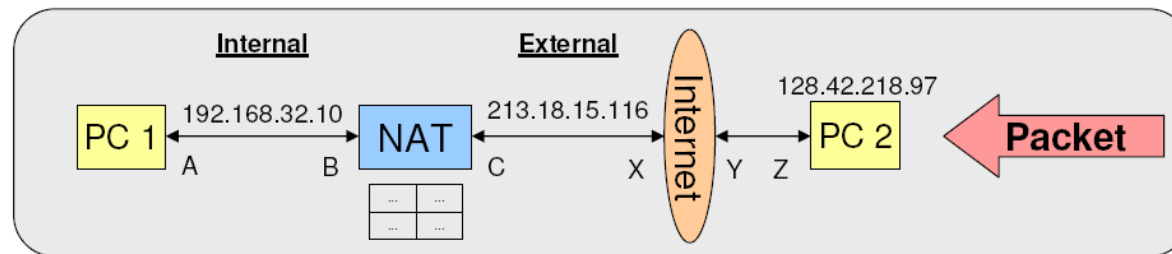
After NAT (external network)

<i>X</i>	<i>C</i>	<i>IP Csum</i>	<i>NAT</i>	<i>PC 2</i>	...	<i>Payload</i>	<i>CRC</i>
----------	----------	-----	-----	----------------	------------	-------------	-----	----------------	------------

- Save internal IP and MAC to mapping table
- Replace source IP and MAC with NAT unit
- Recalculate checksums (Ethernet CRC, IP header, TCP/UDP/... headers)

NAT

NAT Mechanics – Inbound Packet



Ethernet Header				IP Header				Data	
Dst MAC	Src MAC	IP Csum	Src IP	Dst IP	...	Payload	CRC

Before NAT (external network)

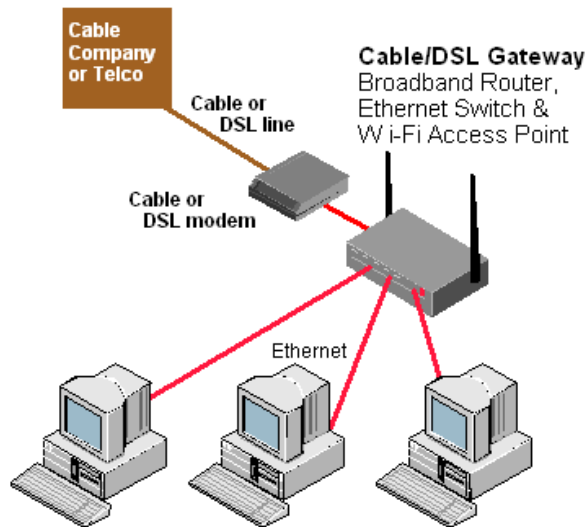
C	X	IP Csum	PC 2	NAT	...	Payload	CRC
---	---	-----	-----	---------	------	-----	-----	---------	-----

After NAT (internal network)

A	B	IP Csum	PC 2	PC1	...	Payload	CRC
---	---	-----	-----	---------	------	-----	-----	---------	-----

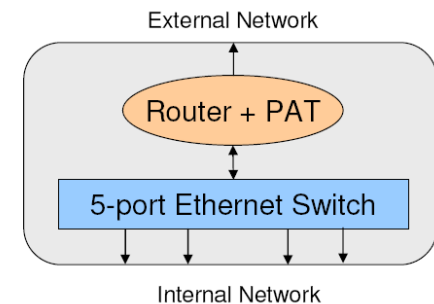
- Lookup Dst IP in mapping table. Only forward if match found
- Replace Dst IP and MAC with private address
- Update checksums (CRC, IP, TCP/UDP/...)

NAT



Home Broadband “Router”

- What is this device?
- Port Address Translation (PAT), plus a...
 - 4-port switch
 - Router
 - DHCP server
 - Wireless access point?
 - Stateful firewall?
 - Blinking LEDs?



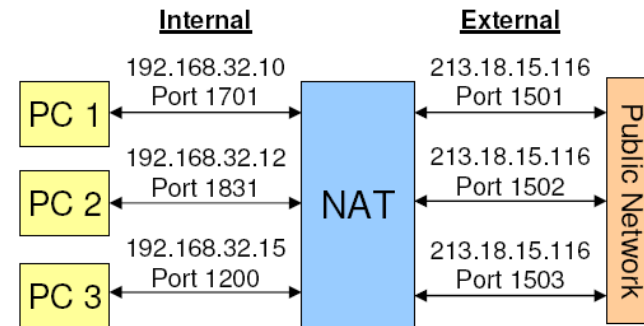
Source : Linksys

NAT

Port Address Translation

■ IP Overloading

- Many internal IPs are mapped to one (or a few) external IPs
- TCP/UDP port number is also changed and used to identify unique connections between internal and external hosts
- Usually dynamic

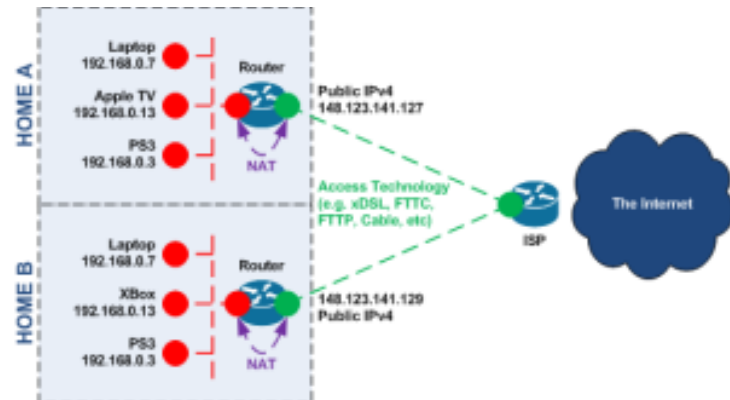


NAT Mapping Table

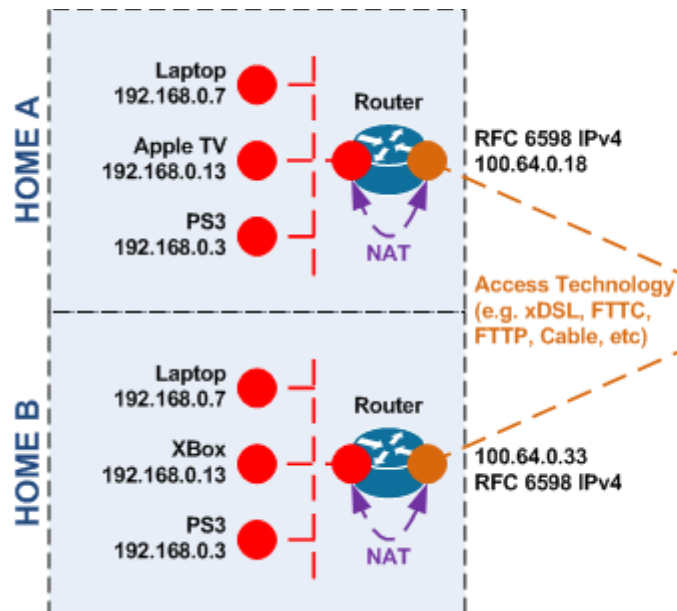
Internal IP	Internal Port	External IP	External Port
192.168.32.10	1701	213.18.15.116	1501
192.168.32.12	1831	213.18.15.116	1502
192.168.32.15	1200	213.18.15.116	1503
...

Not shown in Table: MAC Addresses!

Utilisation NAT connexion maison



Avec adresse public pour le routeur n



Avec adresse ‘privée’ pour le routeur mais

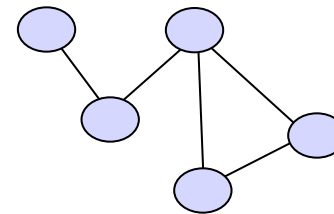
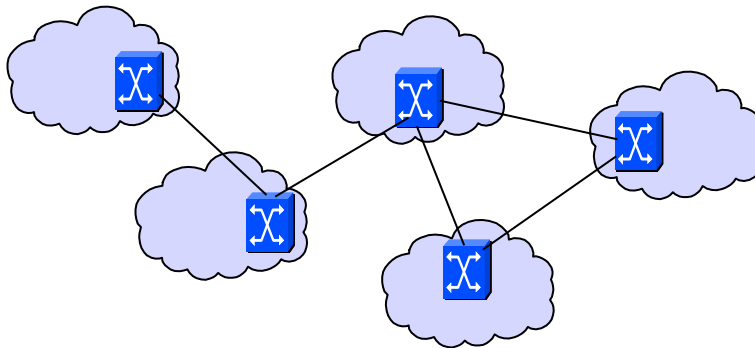
IANA (Internet Assigned Numbers Authority) recently assigned some unallocated public IPv4 address space (RFC6598) for the use of “IPv4 Shared Address Space” – similar to private address space (RFC1918) but for use by ISPs in a Carrier Grade NAT environment

