Ecole Nationale des Sciences de l'Informatique

Réseaux Informatiques

Enseignante: Dr. Nesrine Chakchouk

Année Universitaire: 2024 - 2025

Chapitre II: La Couche Réseau

- Le Concept d'Interconnexion
- Architecture Internet
- Adressage IP
- IP et protocoles associés (ICMP, ARP, RARP)
- Fragmentation et Réassemblage
- Routage: Généralités
- Algorithmes de Routage (LSR, DVR)
- Protocoles de RTG Internet I (RTG intra-domaine: RIP, OSPF)
- Protocoles de RTG Internet II (RTG inter-domaine: BGP)

Internetworks

Problèmes posés

- Réseaux reliés à l'« internetwork » fonctionnent en mode connecté ou en mode non connecté.
- Adressage, chaque réseau a son propre adressage.
- Routage entre réseaux.
- Qualité de service différente d'un réseau à un autre.
- MTU (Taille maximale de paquets) différente d'un réseau à un autre.
- Contrôle d'erreurs et de flux différents selon les réseaux.

Internetworks

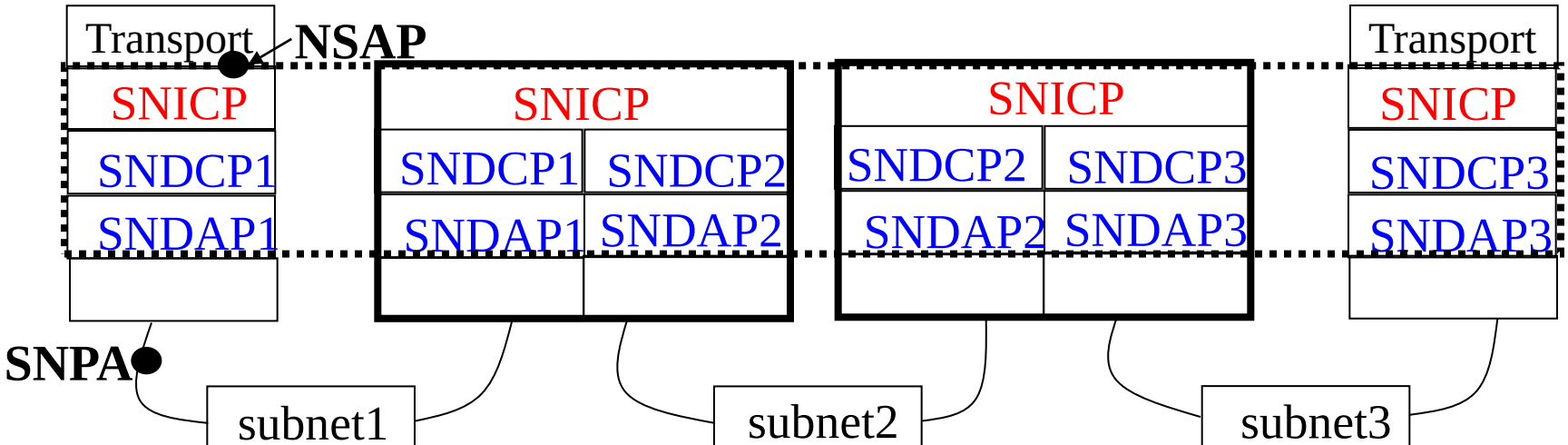
Services offerts par un Internetwork

- Services en modes connecté TCP ou non connecté UDP
- Adresses IP
- Routage
- Fragmentation
- Contrôle de congestion
- Contrôle de flux

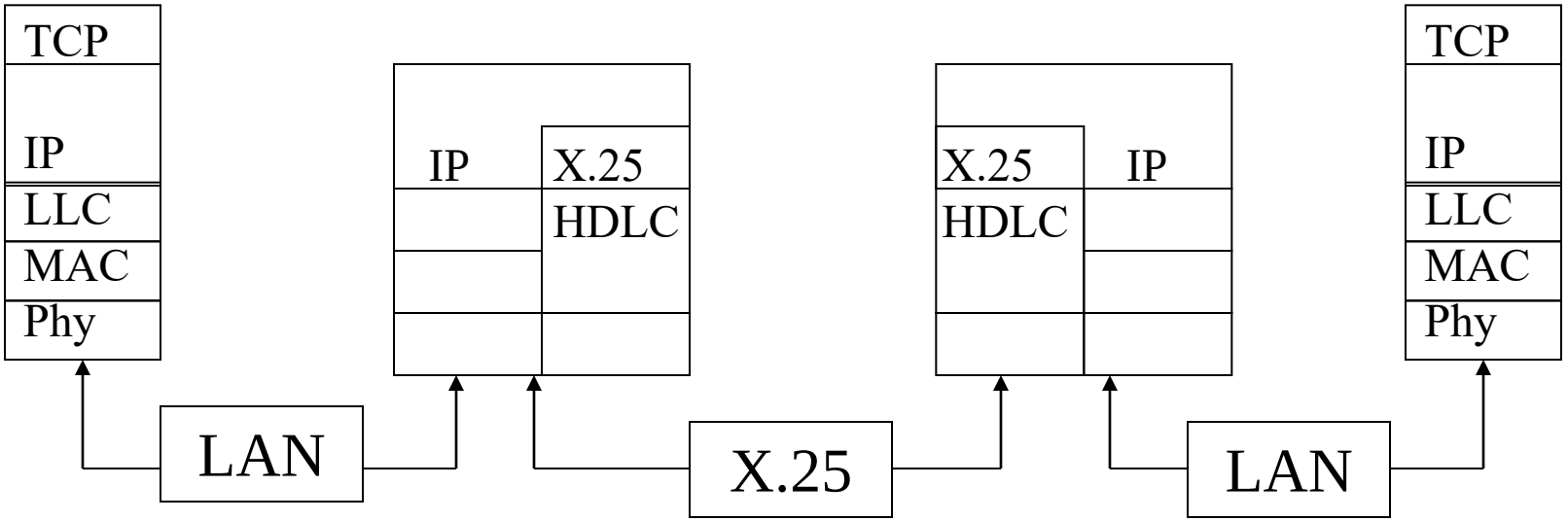
Internetworks

Structure de la couche réseau

- SNICP "SubNet Independent Convergence Protocol" : protocole commun, fragmentation/réassemblage, routage (forwarding), IP.
- **SNDAP** "SubNet Dependent Access Protocol" propre à chaque "subnet"
- **SNDCP** "SubNet Dependent Convergence Protocol" : réalise les fonctions de correspondance entre SNICP & SNDAP en particulier la correspondance entre les adresses SNPA « SubNetwork Point of Attachment » et NSAP « Network Service Address Point ».



Internetworks

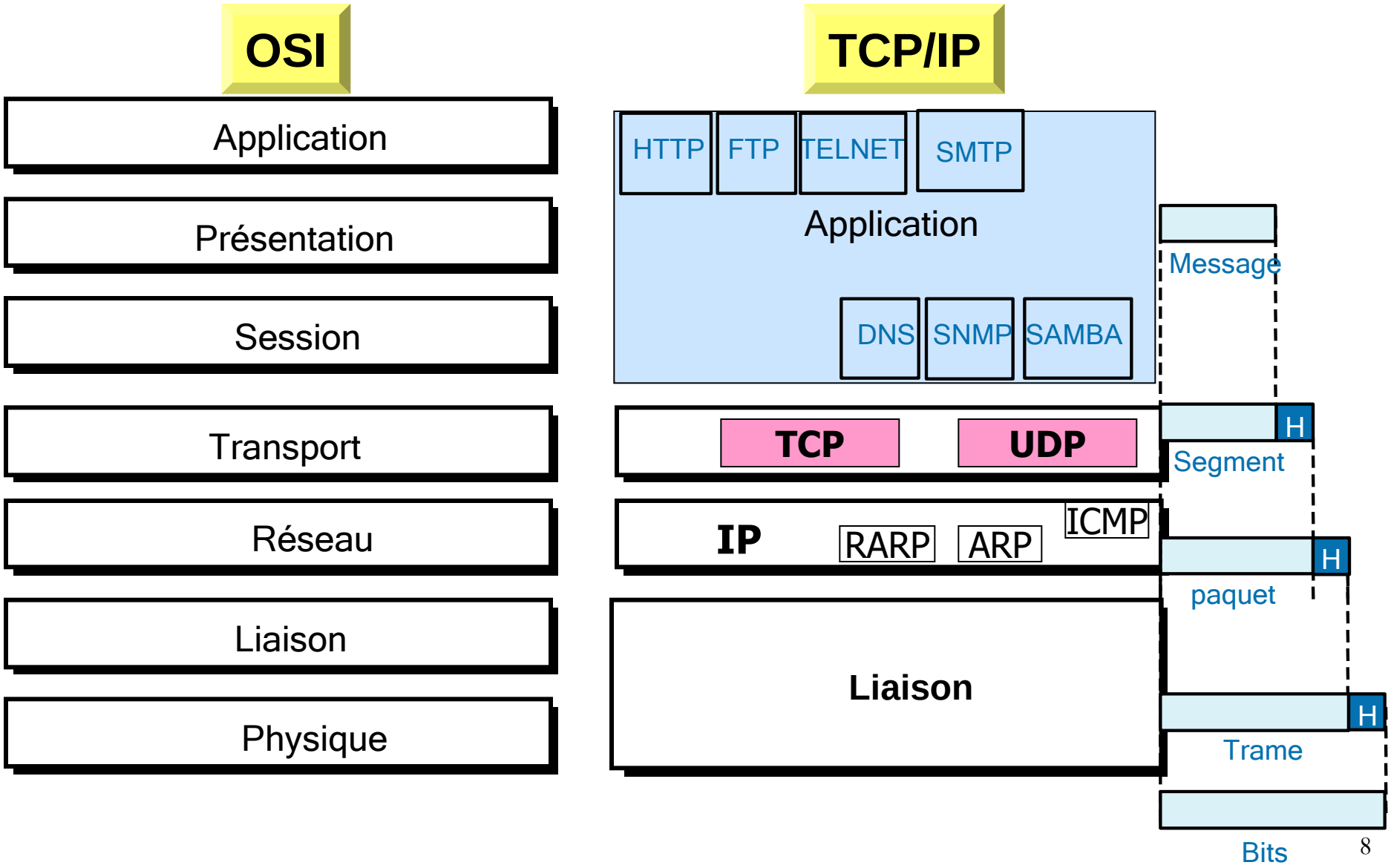


- Dans le cas du LAN, le service de la sous couche **SNDAP** se ramène à celui de LLC/MAC alors que sur le réseau X.25 il correspond à celui de HDLC.

Chapitre II: La Couche Réseau

- Le Concept d'Interconnexion
- Architecture Internet
- Adressage IP
- IP et protocoles associés (ICMP, ARP, RARP)
- Fragmentation et Réassemblage
- Routage: Généralités
- Algorithmes de Routage (LSR, DVR)
- Protocoles de RTG Internet I (RTG intra-domaine: RIP, OSPF ..)
- Protocoles de RTG Internet II (RTG inter-domaine: EGP, BGP..)

TCP/IP : modèle en couches



IP

Internet Protocol

- Routage à travers Internet
- Règles d'adressage Internet (adresses logiques IP)

Protocoles associés:

- Contrôle de l'Internet ICMP
- Conversion d'adresses logiques en adresses physiques ARP
- Conversion d'adresses physiques en adresses logiques RARP

Protocole IP

- Protocole de convergence
- Fonctionne indépendamment des couches basses
  - Ethernet
  - PPP
  - FDDI
  - ATM
  - 802.11

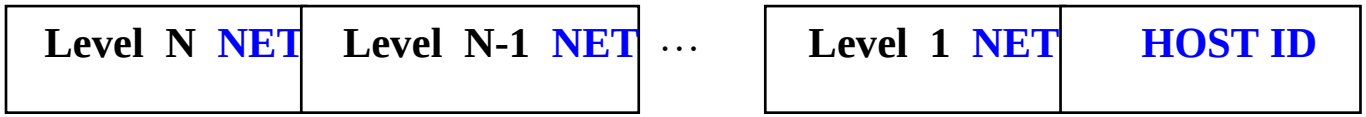
Chapitre II: La Couche Réseau

- Le Concept d'Interconnexion
- Architecture Internet
- Adressage IP
- IP et protocoles associés (ICMP, ARP, RARP)
- Fragmentation et Réassemblage
- Routage: Généralités
- Algorithmes de Routage (LSR, DVR)
- Protocoles de RTG Internet I (RTG intra-domaine: RIP, OSPF)
- Protocoles de RTG Internet II (RTG inter-domaine: BGP)

Adressage: Généralités

Adressage hiérarchique pour faciliter le routage

- Plusieurs niveaux hiérarchiques dans un réseau.
- La hiérarchie n'est pas nécessairement la même. Pour chaque réseau:
  - Le nombre de niveaux est variable
  - La longueur des champs est variable



- Exemples: adressage postale, adressage téléphonique, adressage X.25 (ISO)

Adressage IP

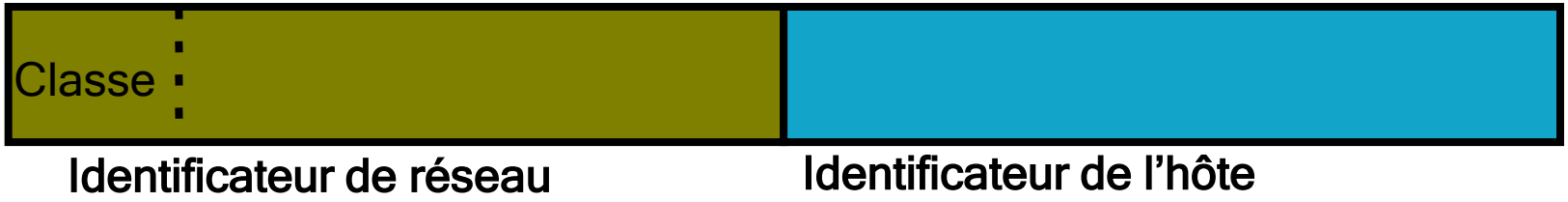
Une adresse IP est constituée de 4 Octets (32 bits).