La couche Réseau

Algorithmes de routage

Stratégie de routage

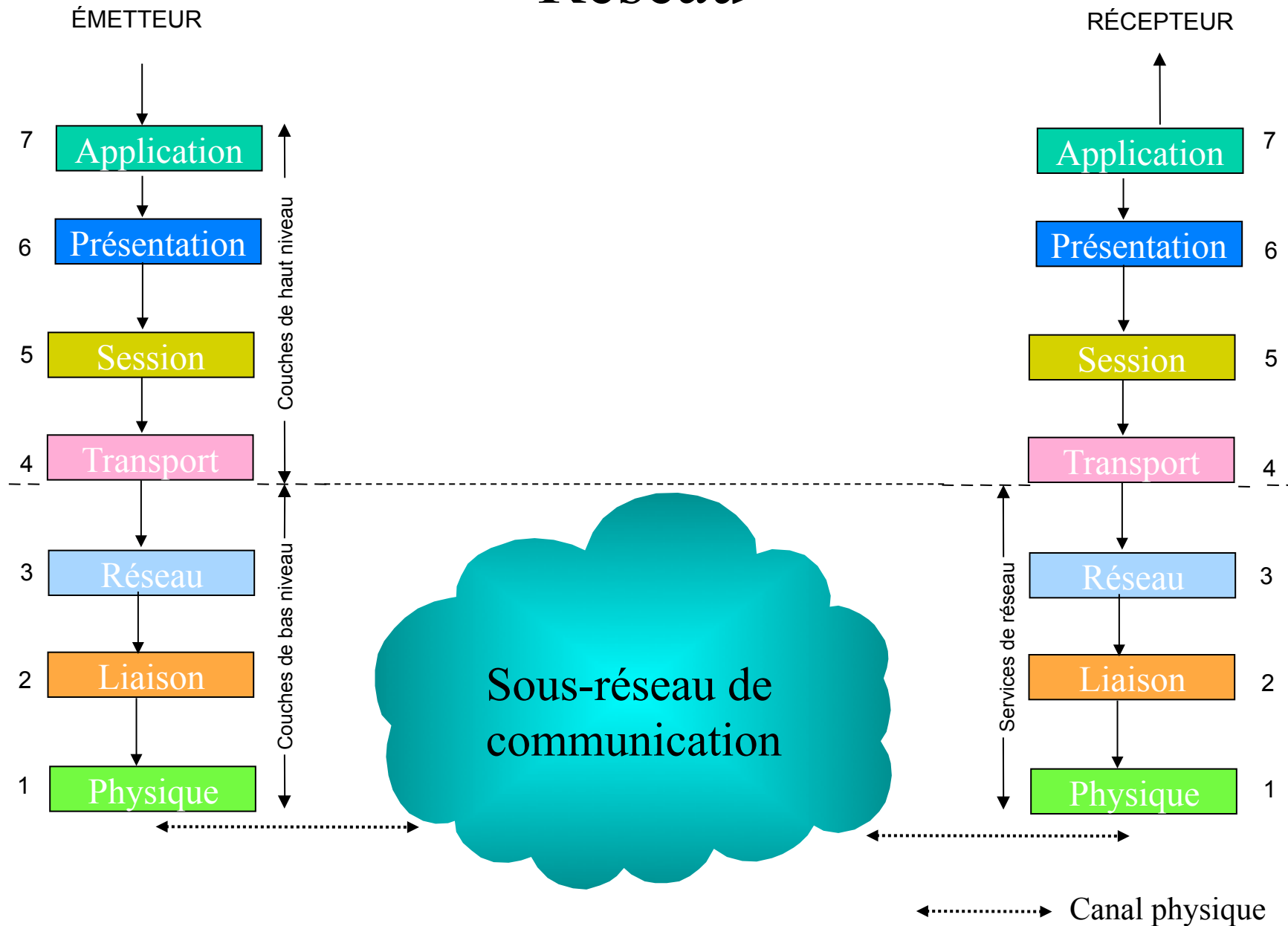
- L'opération par laquelle l'information s'achemine d'un nœud à un autre, en choisissant un chemin parmi plusieurs, constitue le routage.
- La plupart des techniques actuelles de routage se basent sur le plus court chemin, selon une métrique donnée.



Routage dynamique dans les réseaux IP

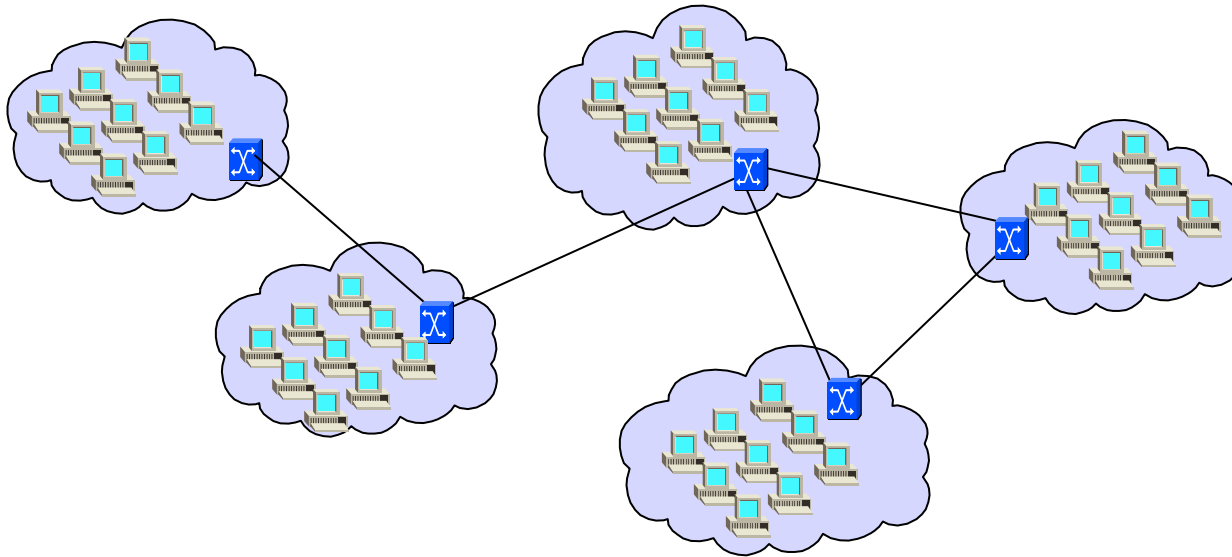
- Le protocole de routage est utilisé pour transmettre les tables d'acheminement dynamiquement entre les routeurs.
- Exemples de protocole intra-domaine
 - RIP (*Routing Information Protocol*)
 - OSPF (*Open Shortest Path First*), etc.
- Exemples de protocole extra-domaine
 - BGP (*Border Gateway Protocol*), etc.

Réseau

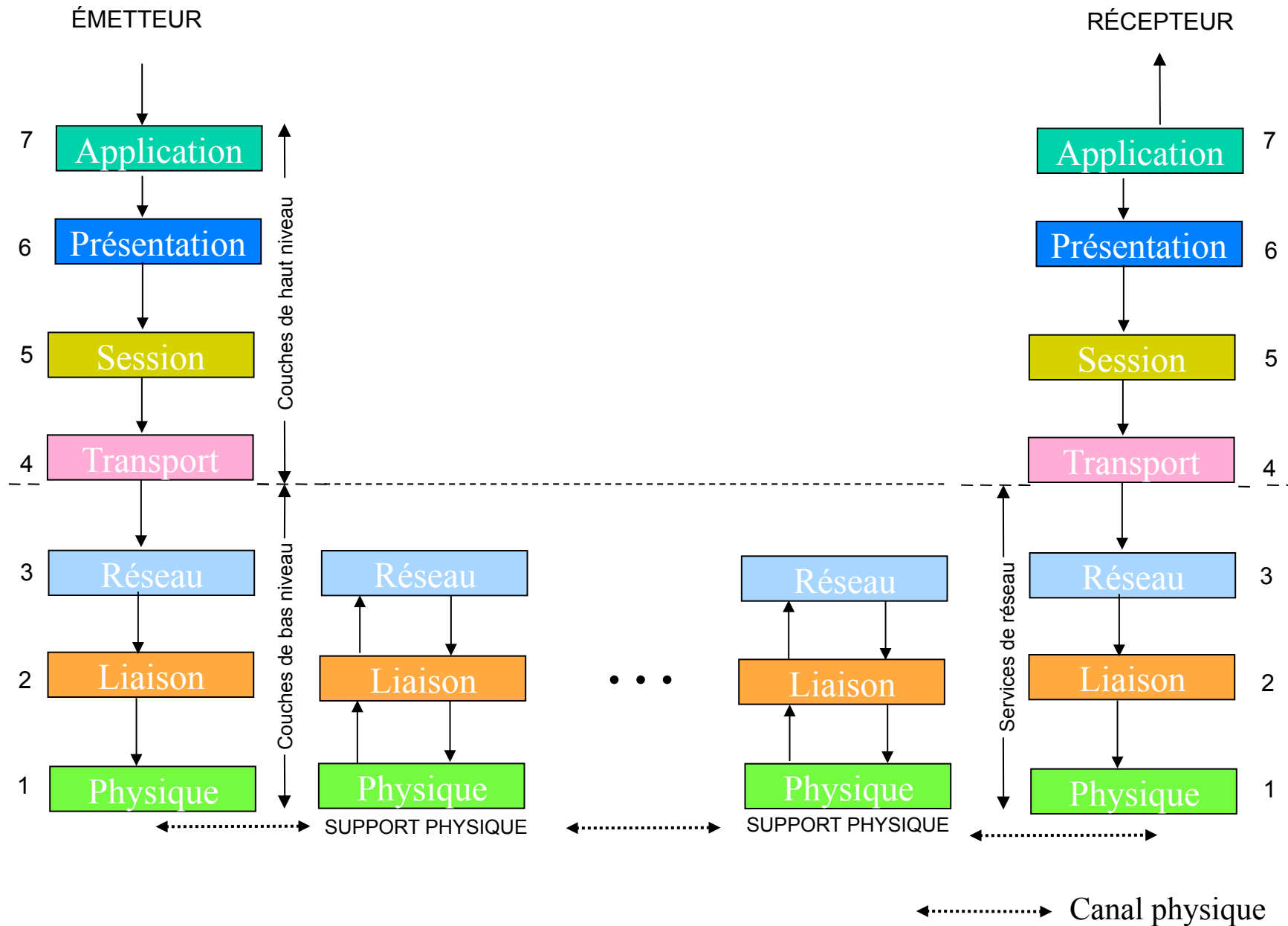


La couche Réseau

Routage

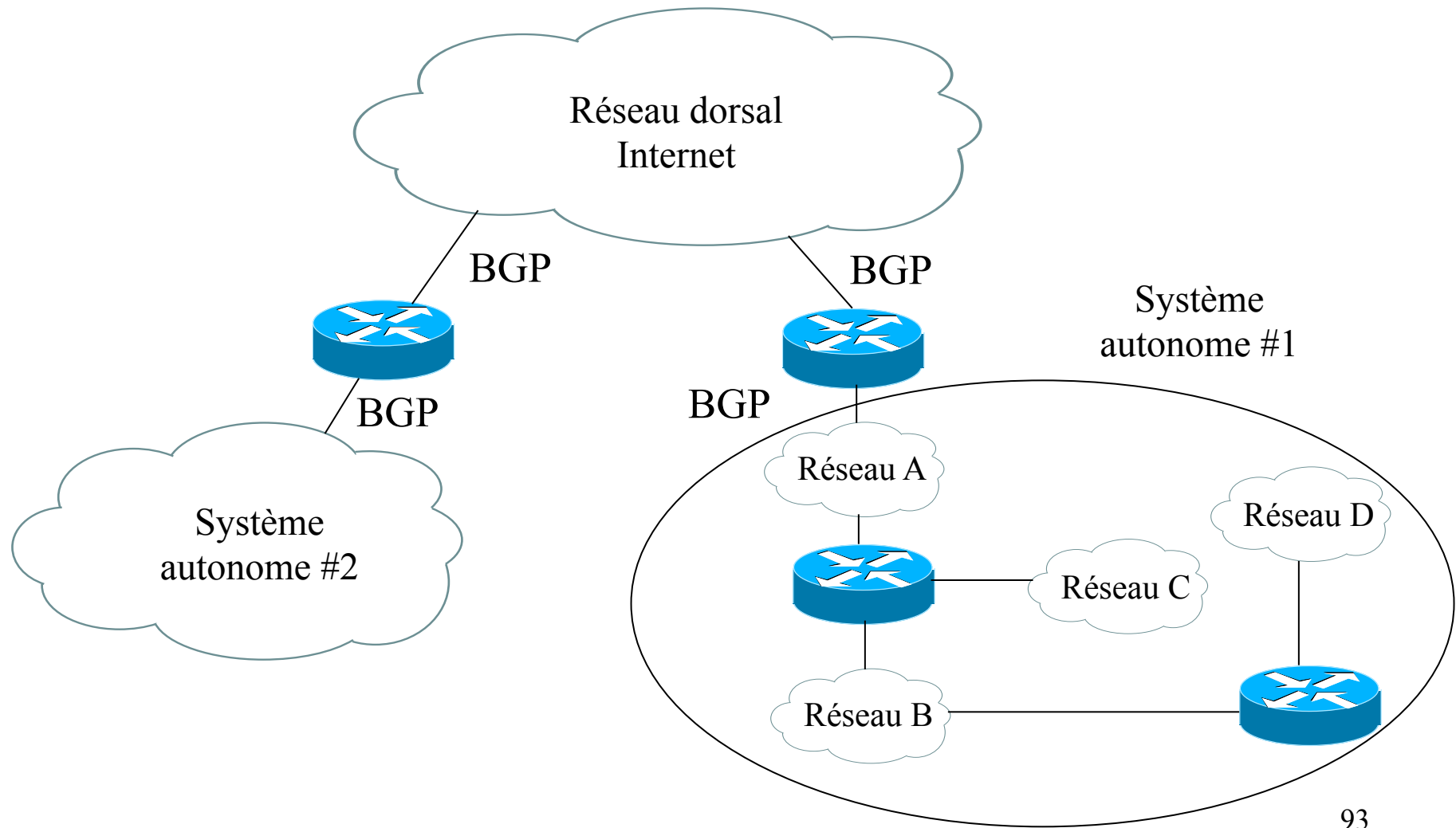


Réseau



Routage dynamique dans les réseaux IP (suite)

- Routage intra- et extra-système autonome (domaine)



Routage dynamique dans les réseaux IP (suite)

- Routage dynamique vs. statique
 - Contrairement qu'avec les protocoles de routages dynamiques (RIP, OSPF, etc.), le routage statique implique d'entrer les tables de routage de façon manuelle.
 - Ainsi, le routage statique ne peut être réalisé qu'avec des petits réseaux (e.g., moins de 10 routeurs).
 - Le routage statique peut être utilisé pour rejoindre des réseaux isolés ou pour réaliser des tests.
 - Pour les routeurs Cisco, la commande est

**ip route <adresse IP de destination> <masque de l'adresse IP de destination>
<adresse IP de la prochaine interface>**

Cette commande doit être faite sous l'interface locale à utiliser pour atteindre la prochaine interface (du prochain routeur). 94

Routage dynamique dans les réseaux IP (suite)

- Routage vecteur distant
 - Le vecteur distant est un type d'algorithme basé sur la notion de distance (nombre de routeurs).
 - Dans ce type d'algorithme, chaque routeur envoie périodiquement sa table de routage complète vers ses voisins.
 - Ces tables de routage sont utilisées par chacun des routeurs pour construire leur propre table de routage en utilisant la route ayant la distance la plus courte (en terme du nombre de routeurs).
 - Cet algorithme ne permet pas au routeur de connaître la topologie du réseau. Seul les routes ayant la plus courte distance vers les autres routeurs sont connues.
 - Le protocole RIP est basé sur cet algorithme.

Routage dynamique dans les réseaux IP (suite)

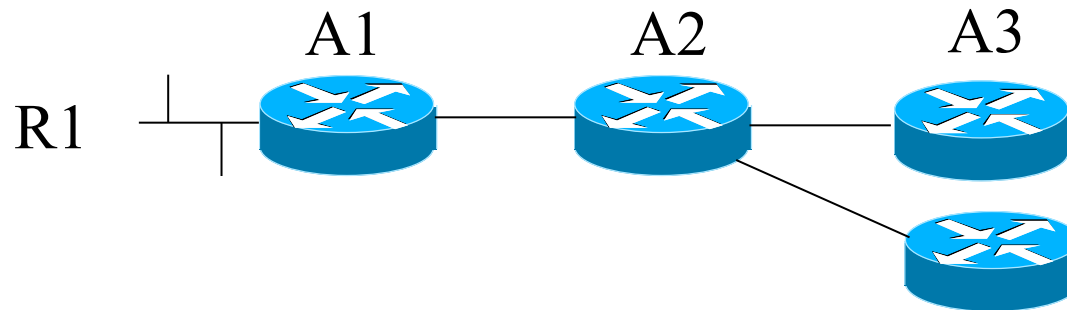
- Routage état des liens
 - Ce type d'algorithme est basé sur les plus courts chemins (algorithme de Dijkstra).
 - Dans ce type d'algorithme, chaque routeur informe ses voisins de l'état de tous ses liens.
 - Pour tous les états des liens qu'un routeur reçoit, il doit à son tour les retransmettre à ses voisins.
 - Ainsi chaque routeur connaît la topologie dans son domaine.
 - Le protocole OSPF est basé sur cet algorithme.