1 réseau IP = 1 plage IP constituée :

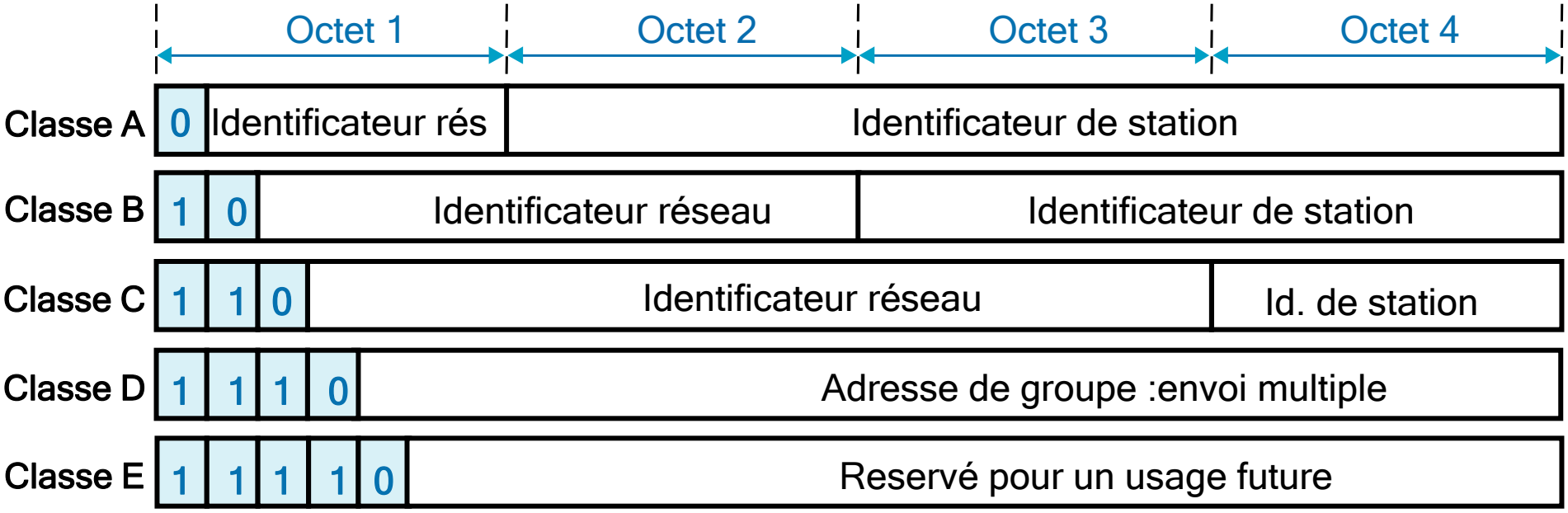
- d'une adresse réseau (première adresse de la plage).
- d'une adresse broadcast (la dernière adresse de la plage).
- d'adresses machines hôtes (le reste des adresses de la plage).

Méthodes de découpage des plages d'adresses :

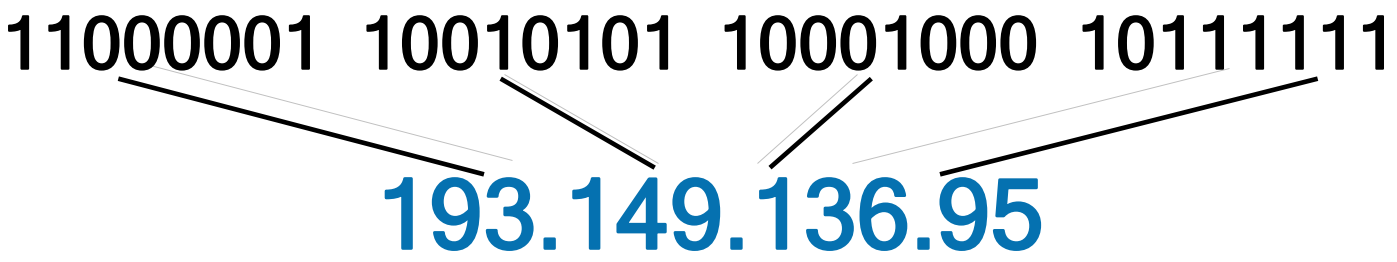
- avec Classes.
- CIDR (Classless Inter-Domain Routing).
- VLSM (Variable Length Subnetwork Mask), sorte de CIDR local à l'entreprise.



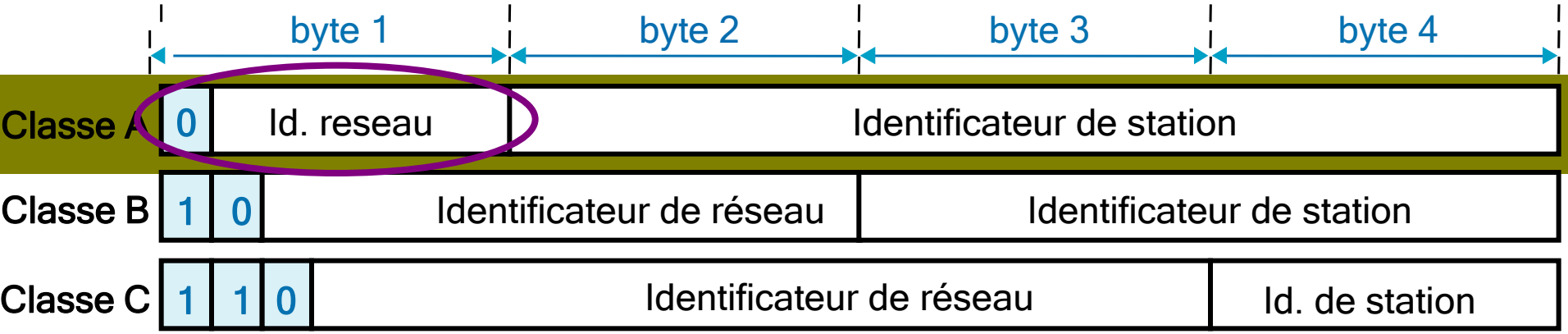
Classes d'adresses IP



Exemple: adresse de classe C



Classes d'adresses IP



BYTE 1

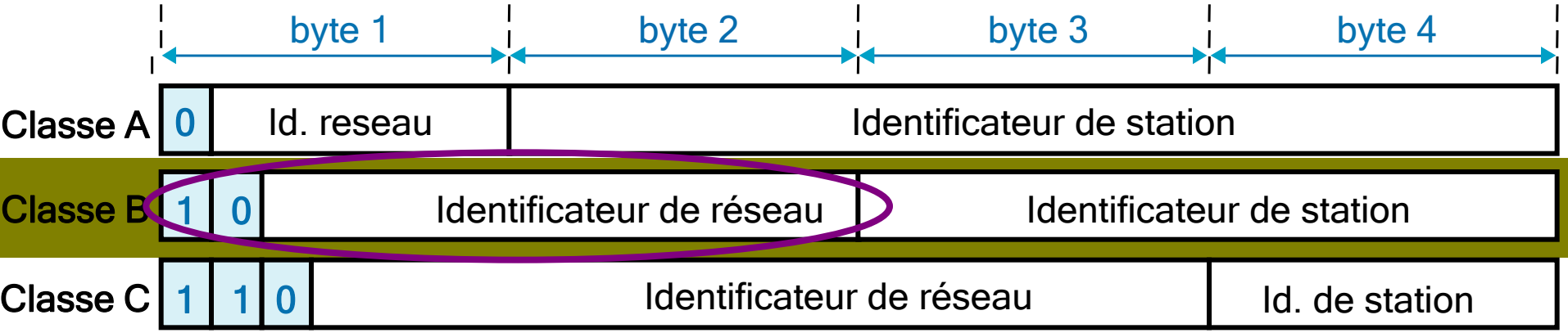
00000000 → **01111111**

	De	**Jusqu'à**
Classe A	0 .0.0.0	127.255.255.255
	Identificateur de réseau / **Identificateur du host**	**Identificateur de réseau** / **Identificateur du host**

128 réseaux x 2^{24} machines

Pour les grand réseaux : US NSFNet

Classes d'adresses IP



BYTES 1 et 2

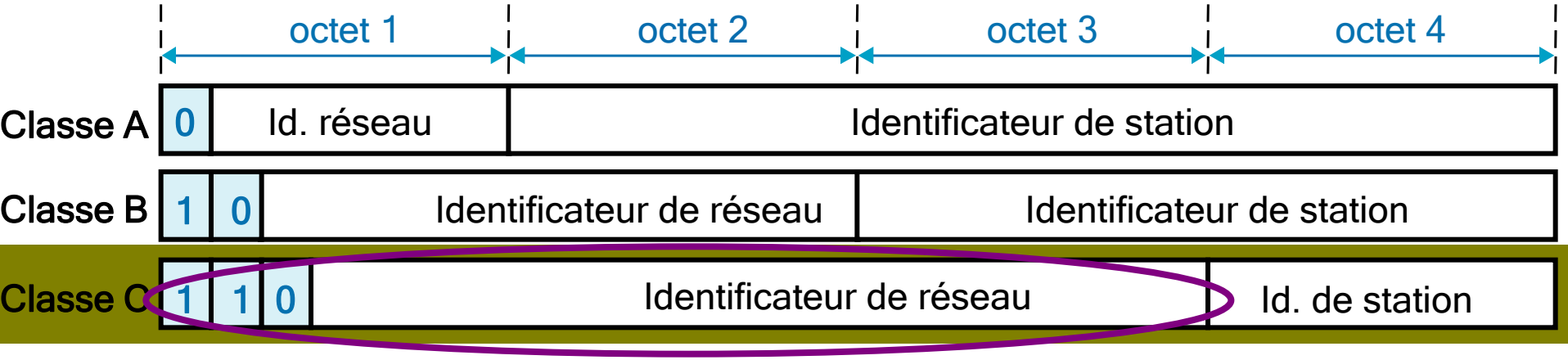
10000000 . 00000000 → **10111111 . 11111111**

	De	Jusqu'à
Classe B	128.0.0.0	191.255.255.255
	Identificateur de réseau / Identificateur du host	Identificateur de réseau / Identificateur du host

2^{14} réseaux x 2^{16} machines

Organisations avec plus de 65 000 ordinateurs telles que les universités.

Classes d'adresses IP



BYTES 1, 2 et 3

11000000 . 00000000 . 00000000

11011111 . 11111111 . 11111111

De **Jusqu'à**

Classe C 192.0.0.0 223.255.255.255

Identificateur de réseau **Identificateur du host** **Identificateur de réseau** **Identificateur du host**

2^{21} réseaux x 2^{8} machines

Pour petites entreprises et autres types de réseaux

Classes d'adresses IP

Masque de réseau

- Indique la partie d'une adresse qui correspond à l'identifiant du réseau
  - Mise à **1** de tous les bits **id réseau**
  - Mise à **0** de tous les bits **id machine**

Classe	Bits du netmask	Notation netmask
A	11111111 00000000 00000000 00000000	255.0.0.0 /8
B	11111111 11111111 00000000 00000000	255.255.0.0 /16
C	11111111 11111111 11111111 00000000	255.255.255.0 /24

Adresses particulières

Les plages IP à ne pas router (réseaux privés)

- Classe A: de 10.0.0.0/8 à 10.255.255.255/8
- Classe B: de 172.16.0.0/16 à 172.31.255.255/16
- Classe C: de 192.168.0.0/24 à 192.168.255.255/24

Les adresses IP réservées

- 0.0.0.0 => utilisée comme adresse de routage par défaut dans une table de routage.
- 255.255.255.255 => diffusion limitée à tous les hôtes du sous-réseau.
- 127.0.0.1 => boucle locale (localhost)
- 224.0.0.0 => adresses multicast

Les adresses interdites

- 128.0.x.x , 191.255.x.x , 192.0.0.x , 223.255.255.x , 0.x.x.x

Adresse du réseau : tous les bits machine à 0

- Exemple : la machine 192.168.0.1 appartient au réseau 192.168.0.0 (classe C)

Adresse de diffusion (broadcast) : tous les bits machines à 1

- Exemple : l'adresse broadcast du réseau 192.168.0.0 (classe C) est 192.168.0.255

Adressage IPv4 avec classes

Utilisation inefficace des adresses

- Réseau classe C avec 2 hôtes (2/255 = 0.78% utilisation)
- Réseau classe B avec 256 hôtes (256/65535 = 0.39% utilisation)

Prolifération des réseaux

- Taille des tables de routage des routeurs du réseau Internet.
- Efficacité des protocoles de routage.

Solution → CIDR : Classless Inter-Domain Routing

Adressage IP avec Subnetting

CIDR Classless Inter-Domain Routing

- Des plages d'adresses CIDR ont été déléguées à des ISPs (Internet Service Providers) qui à leur tour divisent ces plage entre utilisateurs ou autres ISPs.

- Agrégation de plusieurs adresses telle qu'une seule adresse peut représenter des milliers d'abonnés à un même ISP.

- Alléger la charge des routeurs d'Internet.

Préfixes CIDR

CIDR: Classless Inter-domain Routing

- Utilisation d'un préfixe variable.
- Meilleure utilisation des plages d'adresses IP.
- Eviter la saturation des tables de routage.