Routage dynamique dans les réseaux IP: RIP

- RIP (Routing Information Protocol) est un algorithme de routage basé sur l'algorithme vecteur distant.
- RIP envoie sa table d'acheminement à toutes les 30 secondes à ses voisins.
- Chaque voisin va mettre sa table de routage à jour et la transmettre ses voisins. Le processus continu jusqu'à convergence du réseau.
- Il y a deux versions de RIP (v1 et v2).
- RIP n'est plus beaucoup utilisé; il a été remplacé par OSPF.

Routage dynamique dans les réseaux IP: RIP (suite)

- Exemple



- Le routeur A1 publie l'existence de R1 avec une distance de 1 au routeur A2.
- A2 met sa table de routage à jour.
- A2 publie l'existence de R1 avec une distance de 2 aux routeurs A3 et A4.
- A3 et A4 mettent leurs tables à jour.
- A3 et A4 publient à leur voisins l'existence de R1....

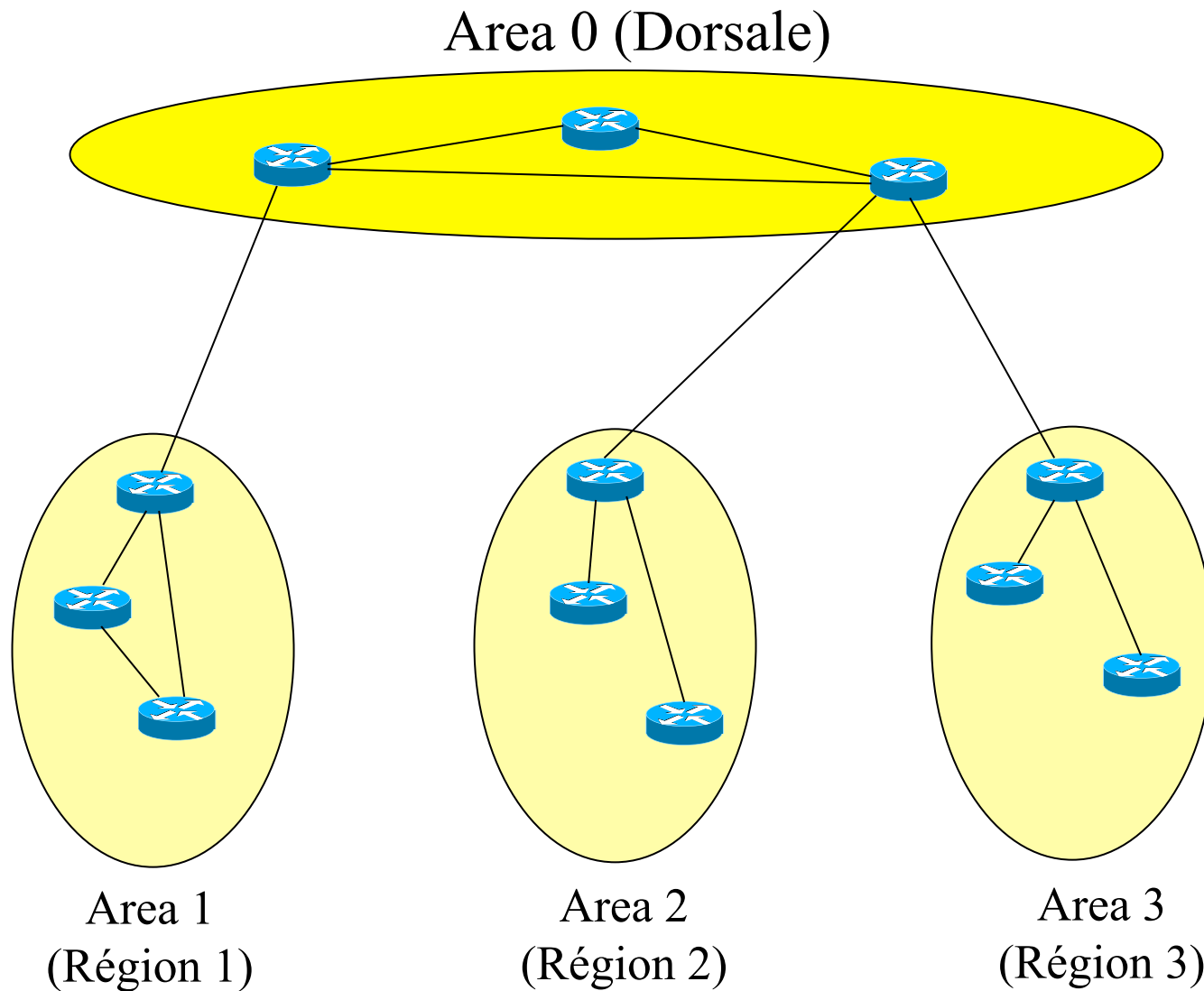
Routage dynamique dans les réseaux IP: OSPF

- OSPF (*Open Shortest Path First*) est un algorithme de routage basé sur l'algorithme état des liens et il est considéré comme LE protocole de routage intra-domaine.
- OSPF permet d'avoir une hiérarchie de routage.
- Communique avec ses voisins lorsqu'il y a des changements dans le réseau ou au moins une fois par 30 minutes.
- OSPF remplace RIP dans l'industrie.
- OSPF est normalisé – RFC 1247.

Routage dynamique dans les réseaux IP: OSPF (suite)

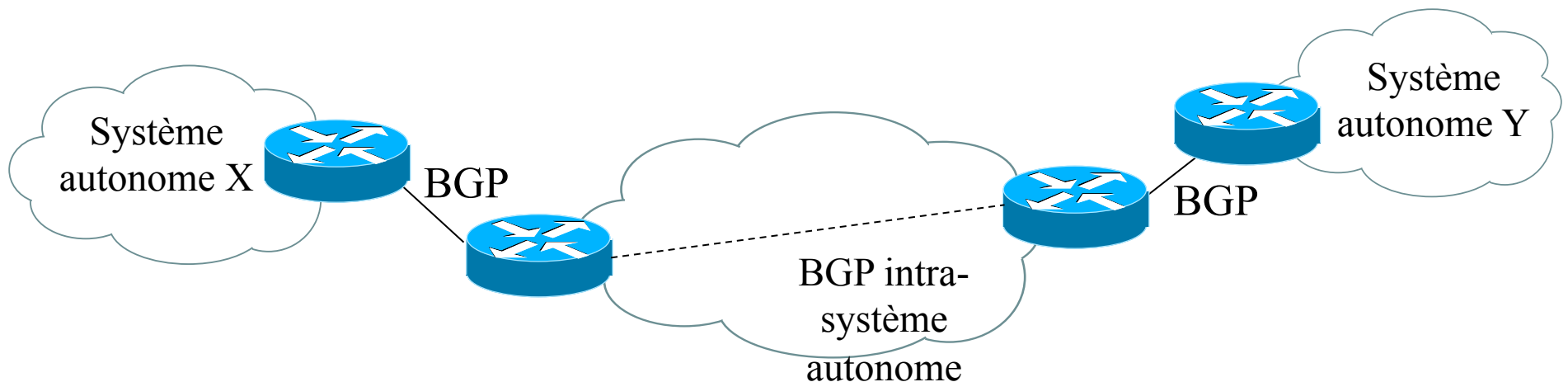
- Caractéristiques de OSPF
 - Utilise des métrique (« link cost ») pour choisir la meilleure route.
 - Support pour les masques de longueur variable.
 - Consomme peu de bande passante.
 - Non compatible avec RIP.
 - Demande au routeur de calculer lui même les routes et de vérifier constamment l'état des liens.
 - Permet d'avoir une hiérarchie au niveau du routage.

Routage dynamique dans les réseaux IP: OSPF (suite)



Routage dynamique dans les réseaux IP: BGP

- BGP (*Border Gateway Protocol*) est un protocole de passerelle utilisé pour échanger de l'information connue d'un système autonome (domaine) à des routeurs de périphérie (« gateway »).
- BGP remplace le protocole EGP (*Exterior Gateway Protocol*).
- BGP est normalisé – RFC 1105.



Routage dynamique dans les réseaux IP: BGP (suite)

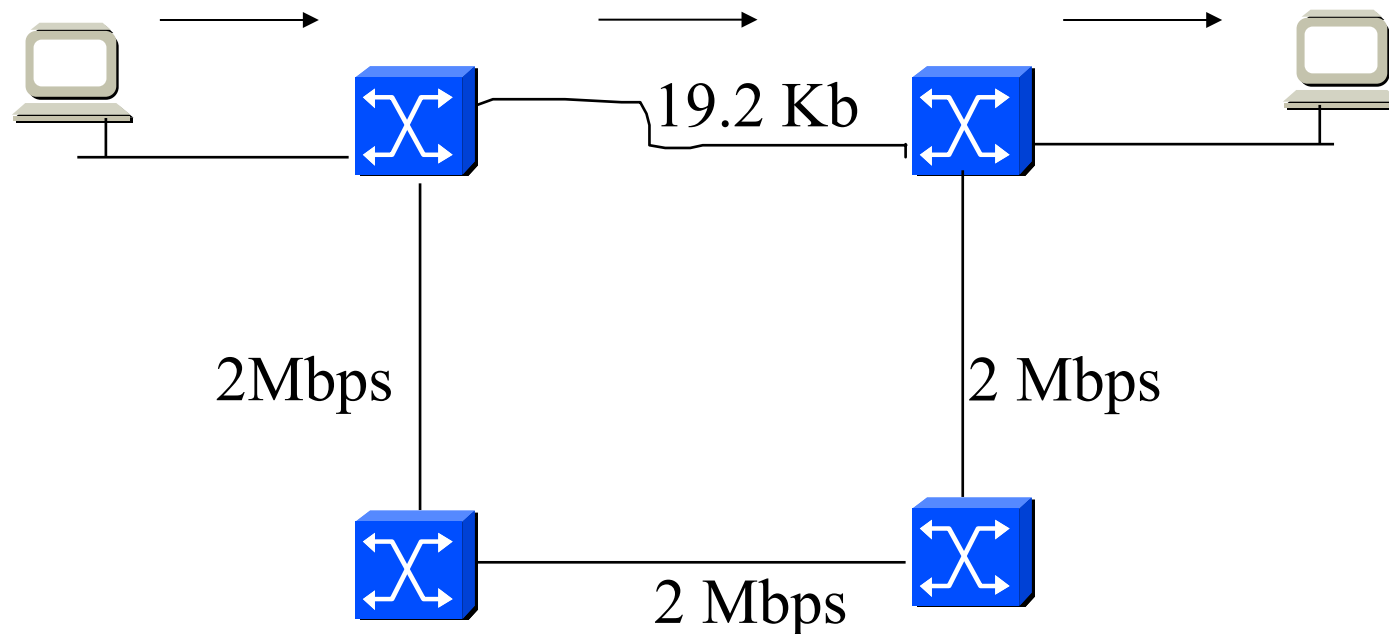
- Caractéristiques de BGP
 - BGP est un hybride en vecteur distant et état des liens.
 - Permet la détection des boucles.
 - Permet une convergence rapide.
 - Permet l'agrégation des routes.
 - BGP est le protocole de passerelle d'Internet.
 - À deux types de voisin : interne (IBGP) et externe (EBGP).

La couche Réseau

Algorithmes de routage

Routage à vecteur de distance (distance vector routing)

- RIP – Internet : Routing Information Protocol

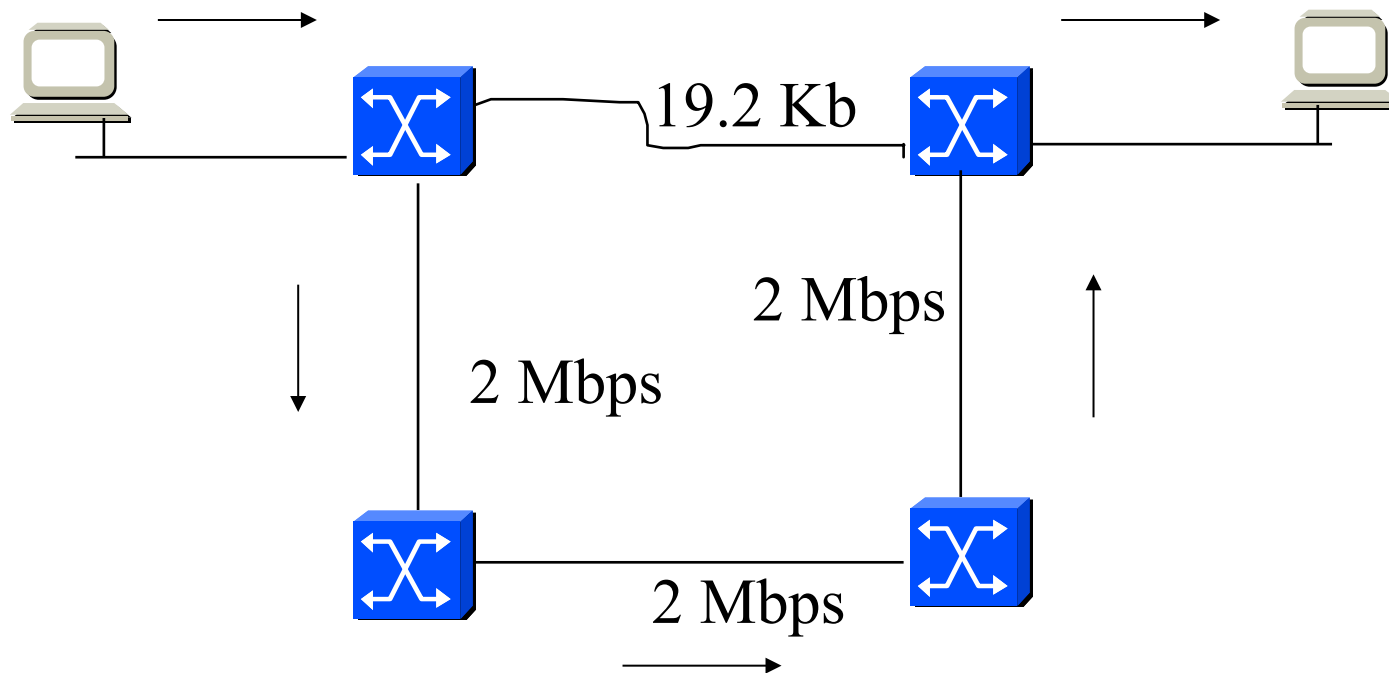


La couche Réseau

Algorithmes de routage

Routage par informations d'état de lien (link state routing)

- OSPF – Internet : Open Shortest Path First

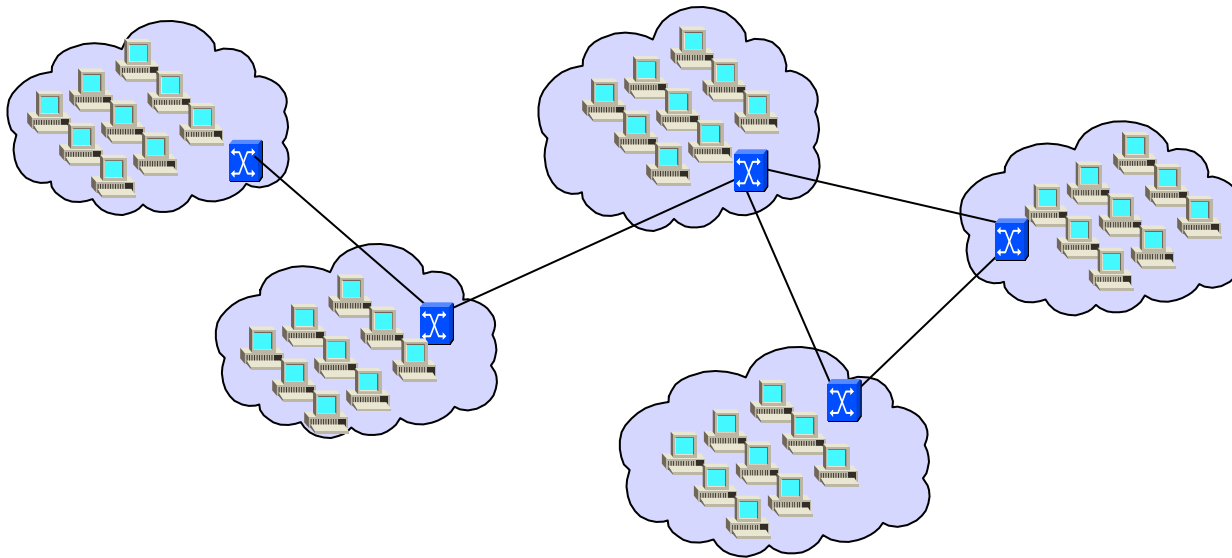


La couche Réseau

Algorithmes de routage

Routage hiérarchique

- Au fur et à mesure que les réseaux grandissent, les tables de routage des routeurs croissent en proportion.
- Avec le routage hiérarchique les routeurs sont réparties par régions