CIDR Prefix	Number of Hosts
/13	524,288
/14	262,144
/15	131,072
/16	65,536
/17	32,768
/18	16,384
/19	8,192
/20	4,096
/21	2,048
/22	1,024
/23	512
/24	256
/25	128
/26	64
/27	32

CIDR

Les plages d'adresses réseaux 193.94.0.0/24 -193.94.255.0/24 est équivalente à 193.94.0.0/16

Exemple: Une société a besoin de 2000 adresses.

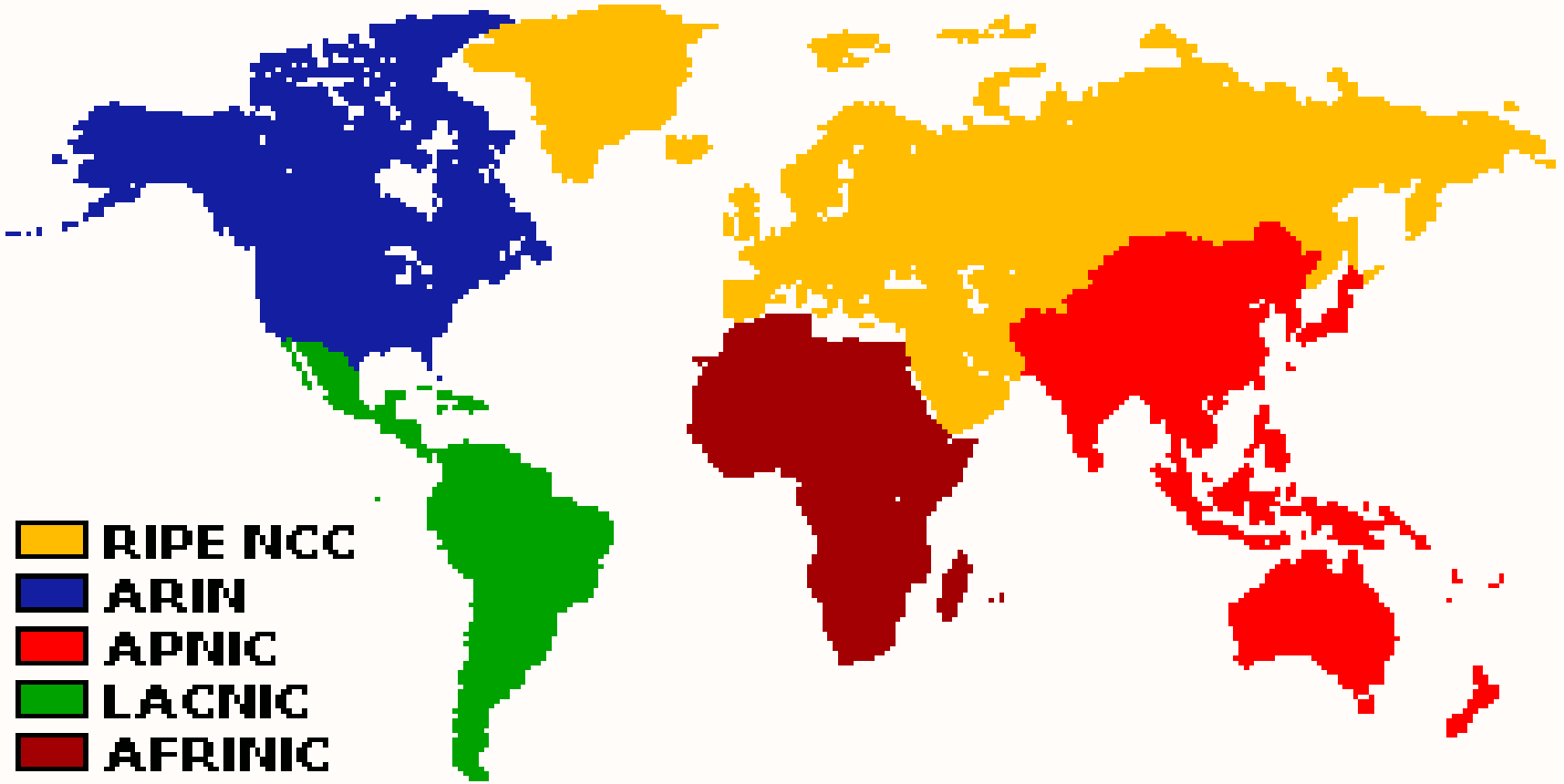
Adresse de classe B: Perte de plus de 64000 adresses

On attribue 8 plages d'adresses de classe C contiguës:

- De 192.24.0.0/24 à 192.24.7.0/24

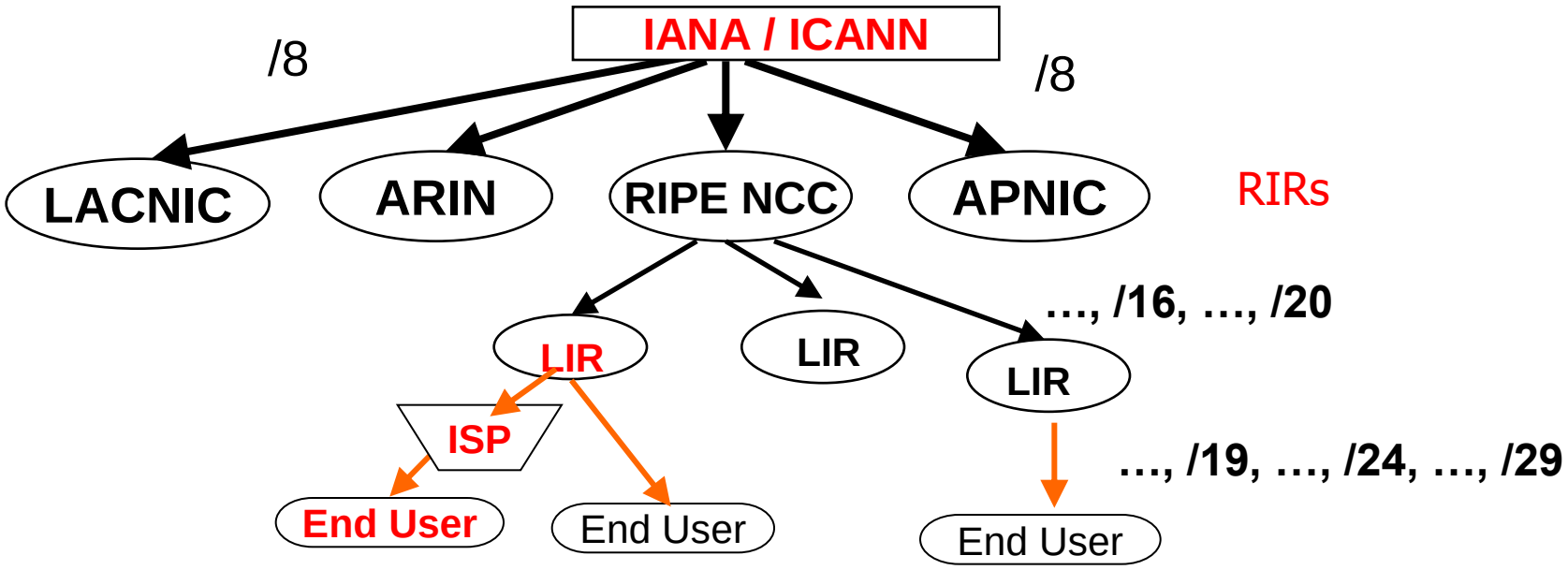
Avec CIDR : 192.24.0.0/21 (Masque 255.255.248.0)

Distribution des adresses IP



5 **RIR** (Regional Internet Registry) : Registre Régional d'Internet à travers le monde.
AFRINIC (AFRIcan Network Information Centre)

Distribution des adresses IP



IANA Internet Assigned Numbers Authority

ICANN Internet Corporation for Assigned Names and Numbers

LIR Local Internet Registry

Chapitre II: La Couche Réseau

- Le Concept d'Interconnexion
- Architecture Internet
- Adressage IP
- IP et protocoles associés (ICMP, ARP, RARP)
- Fragmentation et Réassemblage
- Routage: Généralités
- Algorithmes de Routage (LSR, DVR)
- Protocoles de RTG Internet I (RTG intra-domaine: RIP, OSPF)
- Protocoles de RTG Internet II (RTG inter-domaine: BGP)

Protocoles

Protocoles de Routage

- ISO : **CLNP** ConnectionLess Network Protocol
- Internet : **IP** (Internet Protocol)

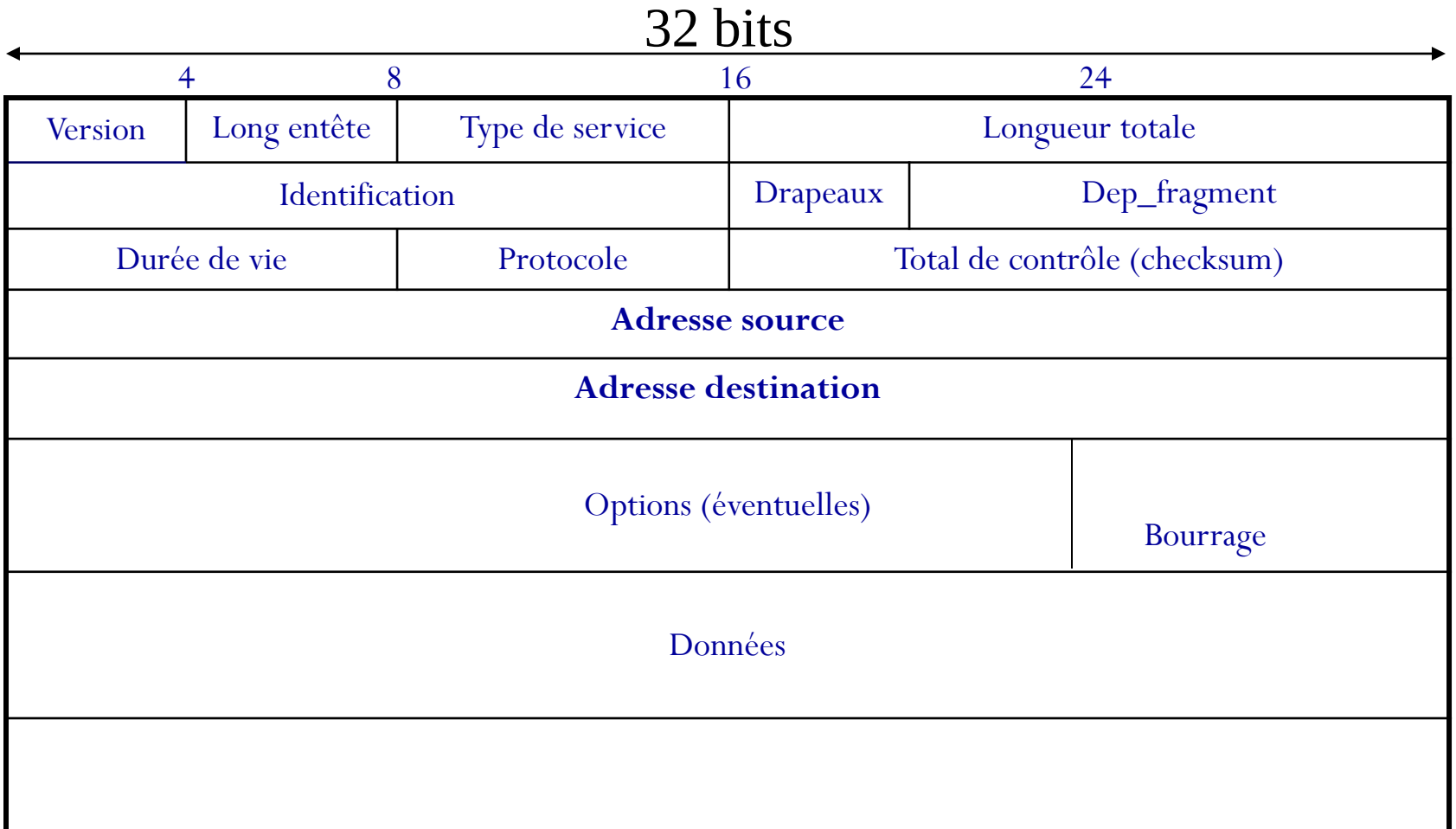
Messages d'erreurs (informations pour source)

- ISO : **partie de CLNP**
- Internet : **ICMP** (Internet Control Message Protocol)

Format des paquets IP

En-tête : partie fixe (20 Octets) + partie optionnelle variable

Données : charge utile du paquet



Format des paquets IP

Champs	Description	Long.
Version	Version du protocole IP doit être supportée par la destination	4 bits
Long entête	Longueur de l'entête en multiple de 32 bits	4 bits
Long Totale	Longueur totale du paquet en octets (jusqu'à 2^{16})	16 bits
Indentification	Numéro de séquence du paquet. Indique à quel paquet appartient un fragment.	16 bits
Drapeaux	**DF** : " Don't fragment ", **MF** : " More fragments ", 1bit inutilisé	3 bits
Dep_fragment	Localisation du fragment dans le paquet. On l'appelle offset. La valeur est en multiple de huit octets.	13 bits
Durée de vie (TTL)	Indique le nombre maximal de sauts (routeurs) pour un paquet : valeur décrémentée à chaque routeur, paquet détruit quand TTL= 0	8 bits
Protocole	Indique par un numéro le protocole de niveau supérieur utilisé (TCP ou UDP ou ICMP).	8 bits
Checksum	Vérifie le champs en-tête, doit être recalculé à chaque saut	16 bits
Bourrage (Padding)	Bits à 0 rajoutés pour avoir une longueur d'entête multiple de 32 bits car longueur du champs « options » est variable	0-4 octets

Format des paquets IP

Type de service

- précise le mode de gestion du paquet (8 bits)

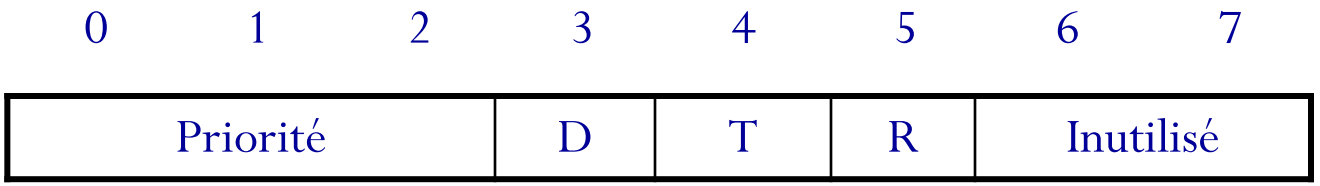
- Informations pour les algorithmes de routage pouvant servir pour le choix de routes satisfaisant certains critères de QoS.