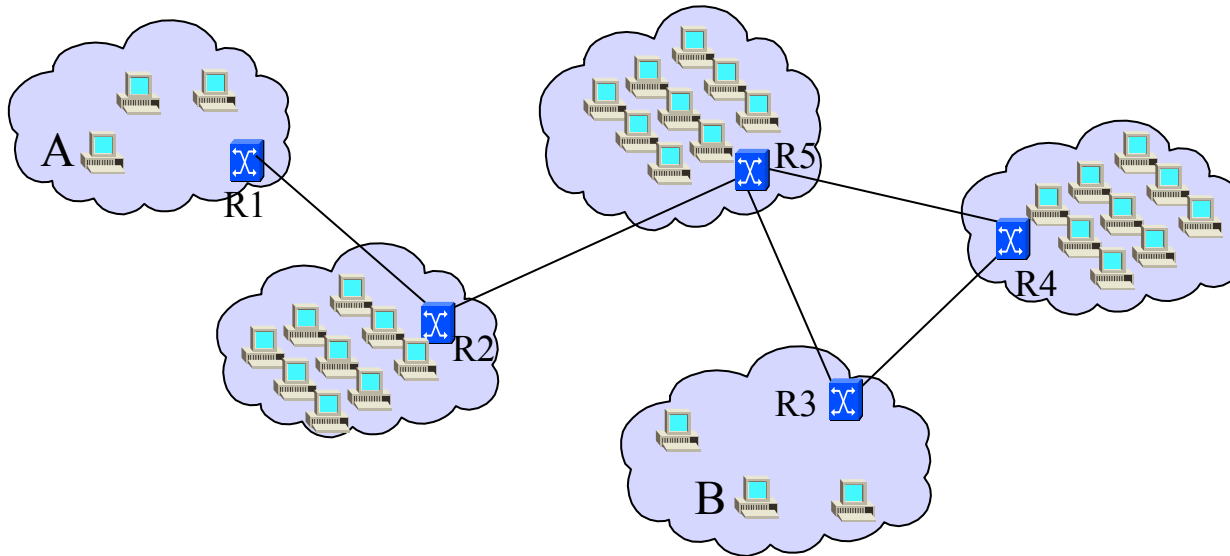


La couche Réseau

Algorithmes de routage

Fonctionnement du Routage hiérarchique

A \longrightarrow B

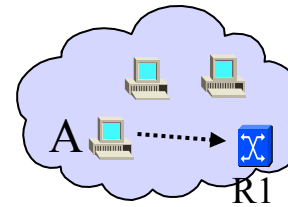


La couche Réseau

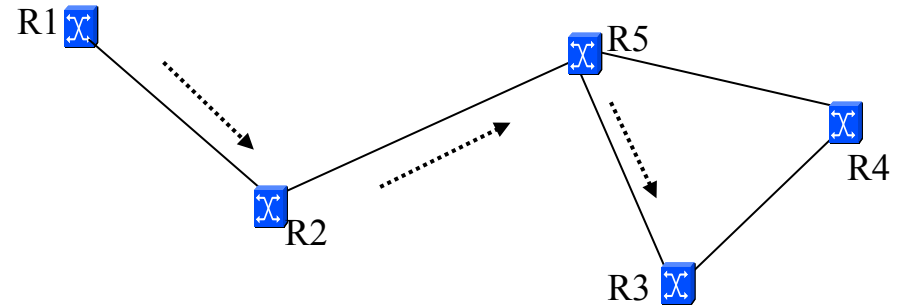
Algorithmes de routage

Fonctionnement du Routage hiérarchique : A \longrightarrow B

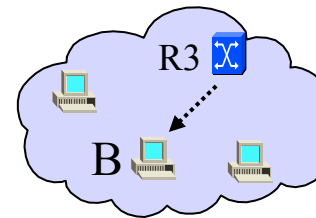
Première Étape : A \longrightarrow R1



Deuxième Étape : R1 \longrightarrow R3



Troisième Étape : R3 \longrightarrow B

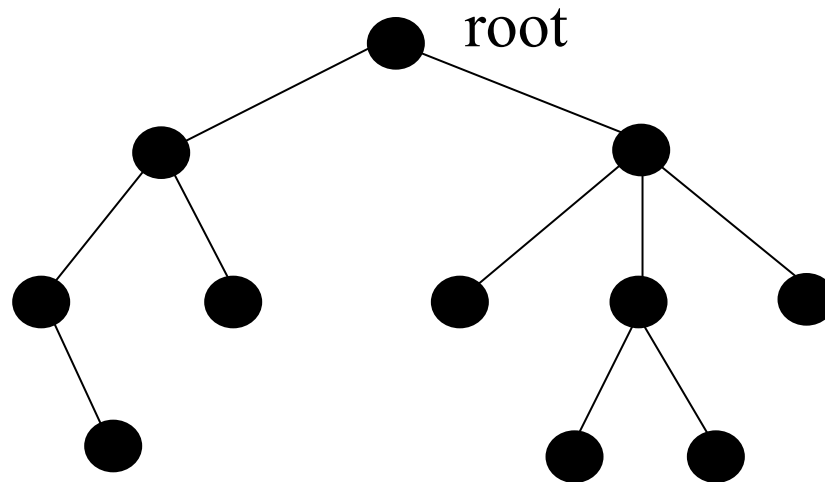


DNS

- DNS (*Domain Name Server*) permet d'effectuer une correspondance entre un nom de système et son adresse IP.
- C'est un protocole qui possède deux parties :
 - client: « Resolver » ;
 - serveur: « Name server ».
- Avant l'arrivée de DNS, les réseaux se basaient sur un fichier appelé HOST.TXT. Ce fichier contenait la correspondance entre un nom de système et son adresse IP.
- Ce fichier était mis à jour manuellement par le Stanford Research Institute.

DNS (suite)

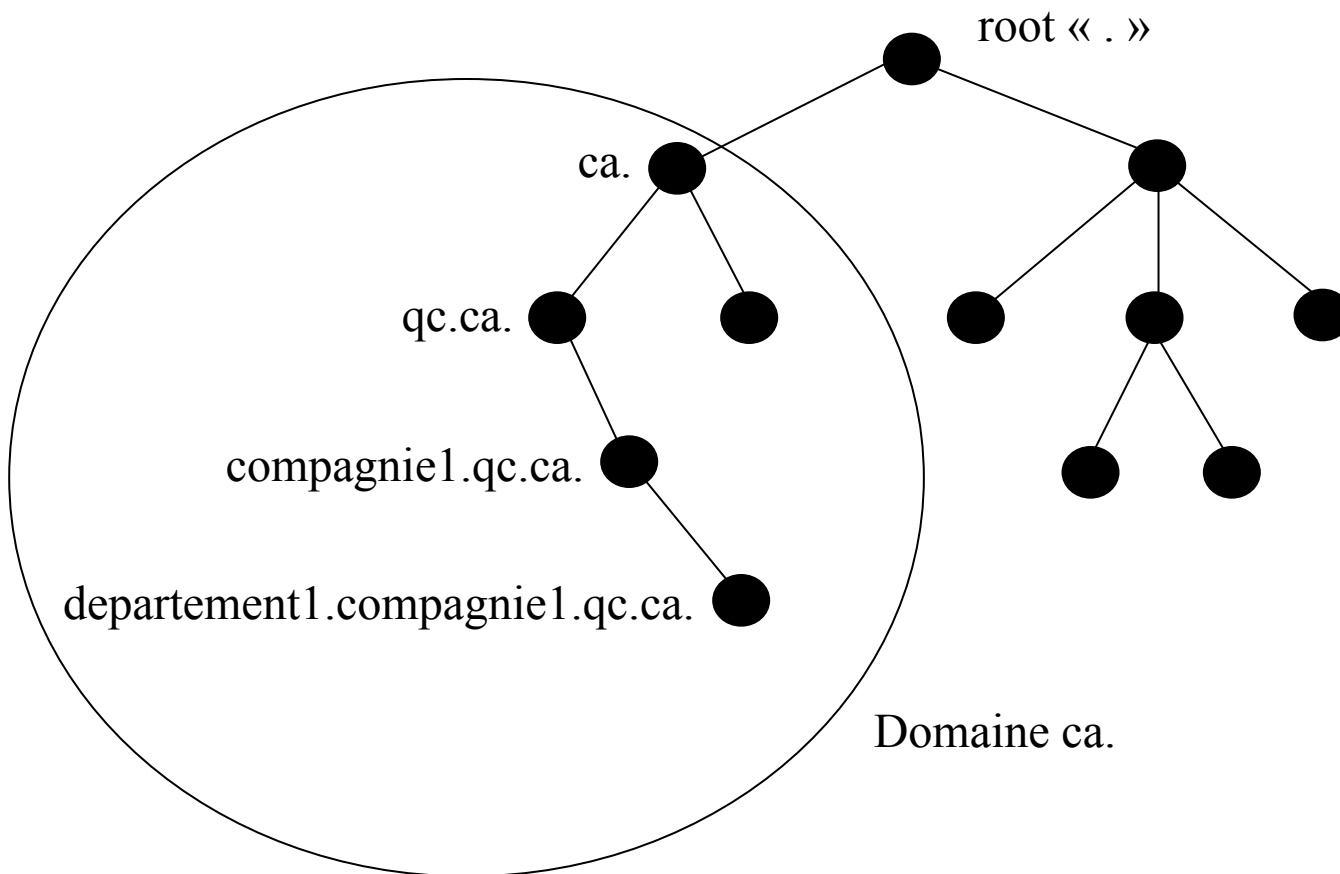
- Plusieurs problèmes sont apparus, en raison de la forte croissance d'Internet. En effet, il devenait difficile de mettre à jour ce fichier manuellement.
- Structure



- La base de données DNS est représentée par un arbre inversé où l'on retrouve la racine (« root ») au sommet.
- Il est possible d'avoir jusqu'à 127 niveaux (pas recommandé).

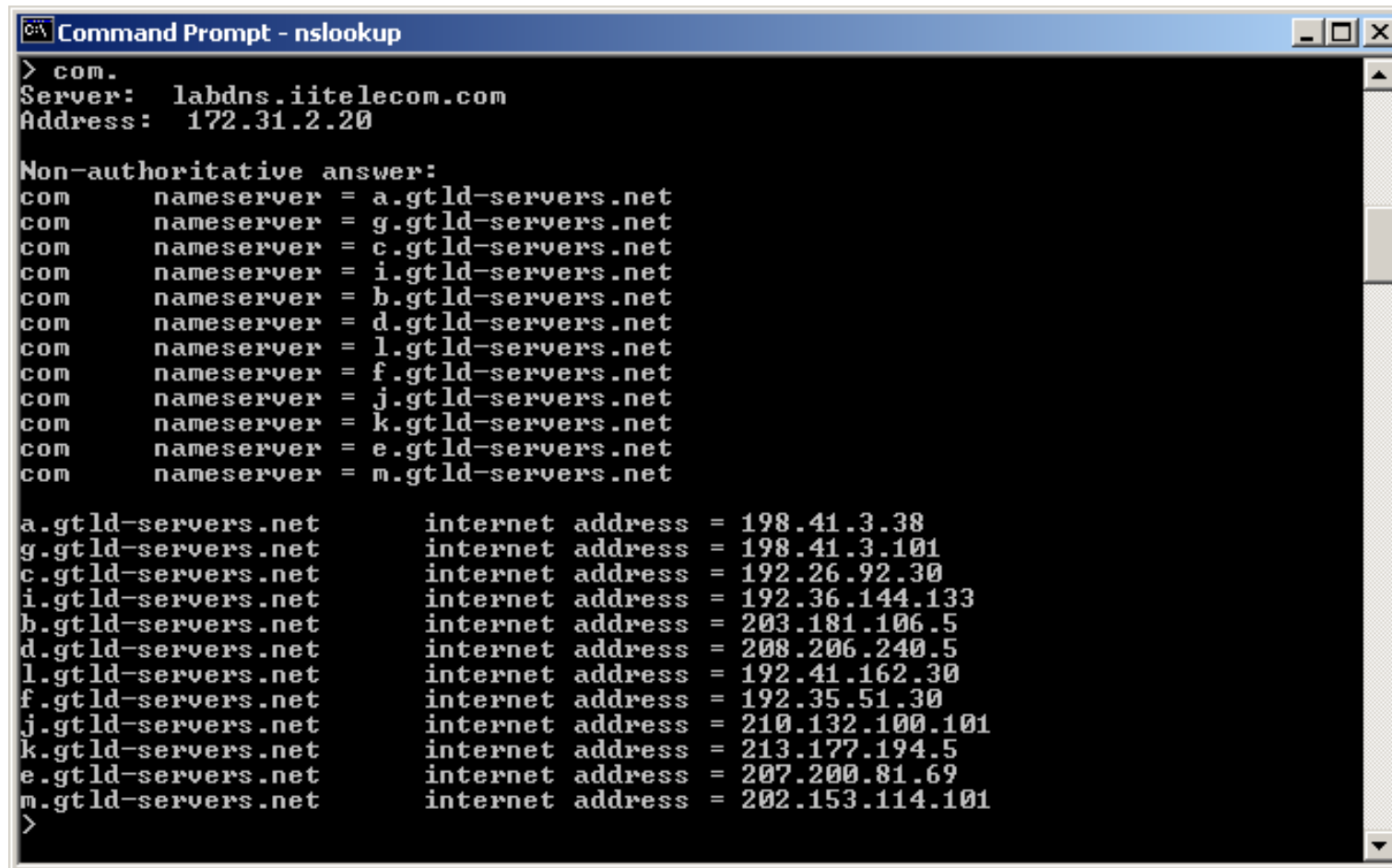
DNS (suite)

- Structure : departement1.compagnie1.qc.ca



DNS (suite)

- Localisation des serveurs : commande nslookup (DOS)



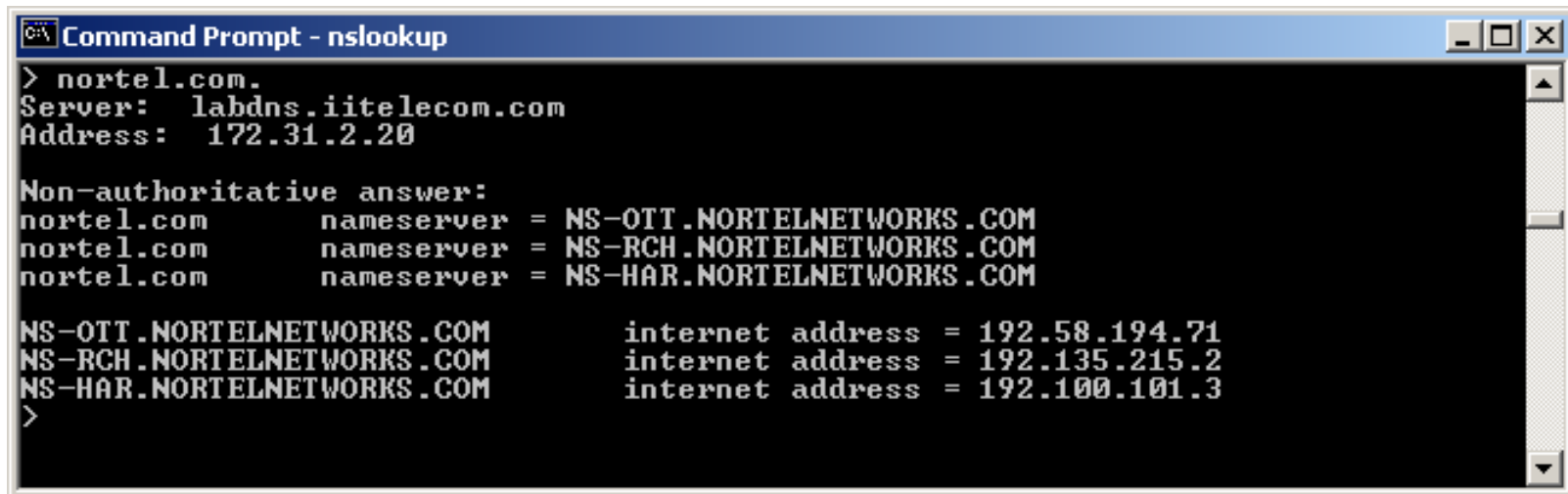
```
Command Prompt - nslookup
> com.
Server:  labdns.iitelecom.com
Address:  172.31.2.20

Non-authoritative answer:
com      nameserver = a.gtld-servers.net
com      nameserver = g.gtld-servers.net
com      nameserver = c.gtld-servers.net
com      nameserver = i.gtld-servers.net
com      nameserver = b.gtld-servers.net
com      nameserver = d.gtld-servers.net
com      nameserver = l.gtld-servers.net
com      nameserver = f.gtld-servers.net
com      nameserver = j.gtld-servers.net
com      nameserver = k.gtld-servers.net
com      nameserver = e.gtld-servers.net
com      nameserver = m.gtld-servers.net

a.gtld-servers.net      internet address = 198.41.3.38
g.gtld-servers.net      internet address = 198.41.3.101
c.gtld-servers.net      internet address = 192.26.92.30
i.gtld-servers.net      internet address = 192.36.144.133
b.gtld-servers.net      internet address = 203.181.106.5
d.gtld-servers.net      internet address = 208.206.240.5
l.gtld-servers.net      internet address = 192.41.162.30
f.gtld-servers.net      internet address = 192.35.51.30
j.gtld-servers.net      internet address = 210.132.100.101
k.gtld-servers.net      internet address = 213.177.194.5
e.gtld-servers.net      internet address = 207.200.81.69
m.gtld-servers.net      internet address = 202.153.114.101
>
```


DNS (suite)