- **Priorité** : 0 (normal) → 7 (supervision réseau)

Champs souvent ignoré, nécessite la prise en charge d'algorithmes de priorité au niveau des routeurs, suppose des files d'attente avec des niveaux de priorités différentes (DiffServ).

- **3 drapeaux** indiquant le type de service requis
  - Délai (**D**) : indique un besoin en courts délais,
  - Débit (**T**) : débit de transmission élevé,
  - Fiabilité (**R**)

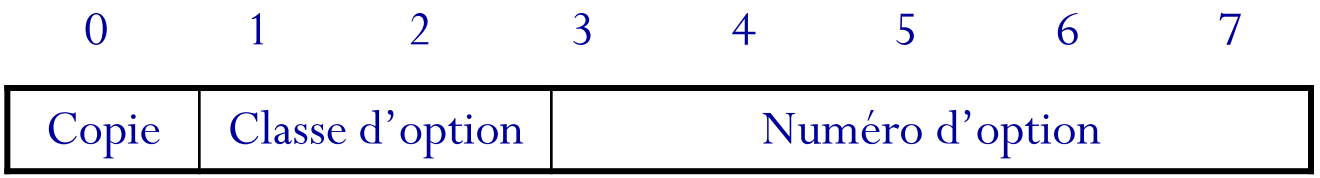
- **2 bits** inutilisés



Format des paquets IP

Options

- Champs optionnels, longueur variable
- Chaque type d'option est codé sur un octet (code option)
- Peut être suivi d'un octet précisant la longueur + ensemble d'octets de données associées à l'option



Code option :

- **Copie** : si 1 : option doit être recopiée dans tous les fragments
- **Classe d'option** :
  - 0 : paquet de contrôle ou supervision
  - 2 : paquet de mesure

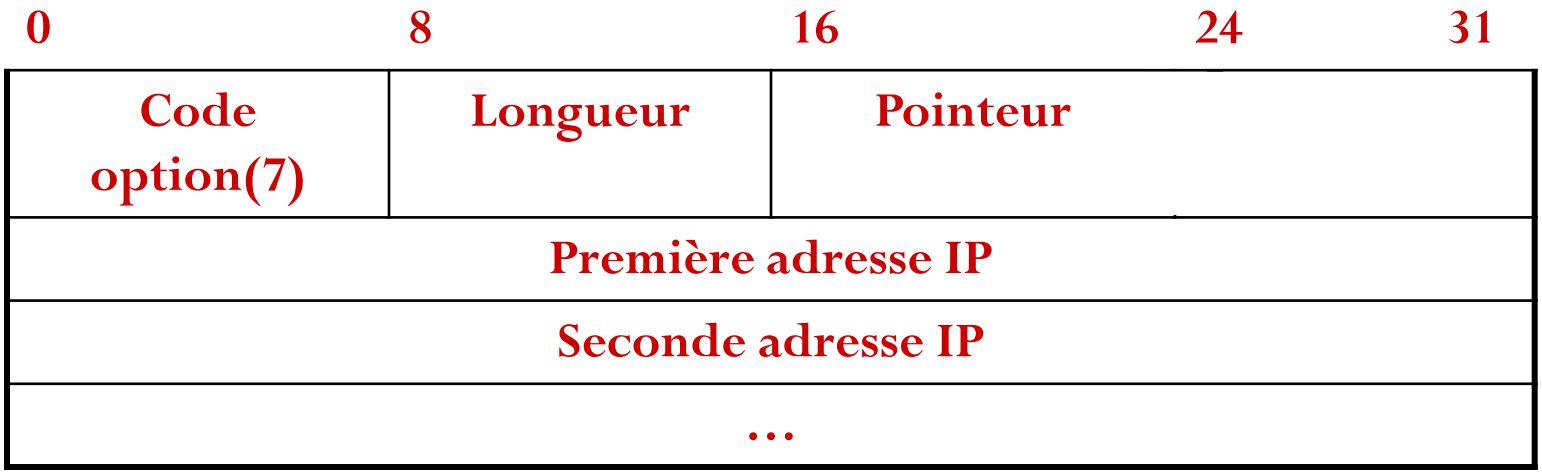
Format des paquets IP

- **Numéro d'option** : identificateur de l'option. Exemples :
  - **3** (classe option 0) **: Option Routage source :** spécifie la route à prendre par le paquet. Le champs code sera alors suivi par un champs d'options comportant la description de la route.
  - **7** (classe option 1) **: Option Enregistrement de route** : utilisé pour enregistrer un itinéraire, chaque routeur fournissant son adresse IP au paquet.
  - **4** (classe option 2) : **Horodatage** dans Internet. Pour enregistrer l'horodatage le long d'une route.

Format des paquets IP

Option Enregistrement de route

- La source initialise la longueur qu'elle suppose nécessaire.
- Au niveau d'un routeur intermédiaire, si « pointeur » est inférieur à « longueur », le routeur ajoute son adresse IP dans le déplacement indiqué par « pointeur » et incrémente pointeur de 4 octets, sinon il achemine le paquet sans y insérer son adresse.



Liste de routage associée à l'option enregistrement de route

ICMP Internet Control Message Protocol

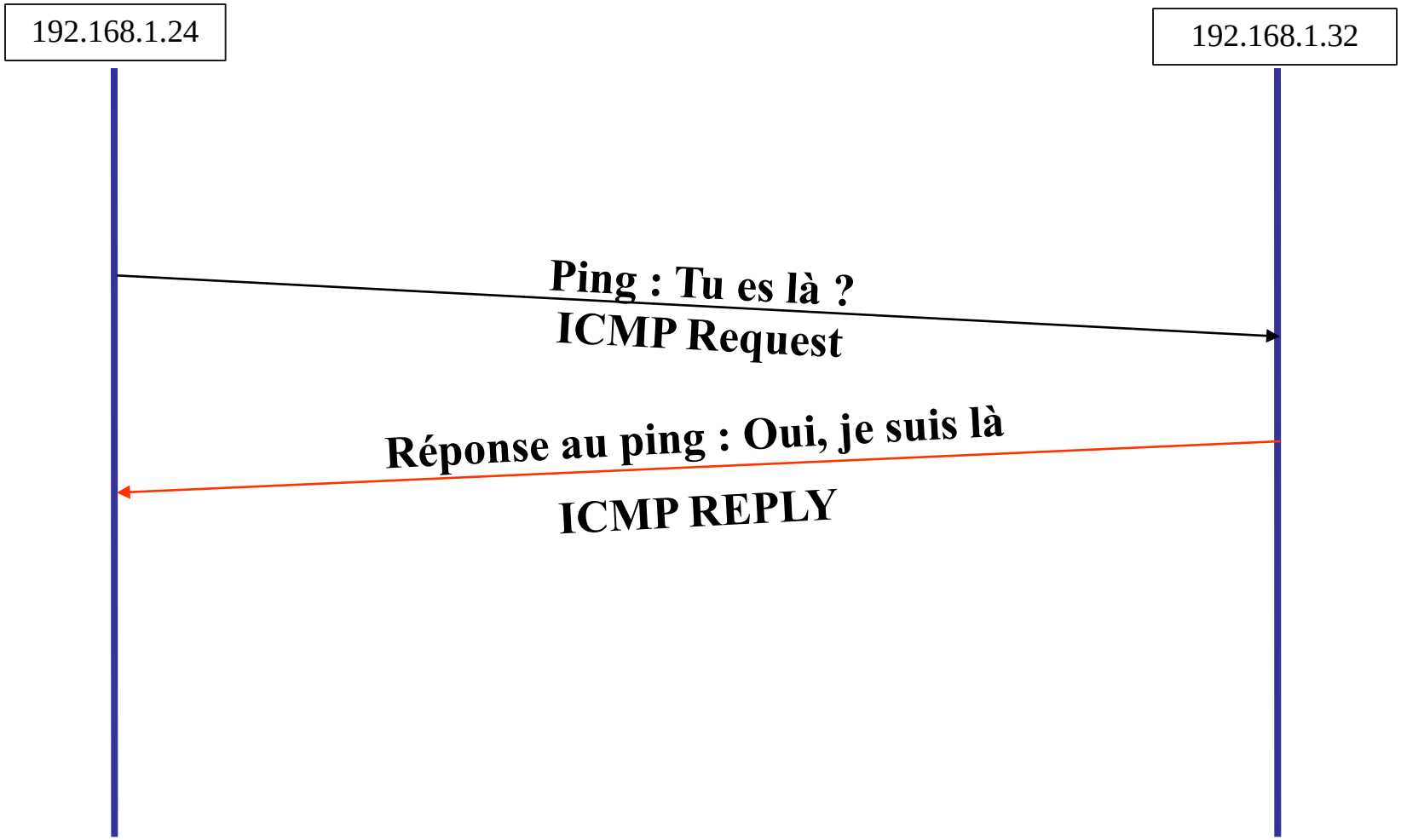
Échange de messages d'**erreur** et de **supervision**.

Rendre compte des problèmes « routeurs »

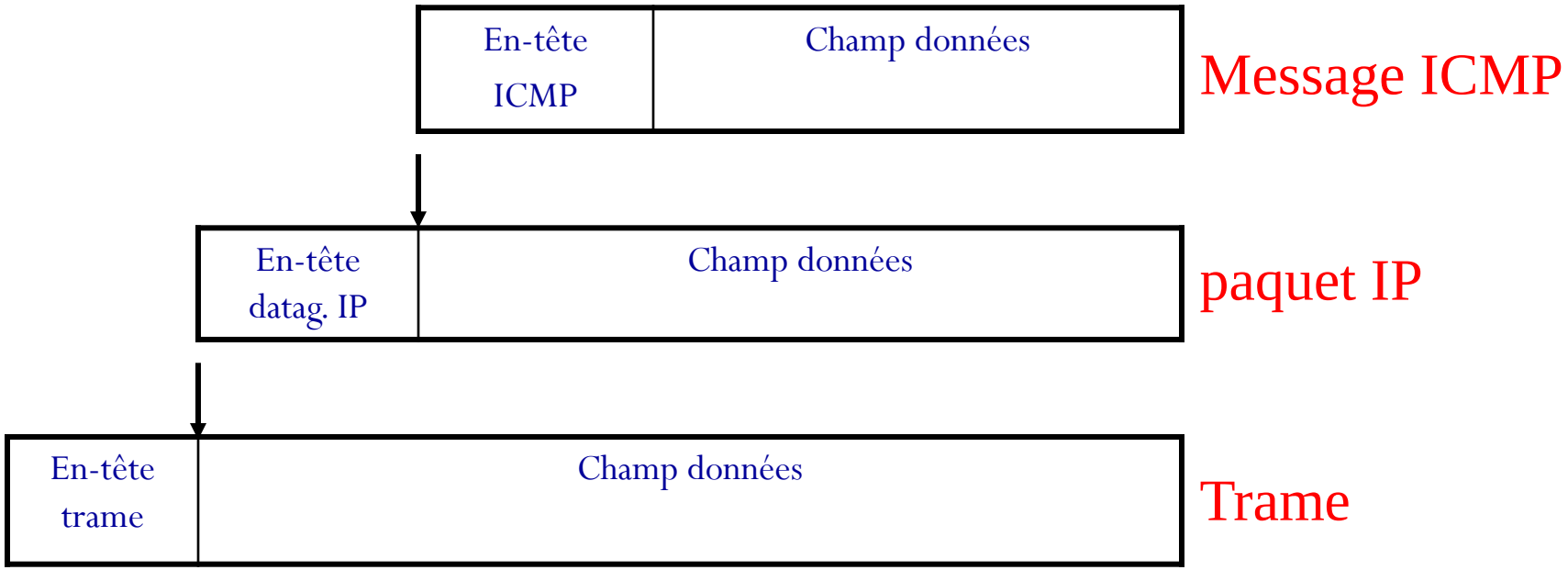
- paquet ne peut pas atteindre sa destination.
- Manque de mémoire tampon.
- Utilisation d'une route alternative pour optimiser le trafic.

Un message ICMP est encapsulé dans un paquet IP.

ICMP Exemple



ICMP (encapsulation)



ICMP (format)

Chaque message ICMP a un format propre.

Ils commencent tous par 3 champs (entête) :

- type (8 bits)
- code (8 bits) info. supplémentaire sur le type
- total de contrôle – checksum (16 bits)

+ 64 premiers bits du paquet ayant provoqué l'erreur (cas de messages d'erreur).

ICMP

Type	Signification
0	réponse à une demande
3	destination inaccessible
4	réduction du débit d'émission (Congestion)
8	demande
11	expiration du TTL
…	

ICMP

- Déterminer si une destination est connectée au réseau (**ping**)
  type= 8/requête; 0/réponse ; Code = 0
  Identifier/Sequence number (2 octets) , et 2 octets pour mesure du RTT

- Echange de date (Timestamp)
  type = 13/requête; 14/réponse
  Code = 0
  Receive timestamp (4 octets): temps à la réception de la requête.
  Transmit timestamp (4 octets): temps à l'émission de la réponse.