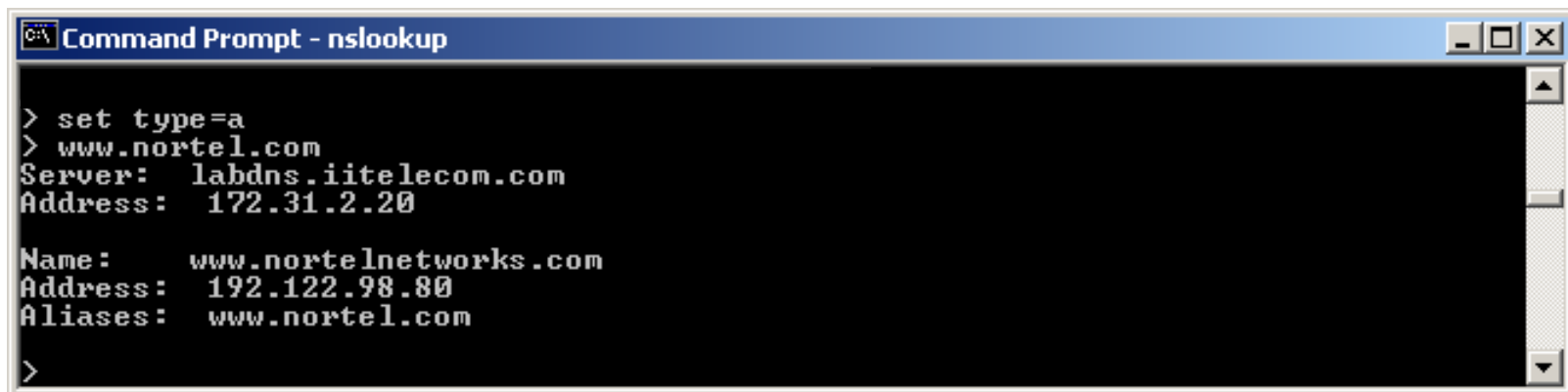
- Localisation des serveurs : commande nslookup (suite)



```
Command Prompt - nslookup
> nortel.com.
Server: labdns.iitelecom.com
Address: 172.31.2.20

Non-authoritative answer:
nortel.com      nameserver = NS-OTT.NORTELNETWORKS.COM
nortel.com      nameserver = NS-RCH.NORTELNETWORKS.COM
nortel.com      nameserver = NS-HAR.NORTELNETWORKS.COM

NS-OTT.NORTELNETWORKS.COM      internet address = 192.58.194.71
NS-RCH.NORTELNETWORKS.COM      internet address = 192.135.215.2
NS-HAR.NORTELNETWORKS.COM      internet address = 192.100.101.3
>
```



```
Command Prompt - nslookup
> set type=a
> www.nortel.com
Server: labdns.iitelecom.com
Address: 172.31.2.20

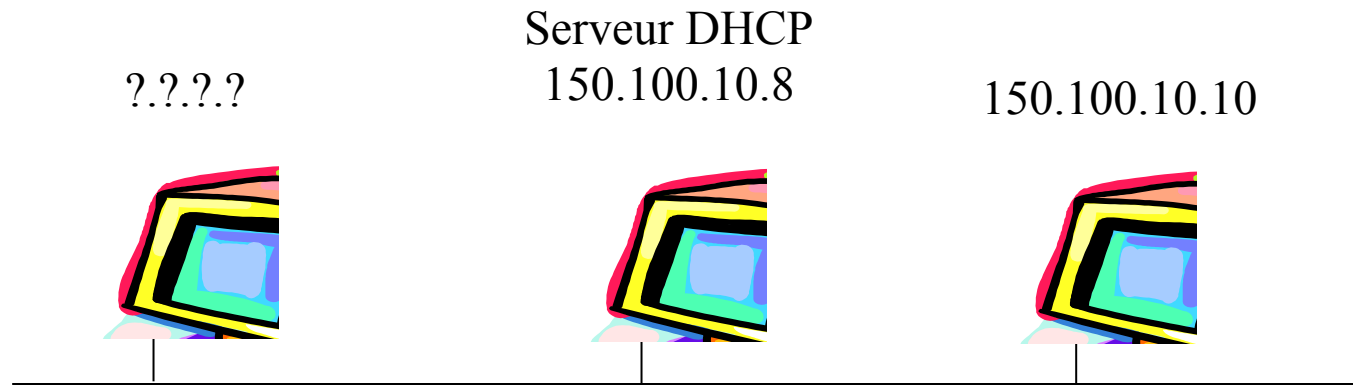
Name: www.nortelnetworks.com
Address: 192.122.98.80
Aliases: www.nortel.com
>
```

DHCP

- DHCP (*Dynamic Host Configuration Protocol*) est un protocole qui permet aux administrateurs de réseaux de gérer automatiquement la distribution des adresses IP et des valeurs associées.
- Le protocole DHCP assigne les adresses IP pendant une période fixe, appelée un bail. La durée du bail est définie par l'administrateur.
- Sans DHCP, l'affectation des adresses IP est faite de manière manuelle.
- DHCP utilise le protocole BOOTP (*Bootstrap Protocol*).
- DHCP est défini dans standards RFC 1531, 1533 et 1534.

DHCP (suite)

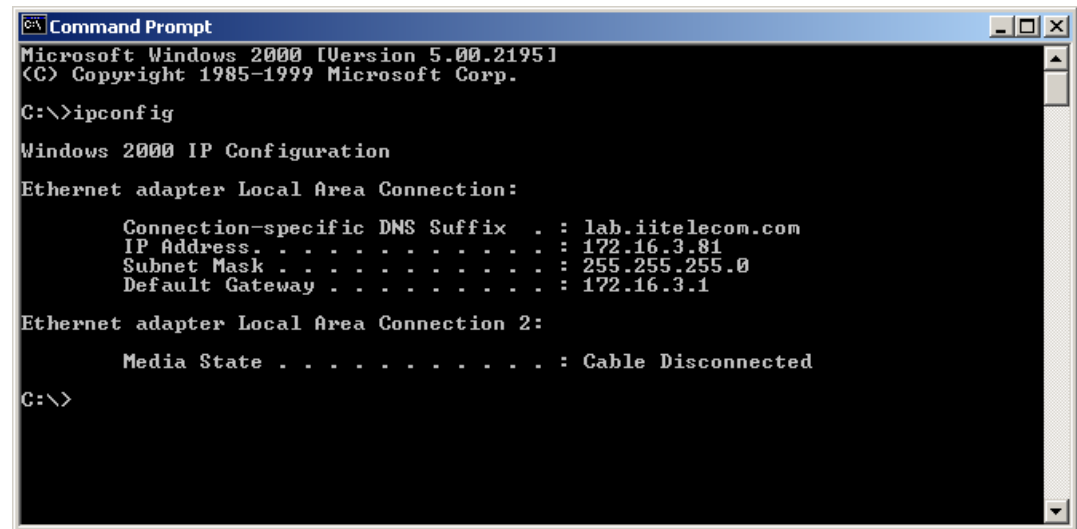
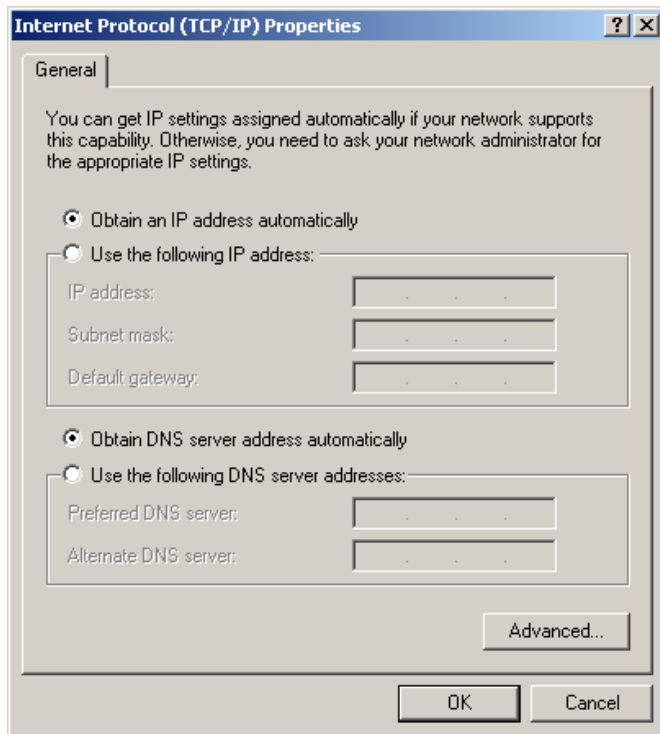
- Exemple



- Un poste qui a besoin d'une adresse IP, envoie une requête au serveur DHCP via un paquet « broadcast ». Le serveur capture la requête et y répond.
- Le serveur répond en fournissant l'adresse IP et la durée du bail.
- À ce moment, le poste a une adresse IP et fait partie du réseau.
- Lorsque le bail expire, le poste relâche l'adresse. Une nouvelle requête est envoyée.

DHCP (suite)

- Configuration et commande ipconfig (DOS)



IPv6 ou IPng

- Actuellement c'est la version 4 du protocole IP (IPv4) qui est majoritairement utilisée.
- IPv6 ou IPng (*Next Generation*) est la nouvelle version de IP.
- La différence majeure de IPv6 est au niveau de l'adressage; IPv6 utilise une adresse de 128 bits (16 octets) au lieu de 32 bits.

IPv6 ou IPng (suite)

- Format du paquet IPv6