- Demande d'une adresse réseau
  type = 15/requête; 0/réponse
  Code = 0
  « Obsolète » car remplacé par BOOTP ou DHCP

ICMP

- Demande du masque du sous-réseau

  type 17/requête; 18/réponse ;

  Code = 0

  Identifier/Sequence number (4 octets) : identifier la requête et sa réponse

  Address mask : 4 octets

- Le réseau est en congestion; la source doit diminuer son utilisation réseau

  type = 4; Code = 0

  Entête IP + 64 bits du paquet cause du problème

- Reroutage (Indication de changement de route)

  type = 5; Code (indique la nature de la redirection).

ICMP

Messages d'erreurs

type (1 octet) + **code** (1 octet)+ checksum (2 octets) + données spécifiques au type (4 octets)+ entête Internet (variable) + 64 bits du paquet cause du problème.

- Problème de paramétrage (Cause: erreur)

  type = 12, code = 0

  Pointer : 1 octet; pointeur de l'erreur

- TTL expiré

  type = 11

  Code = 0 : expiré en transit ; Code = 1 : expiré pendant réassemblage

- Destination inaccessible

  type = 3

  Code = 0 : net unreachable ; Code = 1 : host unreachable ; Code = 2 : protocol unreachable ; Code = 3 : port unreachable

Adresses MAC et IP

- Les adresses IP sont utilisées pour l'acheminement des paquets.

- Tout ordinateur a une adresse MAC sur 48 bits attribuée par le constructeur .

Adresse IP (32 bits) ≠ adresse MAC (48 bits)

- Comment translater les adresses IP en adresses MAC?

=> Protocole ARP

.

Protocole ARP Address Resolution Protocol

Fonctionnement :

- Une machine émet un paquet en diffusion qui demande « Qui possède l'adresse IP x.y.z.t ? » à chaque ordinateur du réseau local destination.

- Chaque machine vérifie sa propre adresse et seule la machine ayant l'adresse IP correspondante envoie en réponse son adresse Ethernet.

Utiliser un cache pour enregistrer les adresses Ethernet des machines.

Protocole RARP

Problème :
Pour une adresse Ethernet donnée, quelle est l'adresse IP correspondante ?

→ protocole Reverse ARP.

- Utilisé au démarrage du réseau pour l'affectation des adresses IP.

- Le serveur RARP consulte les adresses Ethernet à partir des fichiers de configuration, et renvoie une adresse IP à chaque ordinateur du réseau local.

Remplacé dans la pratique par DHCP et BOOTP.

IPv4 et ses limites

Epuisement d'adresses.

N'implémente pas des mécanismes de sécurité

- authentification des paquets, intégrité, confidentialité
- Il a toujours été considéré que ces techniques étaient de la responsabilité des applications.

Les objectifs d'IPv6

- Supporter des milliards de machines → Adressage sur 16 octets (128 bits).

- Optimiser la taille des tables de routage.

- Router les paquets plus rapidement → en simplifiant le protocole (Utilisation des champs optionnels).

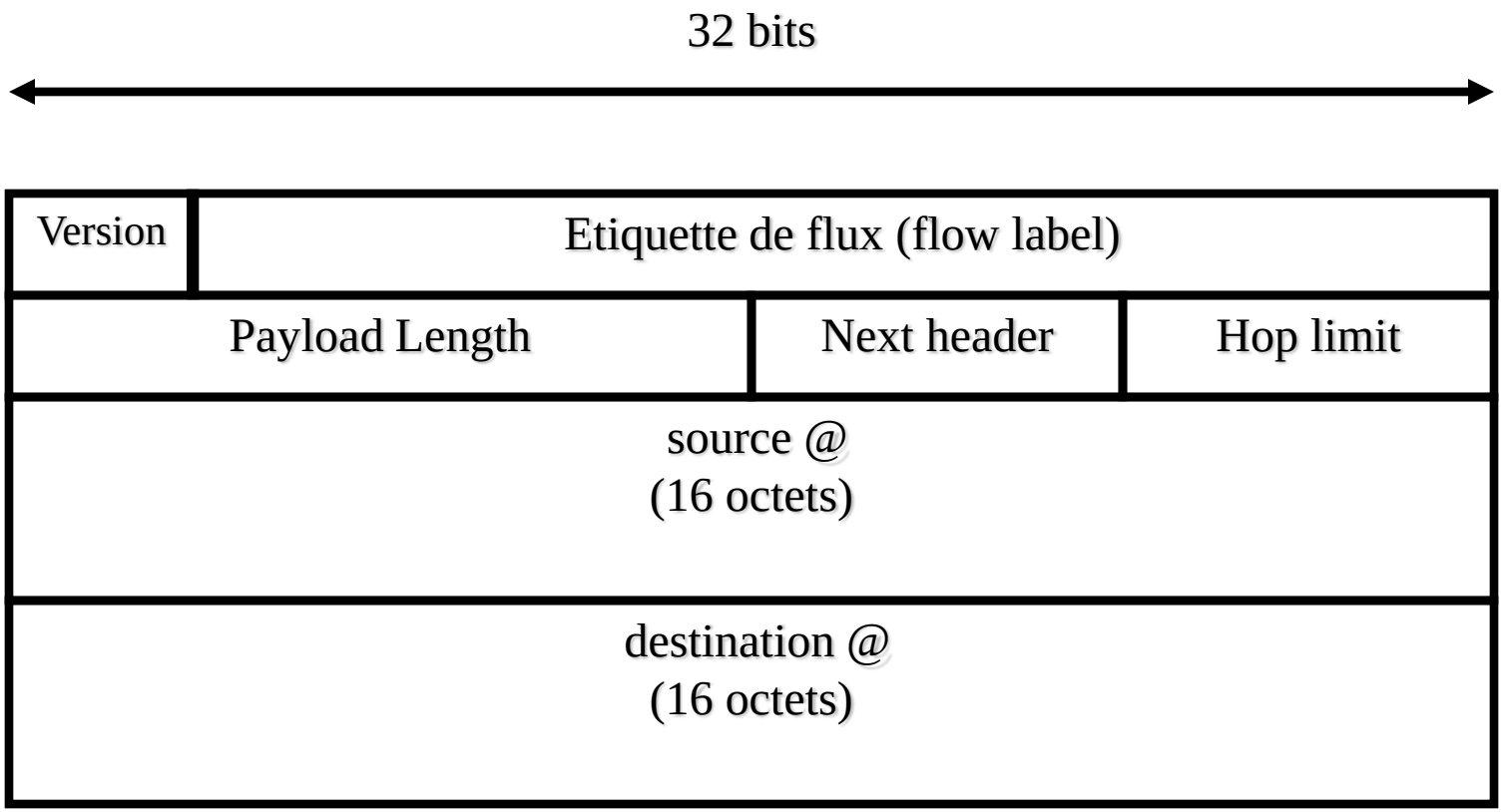
- Meilleure sécurité → authentification et confidentialité.

- Types de service

- Permettre une évolution future.

- Compatibilité avec IPv4.

Entête paquet IPv6



Les champs de l'entête IPv6

Version (4 bits): numéro de version du Protocole IP.

Flow Label (28 bits): étiquette de flux, peut être utilisé par une station pour "marquer" certains paquets afin qu'ils suivent un routage déterminé dans un réseau.

Payload Length (16 bits): représente la longueur des données après l'en-tête IPv6 en octets.

Next Header (8 bits): identifie le type d'en-tête suivant immédiatement l'en-tête IPv6. Ce champ ressemble au champs protocole d'IPv4.

Hop limit (8 bits): ce champs est décrémenté à chaque routeur qui retransmet le paquet (équivalent au champs TTL d'IPv4).

Source Address (128 bits): adresse IP de l'émetteur du paquet.

Destination Address (128 bits): adresse IP du destinataire du paquet.

Entêtes supplémentaires IPv6

IPv6 Next Header

Routing Header: utilisée pour le routage source.

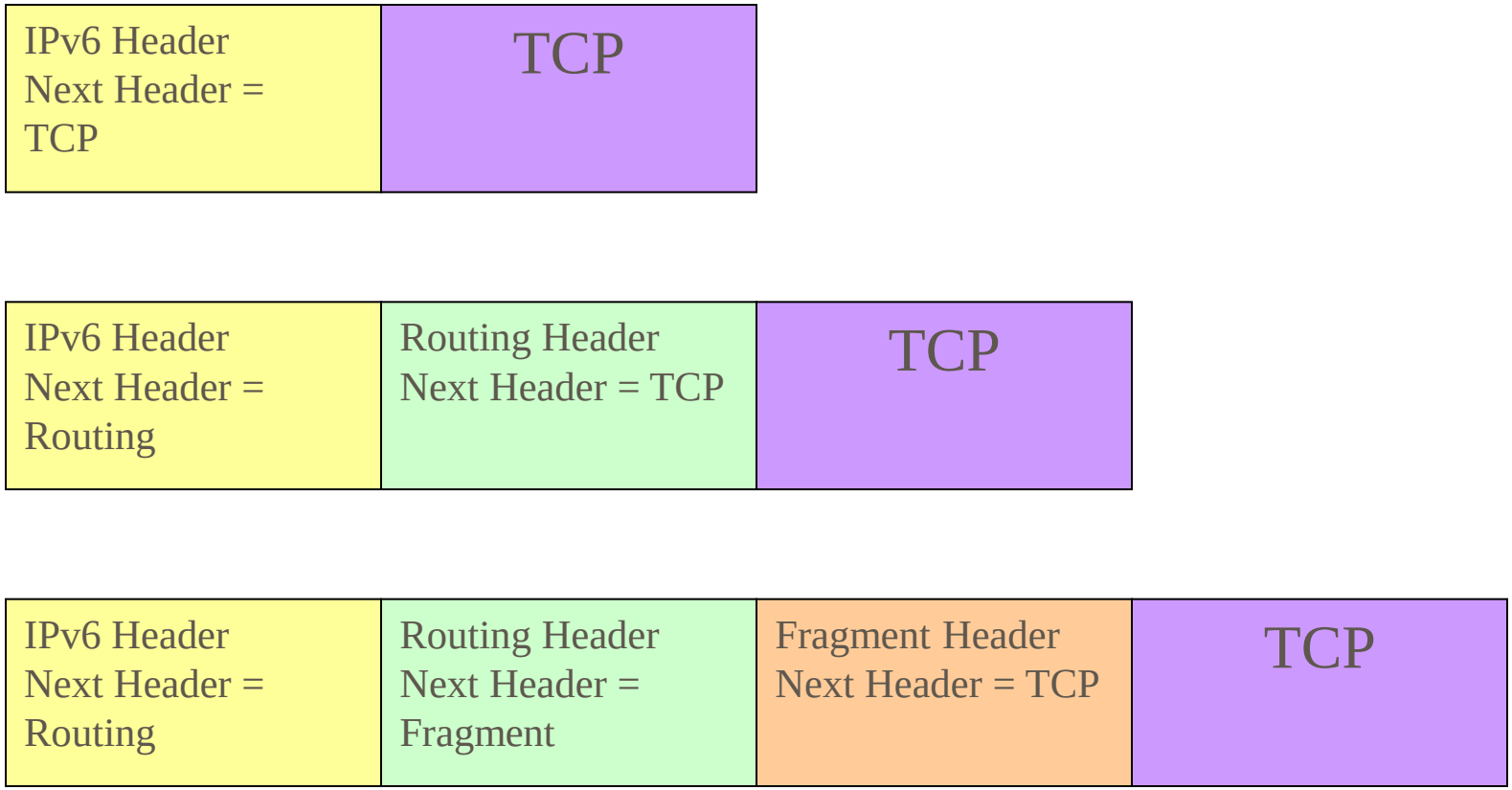
Fragment Header: gère la fragmentation des paquets.

Contrairement à IPv4, la fragmentation est exécutée uniquement par la source après découverte de la MTU.

Authentication Header: sécurité

Privacy Header: chiffrement

Entêtes supplémentaires IPv6
Exemple



L'adressage

Notation

- Les adresses sont représentées sur 128 bits
  - Une adresse est divisée en 8 blocs de 16 bits
  - Les blocs sont séparés par « : »
  - Les valeurs de chaque bloc sont écrites en hexadécimal (entre 0 et ffff)
- Exemples
  - 2002:8ac3:802d:1242:20d:60ff:fe38:6d16
  - 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

3 types d'adresse :

- Unicast
- Multicast : envoyer un paquet à un groupe d'utilisateurs
- Cluster ou anycast : identifier un groupe d'utilisateurs qui ont en commun un préfixe d'adresse. Un paquet envoyé à une adresse cluster sera délivré à un membre du groupe.

Représentation des adresses

Normal:
x:x:x:x:x:x:x:x (x=16bits en hexa)
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:8:800:200C:417A

Compressé: FF01:0:0:0:0:0:0:43 ⇒ FF01::43

IPv4:
x:x:x:x:x:x:d.d.d.d
0:0:0:0:0:0:13.1.68.3 ⇒ ::13.1.68.3

Exemples d'adresses particulières

- Adresse Unspecified : 0:0:0:0:0:0:0:0
- Adresse localhost : FE00:0:0:0:0:0:0:1

Configuration d'adresse

- Configuration manuelle
  - L'administrateur fixe l'adresse.
- Configuration automatique
  - Utiliser le protocole de configuration dynamique des stations pour IPv6 [Dynamic Host Configuration Protocol DHCPv6].

ICMPv6

Version modifiée d'ICMP (ICMPv6)

La nouvelle version IP emploie le protocole ICMP de la même manière que pour IPv4, avec quelques changements.

Neighbor Discovery

- Découverte des routeurs voisins (directement connectés)

Path MTU Discovery

- MTU : taille maximale du paquet pouvant être transportée sans fragmentation.
- Path MTU = min des MTU sur l'ensemble des liens du chemin.

Gestion de la mobilité (Protcole MobileIP - MIP)

Chapitre II: La Couche Réseau

- Le Concept d'Interconnexion
- Architecture Internet
- Adressage (IP, OSI)
- IP et protocoles associés (ICMP, ARP, RARP)
- Fragmentation et Réassemblage
- Routage: Généralités
- Algorithmes de Routage (LSR, DVR)
- Protocoles de RTG Internet I (RTG intra-domaine: RIP, OSPF)
- Protocoles de RTG Internet II (RTG inter-domaine: BGP)

Fragmentation

Paquet IP :

- a une taille variable : jusqu'à 65 535 Octets
- doit être encapsulé dans une trame
- transite par plusieurs réseaux caractérisés par une valeur **MTU,** Unité de Transfert Maximale différente.
  - Exemples : MTU Ethernet=1500 octets, MTU FDDI=4470 octets.

- À l'entrée de réseaux ayant une valeur MTU inférieure, un paquet est découpé en fragments → fragmentation.

- La fragmentation est réalisée par des routeurs.

- La taille des fragments est choisie de telle sorte qu'elle puisse être encapsulée dans une trame du réseau de transit.

Fragmentation et Réassemblage

Deux stratégies de Fragmentation/ Ré-assemblage

(1) Paquet fragmenté par le routeur à l'entrée du réseau et ré-assemblé par le routeur à la sortie du réseau « **Intranet Segmentation Strategy** »

- Les fragments sont stockés au niveau des routeurs, jusqu'à la réception de tous les fragments d'un paquet.
- Réassemblage répétitif.

Fragmentation et Réassemblage

(2) Le réassemblage se fait à la destination « **Internet Segmentation Strategy** »

- Les fragments générés sont acheminés indépendamment vers la destination.
- Au niveau de la destination un temporisateur de réassemblage est déclenché à la réception d'un premier fragment.
- Si au bout de ce temporisateur tous les fragments d'un même paquet ne sont pas reçus, tous les fragments sont détruits.

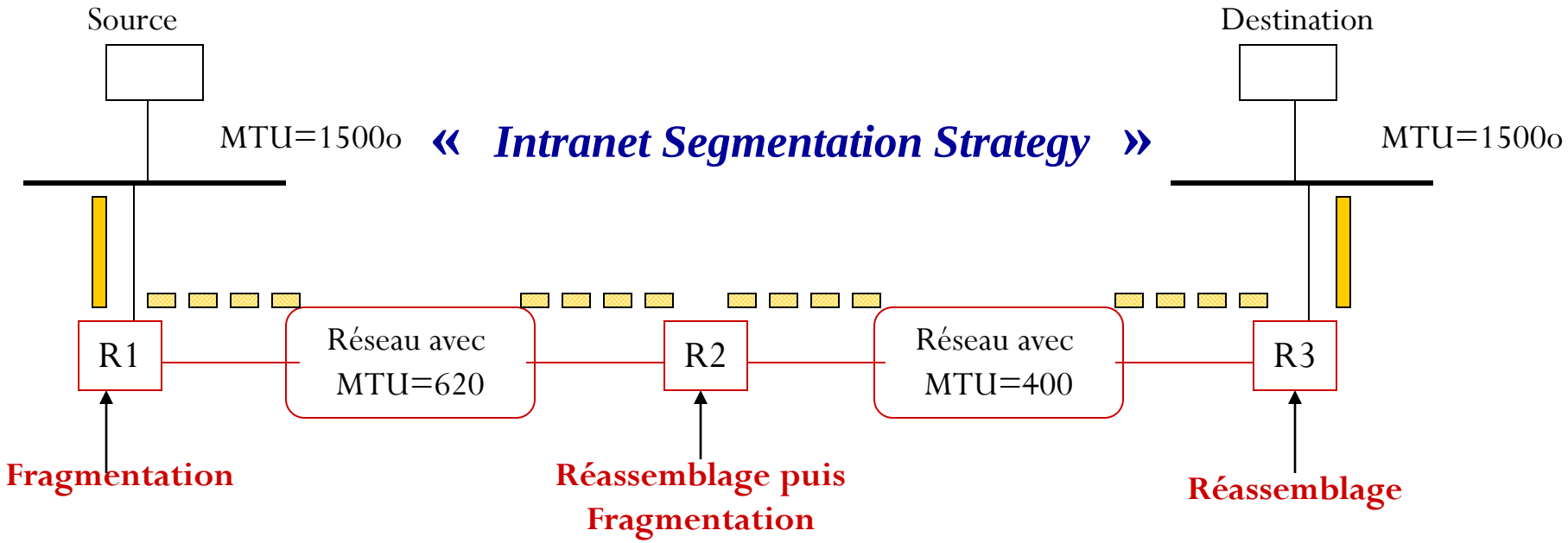
- **Inconvénients :**

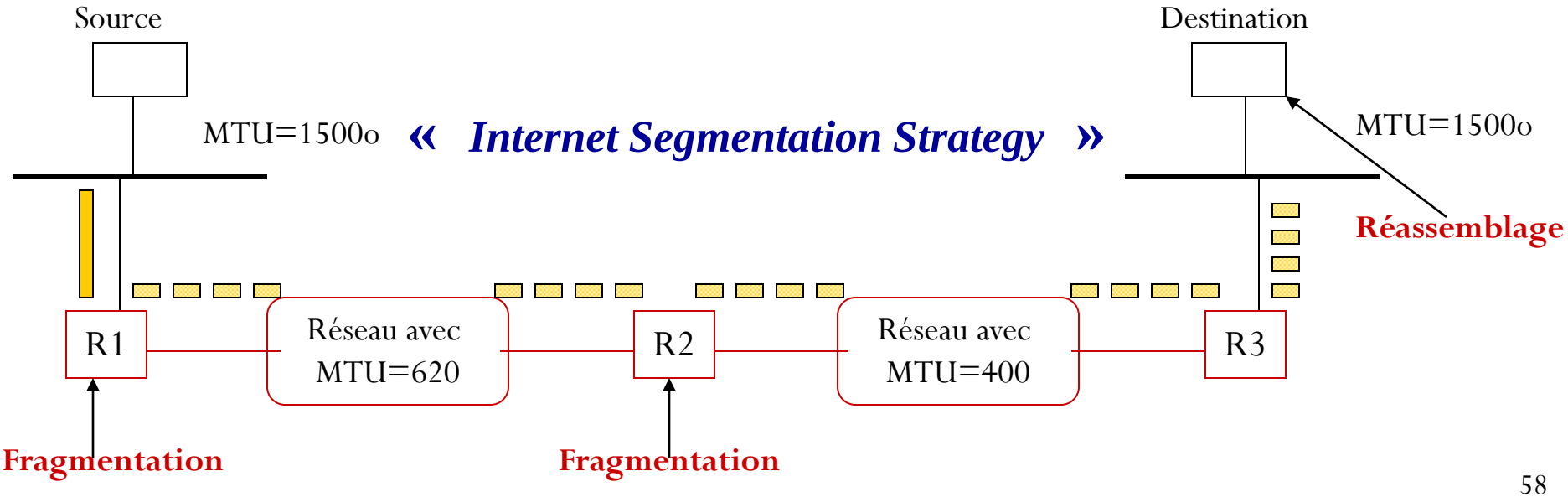
Nombre plus grand de fragments

- **Avantages :**

Alléger la charge des routeurs d'Internet → meilleurs délais, moindre coût en mémoire des routeurs, etc.

Fragmentation et Réassemblage





Fragmentation et Réassemblage

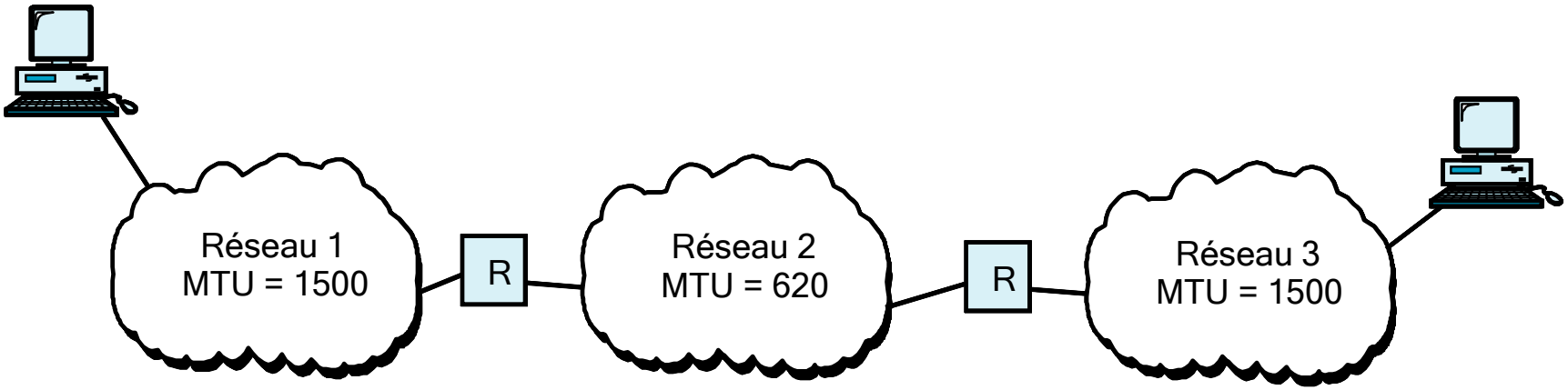
Rappels des champs utilisés dans l'entête IP

- Champs recopiés : adresse IP Source + adresse IP destination + protocole + identification

- Champs pouvant changer d'un fragment :
  - "longueur totale"
  - "offset field"
  - "more fragments"

Fragmentation et Réassemblage

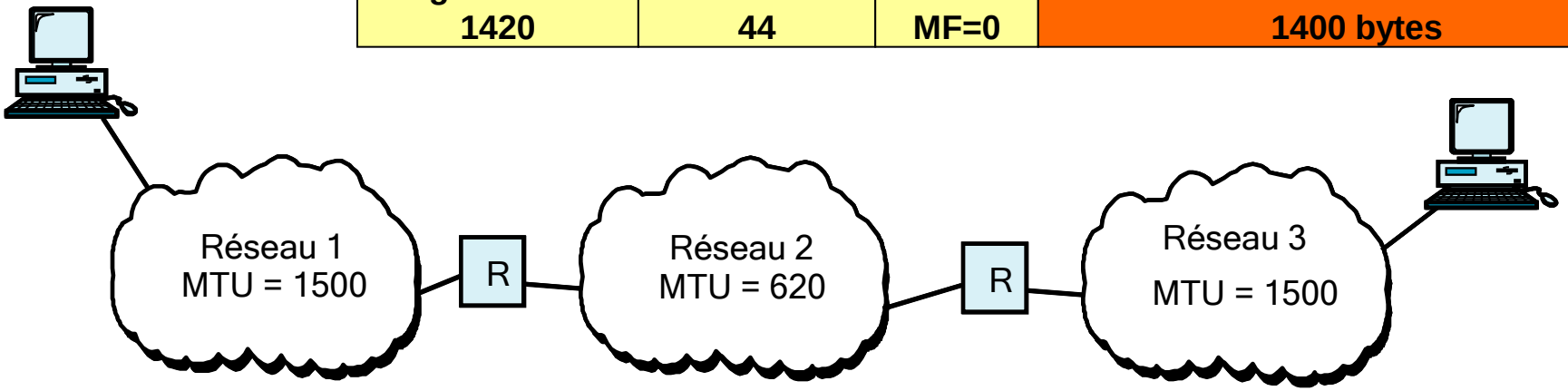
- **Exemple: paquet de 1420 octets**



Longueur Totale 1420	Identificateur 44	DF=1 MF=0	Données 1400 bytes

Fragmentation et Réassemblage

Longueur Totale 1420	Identificateu 44	DF=1 MF=0	Données 1400 bytes



Longueur Totale 620	Identificateur 44	DF=0 MF=1	Offset (0)	Données 1 600 bytes

Longueur Totale 620	Identificateur 44	DF=0 MF=1	Offset 75 (600)	Données 2 600 bytes

Longueur Totale 220	Identificateur 44	DF=0 MF=0	Offset 150 (1200)	Données 3 200 bytes

Chapitre II: La Couche Réseau

- Le Concept d'Interconnexion
- Architecture Internet
- Adressage (IP)
- IP et protocoles associés (ICMP, ARP, RARP)
- Fragmentation et Réassemblage
- Routage: Généralités
- Algorithmes de Routage (LSR, DVR)
- Protocoles de RTG Internet I (RTG intra-domaine: RIP, OSPF)
- Protocoles de RTG Internet II (RTG inter-domaine: BGP)

Introduction

Réseau étendu = Interconnexion de plusieurs réseaux par des routeurs.

Chaque routeur est connecté directement à 2 ou plusieurs réseaux, en général, les machines hôtes ne sont connectés qu'à un seul réseau.

Types de remise de paquets :

Remise directe

Transfert direct de paquets entre 2 ordinateurs connectés au même réseau ne nécessite pas des routeurs.

Remise indirecte

- Il faut identifier un routeur vers lequel envoyer un paquet.
- Un paquet transite de routeur en routeur jusqu'au réseau destination.

Tables de routage

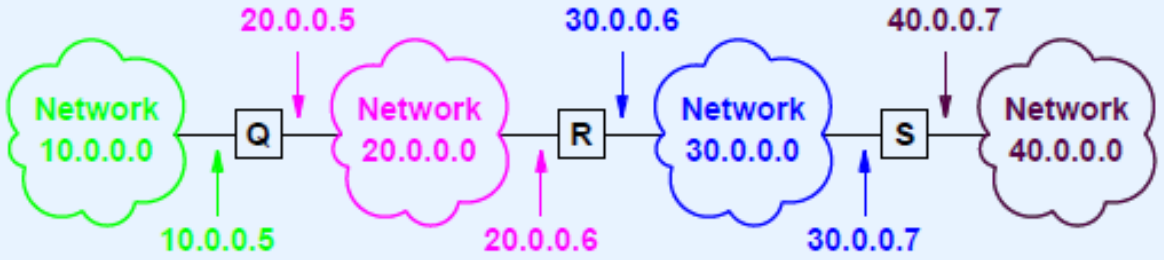
Table de routage:

- Initialisation
- Mise à jour (via Protocole)

- La table contient, pour chaque réseau à atteindre, l'adresse IP de l'interface du routeur suivant (passerelle) qui mène au réseau destination.

- Si aucune entrée n'existe pour un réseau donné dans la table de routage, le paquet est envoyé à un routeur par défaut.

Tables de routage



An example Internet with IP addresses

Destination	Interface	Passerelle
20.0.0.0 / 8	20.0.0.6	DELIVER DIRECT
30.0.0.0 / 8	30.0.0.6	DELIVER DIRECT
10.0.0.0 / 8	20.0.0.6	20.0.0.5
40.0.0.0 / 8	30.0.0.6	30.0.0.7

The routing table for router R

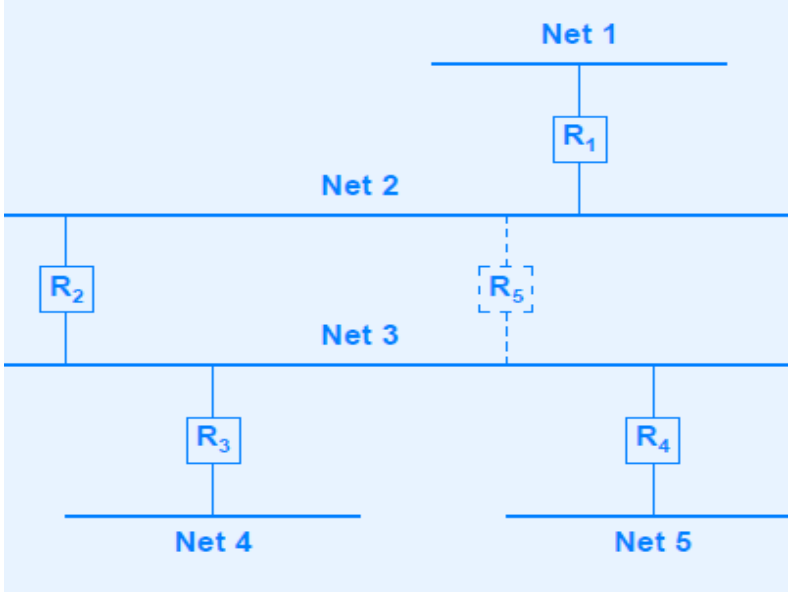
Types de Routage

Routage statique, non adaptatif

- Routes fixées au démarrage (configuration des tables de routage).
- Algorithme du plus court chemin (optionnel).

Routage dynamique

- Table de routage initialisée au démarrage + mise à jour via propagation d'informations.
- Nécessaire pour de larges réseaux (Internet, réseau sur grande étendue géographique).
- Routage à vecteur de distance (Bellman-Ford)
- Routage à états de liens (Dijkstra)



Principales Opérations dans le Routeur

- Les champs « TTL » et « Total de contrôle » sont modifiés par les routeurs.

- Les champs source et destination ne sont pas affectés : ils contiennent toujours l'adresse de l'émetteur initial et celle du destinataire final.

- L'adresse du routeur suivant n'est pas enregistrée dans le paquet mais elle est calculée à partir de la table de routage.

- Après avoir calculé l'adresse, le paquet est encapsulé dans une trame et envoyé.

Chapitre II: La Couche Réseau

- Le Concept d'Interconnexion
- Architecture Internet
- Adressage (IP, OSI)
- IP et protocoles associés (ICMP, ARP, RARP)
- Fragmentation et Réassemblage
- Routage: Généralités
- Algorithmes de Routage (DVR, LSR)
- Protocoles de RTG Internet I (RTG intra-domaine: RIP, OSPF)
- Protocoles de RTG Internet II (RTG inter-domaine: BGP)

Algorithmes de Routage

Objectif: Calculer la route d'une source vers une destination.

Propriétés

- Exactitude
- Simplicité
- Robustesse même en présence de pannes
- Stabilité : converge
- Equité avec possibilité d'avoir des priorités
- Optimalité : minimise les coûts

Algorithmes de Routage

2 classes d'algorithmes de Routage:

(1) Routage à Vecteur de Distance (DVR)

Exemple:

Algorithme de Bellman-Ford :

Distribué, Temps de Convergence Variable, O(d).

(2) Routage à Etats de Liens (LSR)

Exemple:

Algorithme de Dijkstra:

Centralisé, Complexité $O(n^2)$, O(n*e).

--

avec n = nombre de nœuds (routeurs) dans le réseau, d = degré moyen d'un nœud, et e = nombre de liens dans le réseau.

--

Diverses implémentations (Protocoles) existent pour ces deux approches.

Routage à Vecteur de Distance

Principe: Diffusion d'un vecteur où chaque entrée contient une distance vers une destination.

- Envoi des vecteurs de distances entre voisins directs (diffusion locale).

- Métrique : nombre de sauts (*hop count)*.

Routage à Vecteur de Distance

Algorithme

Décrit par [Bellman - 1957]

Amélioré par [Bellman & Ford]

Algorithme réparti [Ford Fulkerson 1962]

Protocoles

RIP-1 : RFC 1058 - 1988

RIP-2 : RFC 2453 - 1998

Algorithme de Bellman-Ford

Etat initial :

Chaque routeur/noeud connaît son environnement immédiat, son voisinage.

Algorithme de mise à jour (suite à la réception d'un vecteur de distance «DV»)

Pour chaque noeud A ayant reçu la mise a jour, calculer son nouveau DV.

Notation:

DV: Vecteur de Distance (contenant valeur de la distance d'un nœud vers toutes les destinations).

c(X,Y): coût du lien (X,Y).

$D_A(X)$= Distance minimale entre nœud A et nœud X.

V(A) = Voisinage du nœud A.

Algorithme de Bellman-Ford

Initialisation

- Distance du noeud A vers A est zéro: $D_A(A) = 0$.
- Distance de chaque noeud $U \in V(A)$ vers A est égale au coût du lien (A,U): $D_A(U) = c(A,U)$.
- Les distances vers les noeuds qui ne sont pas dans V(A) sont initialisées à ∞.

Etape d'Envoi

Envoyer les nouveaux DVs vers les voisins.

Etape de Réception

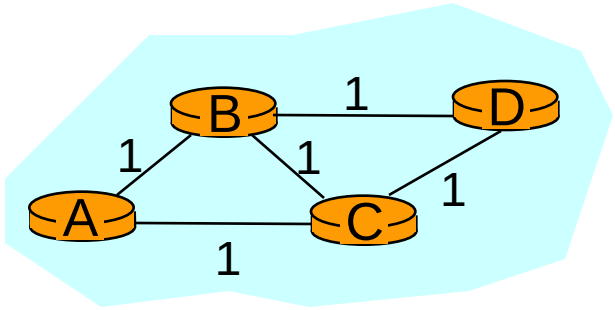
Pour chaque noeud A ayant reçu la mise à jour, calculer son nouveau DV en utilisant la formule:

$$D_A(X) = \min_{u \in V(A)} \{c(A,u) + D_u(X)\}, \forall X.$$

Si au moins un nouveau DV est obtenu aller vers Etape d'Envoi.
Sinon Terminer.

Algorithme de Bellman-Ford: Exemple

(1) Initialisation



Noeud A { Destinations } — { V(A) }

	A	B	C	D
DV	0	1	1	∞
B	∞	∞	∞	∞
C	∞	∞	∞	∞

Noeud B

	A	B	C	D
DV	1	0	1	1
A	∞	∞	∞	∞
C	∞	∞	∞	∞
D	∞	∞	∞	∞

Noeud C { Destinations } — { V(C) }

	A	B	C	D
DV	1	1	0	1
A	∞	∞	∞	∞
B	∞	∞	∞	∞
D	∞	∞	∞	∞

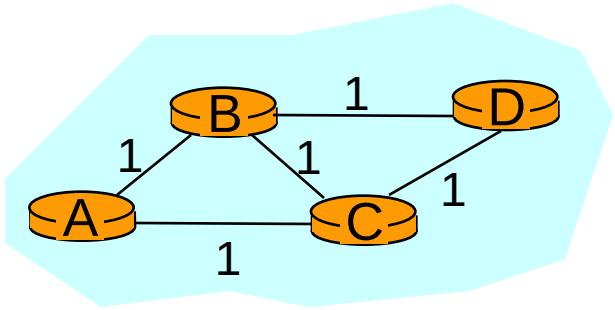
Noeud D

	A	B	C	D
DV	∞	1	1	0
B	∞	∞	∞	∞
C	∞	∞	∞	∞

```
1 Initialization:
2    for all neighbors V  do
3      if V adjacent to A
4        D_A(V) = c(A,V);
5      else
6        D_A(V) = ∞;
```

Algorithme de Bellman-Ford: Exemple

(2) Diffusion du DV



Noeud A

	A	B	C	D
DV	0	1	1	∞
B	1	0	1	1
C	∞	∞	∞	∞

Noeud B

	A	B	C	D
DV	1	0	1	1
A	0	1	1	∞
C	∞	∞	∞	∞
D	∞	∞	∞	∞

Noeud C

	A	B	C	D
DV	1	1	0	1
A	0	1	1	∞
B	1	0	1	1
D	∞	∞	∞	∞

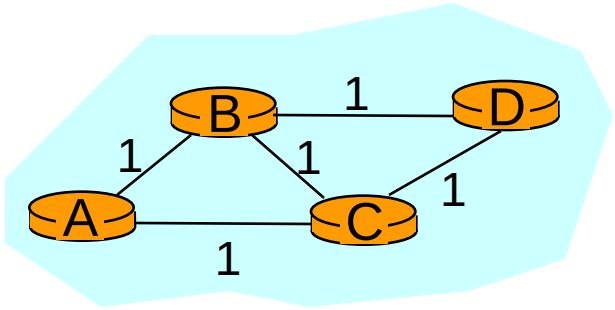
Noeud D

	A	B	C	D
DV	∞	1	1	0
B	1	0	1	1
C	∞	∞	∞	∞

Envoi du DV

A diffuse son DV à ses voisins B et C.
B diffuse son DV à ses voisins A, C et D.
C diffuse son DV à ses voisins A,B et D.
D diffuse son DV à ses voisins B et C

Algorithme de Bellman-Ford: Exemple



Noeud A

	A	B	C	D
DV	0	1	1	∞
B	1	0	1	1
C	1	1	0	1

Noeud B

	A	B	C	D
DV	1	0	1	1
A	0	1	1	∞
C	1	1	0	1
D	∞	1	1	0

Noeud C

	A	B	C	D
DV	1	1	0	1
A	0	1	1	∞
B	1	0	1	1
D	∞	1	1	0

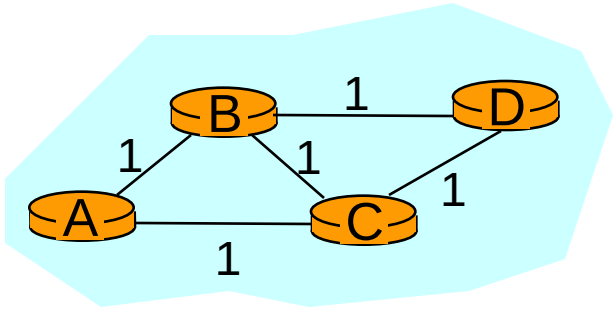
Noeud D

	A	B	C	D
DV	∞	1	1	0
B	1	0	1	1
C	1	1	0	1

Algorithme de Bellman-Ford: Exemple

(3) Calcul du nouveau DV

$D_A(D) = \min\{c(A,B)+ D_B(D); c(A,C)+ D_C(D)\}$
$= \min\{1+1 ; 1+1\} = 2$ via B



Noeud A

	A	B	C	D
DV	0	1	1	2/B
B	1	0	1	1
C	1	1	0	1

Noeud B

	A	B	C	D
DV	1	0	1	1
A	0	1	1	∞
C	1	1	0	1
D	∞	1	1	0

Calcul du nouveau DV
Chaque noeud calcule son nouveau DV

Notes:
- La valeur d'une case du DV d'un noeud est le coût du plus court chemin de ce noeud vers la destination correspondant à cette case.

- On peut indiquer dans cette case aussi le prochain saut pour atteindre la destination.

Noeud C

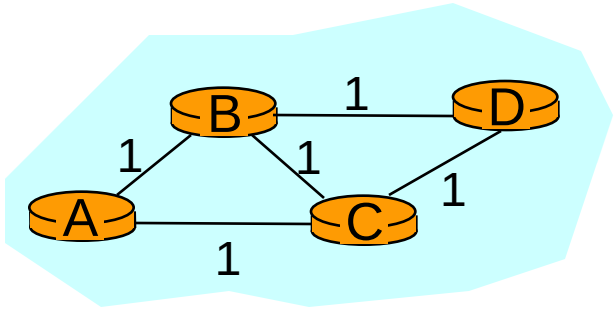
	A	B	C	D
DV	1	1	0	1
A	0	1	1	∞
B	1	0	1	1
D	∞	1	1	0

Noeud D

	A	B	C	D
DV	2	1	1	0
B	1	0	1	1
C	1	1	0	1

Algorithme de Bellman-Ford: Exemple

(4) Rediffusion du DV



Envoi du nouveau DV

Chaque noeud diffuse son nouveau DV obtenu après calcul à ses voisins.

Noeud A

	A	B	C	D
DV	0	1	1	2
B	1	0	1	1
C	1	1	0	1

Noeud B

	A	B	C	D
DV	1	0	1	1
A	0	1	1	2
C	1	1	0	1
D	2	1	1	0

Noeud C

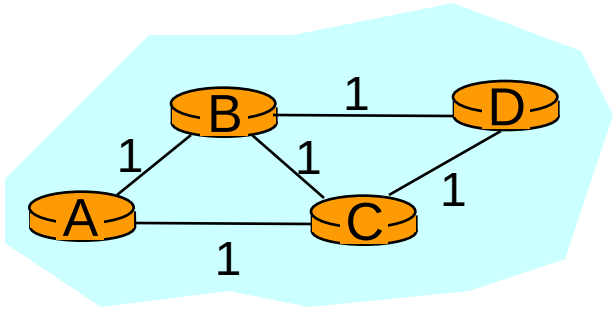
	A	B	C	D
DV	1	1	0	1
A	0	1	1	2
B	1	0	1	1
D	2	1	1	0

Noeud D

	A	B	C	D
DV	2	1	1	0
B	1	0	1	1
C	1	1	0	1

Algorithme de Bellman-Ford: Exemple

(5) Recalcul



Noeud A

	A	B	C	D
DV	**0**	**1/B**	**1/C**	**2/B**
B	1	0	1	1
C	1	1	0	1

Noeud B

	A	B	C	D
DV	**1/A**	**0**	**1/C**	**1/D**
A	0	1	1	2
C	1	1	0	1
D	2	1	1	0

Recalcul du DV

Rien ne change => Arrêt
L'algorithme Termine

Noeud C

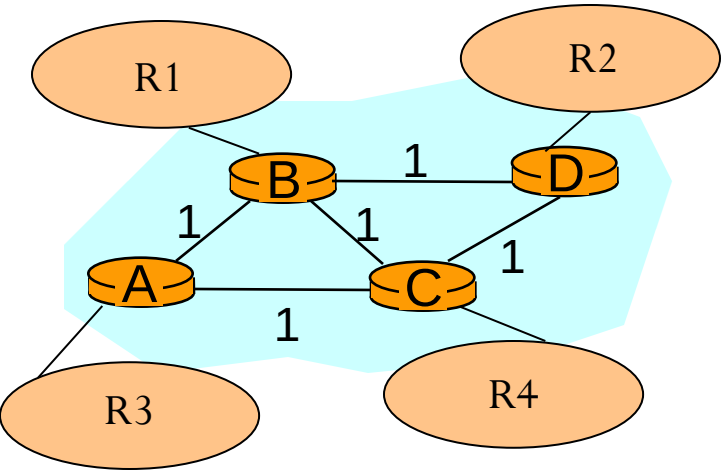
	A	B	C	D
DV	**1/A**	**1/B**	**0**	**1/D**
A	0	1	1	2
B	1	0	1	1
D	2	1	1	0

Noeud D

	A	B	C	D
DV	**2/C**	**1/B**	**1/C**	**0**
B	1	0	1	1
C	1	1	0	1

Algorithme de Bellman-Ford: Exemple

Soient les réseaux R1, R2, R3 et R4 directement connectés aux routeurs A , B, C, et D respectivement.



Tables de Routage obtenues

Routeur A

Destination	Saut suivant	Coût
R1	B	1
R2	B	2
R3	-	0
R4	C	1

Routeur B

Destination	Saut suivant	Coût
R1	-	0
R2	D	1
R3	A	1
R4	C	1

Routeur C

Destination	Saut suivant	Coût
R1	B	1
R2	D	1
R3	A	1
R4	-	0

Routeur D

Destination	Saut suivant	Coût
R1	B	1
R2	-	0
R3	C	2
R4	C	1

Routage à états de liens

Principe

- Routeur doit connaître la base de données topologique.

- Utilisation d'une métrique « coût » associée à chaque lien (pas nécessairement nombre de sauts).

- Le réseau peut être modélisé par un graphe pondéré.

- Meilleures routes: celles minimisant la somme des coûts des liens.

- Routes calculées selon l'algorithme de **Dijkstra.**

- Avantages: Chaque routeur calcule indépendamment les meilleures routes, ainsi l'algorithme converge plus rapidement que le routage à vecteur de distance.

- Inconvénients: Nécessite un espace mémoire plus important pour le stockage, les calculs sont assez complexes.

Algorithme de Dijkstra

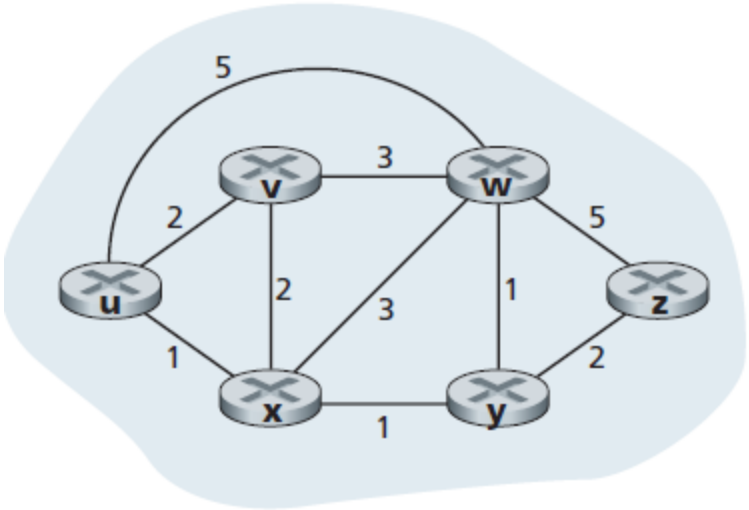
Au niveau du Routeur « u »

```
1   Initialization:
2     N' = {u}
3     for all nodes v
4       if v is a neighbor of u
5         then D(v) = c(u,v)
6       else D(v) = ∞
7
8   Loop
9     find w not in N' such that D(w) is a minimum
10    add w to N'
11    update D(v) for each neighbor v of w and not in N':
12          D(v) = min( D(v), D(w) + c(w,v) )
13    /* new cost to v is either old cost to v or known
14     least path cost to w plus cost from w to v */
15  until N'= N
```

D(v) = Distance Minimale entre routeur « u » et routeur « v ».

c(x,y)= coût du lien entre nœud « x » et nœud «y ».

Algorithme de Dijkstra: Exemple



Au niveau du Routeur « u »

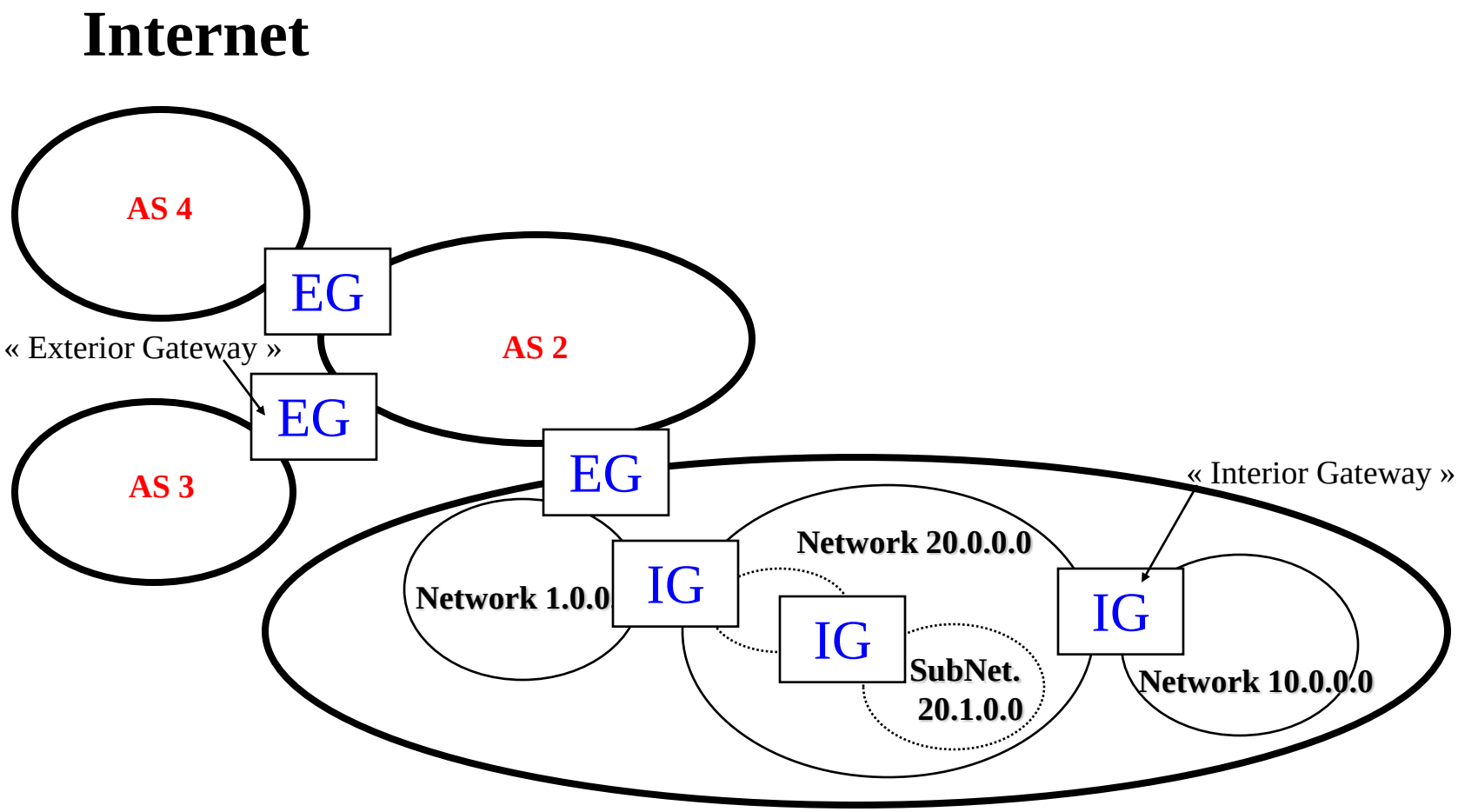
step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					

p(v)=voisin antérieur de v, c'est-à-dire qui précède le nœud v dans le plus court chemin entre le routeur u et le nœud v.

Chapitre II: La Couche Réseau

- Le Concept d'Interconnexion
- Architecture Internet
- Adressage (IP, OSI)
- IP et protocoles associés (ICMP, ARP, RARP)
- Fragmentation et Réassemblage
- Routage: Généralités
- Algorithmes de Routage (DVR, LSR)
- Protocoles de RTG Internet I (RTG intra-domaine: RIP, OSPF)
- Protocoles de RTG Internet II (RTG inter-domaine: BGP)

Domaines Internet



Domaines Internet

Système autonome (AS)

- Domaine (entreprise, AS) géré par une autorité administrative unique.
- Libre de choisir sa propre politique de routage interne.
- Peut se connecter à un ou plusieurs autres systèmes autonomes.

Routage intra-domaine (à l'intérieur d'un système autonome)

- Réalisé par les Interior Gateways IG
- Protocoles IGP « Interior Gateway Protocol » différent d'un AS à un autre, Exemples de IGPs: RIP Routing Information Protocol et OSPF Open Shortest Path First.

Routage inter-domaines (entre systèmes autonomes)

- Réalisé par les Exterior Gateways EG
- Exemples de protocoles EGP « Exterior Gateway Protocol »: BGP Border Gateway Protocol s'occupe du routage entre routeurs d'extrémités.

Protocoles de Routage

L'ensemble des protocoles qui s'occupent du routage à l'intérieur d'un système autonome sont appelés des IGPs.

Exemples d'IGPs:

Routing Information Protocol RIP

Open Shortest Path First OSPF

Le protocole RIP Routing Information Protocol

- Un protocole de routage à Vecteur de Distance, basé sur l'algorithme Bellman-Ford.

- Basé sur la diffusion de messages de routage.

- Utilise comme métrique « nombre de sauts ».

- 1 saut = 1 routeur.

- 16 sauts = Infini, c'est-à-dire au delà de 15 sauts une destination est considérée inaccessible.

Routing Information Protocol :

- RIP-1 : RFC 1058
- RIP-2 : RFC 2453

Le protocole RIP

Principes

- Chaque routeur maintient localement une liste (BdD) des meilleures routes

→table de routage <@ de destination, @ du prochain routeur, distance >

- Chaque routeur actif diffuse un message de routage:
  - Périodiquement (30 secondes)
  - A tous ses voisins immédiats
  - Contient une liste de <@ de destination, distance>

- Les routeurs ayant reçu les messages de routage mettent à jour leur tables de routage en conséquence. L'adresse du prochain routeur est implicitement celle de l'émetteur du message de routage.

Le protocole RIP

Etat initial:

Chaque routeur connaît son environnement immédiat :

- son adresse, ses interfaces,
- ses (sous)réseaux directs: distance = 0.

Algorithme de mise à jour (suite à la réception d'un message de routage)

Chaque entrée du message est comparée aux entrées de la table de routage:

[1] l'entrée n'existe pas dans la table et la distance reçue n'est pas infinie:

- Une nouvelle entrée est créée : prochain routeur = routeur d'où provient la liste; distance = distance reçue + 1.

[2] l'entrée existe et sa distance est supérieure à celle reçue +1 :

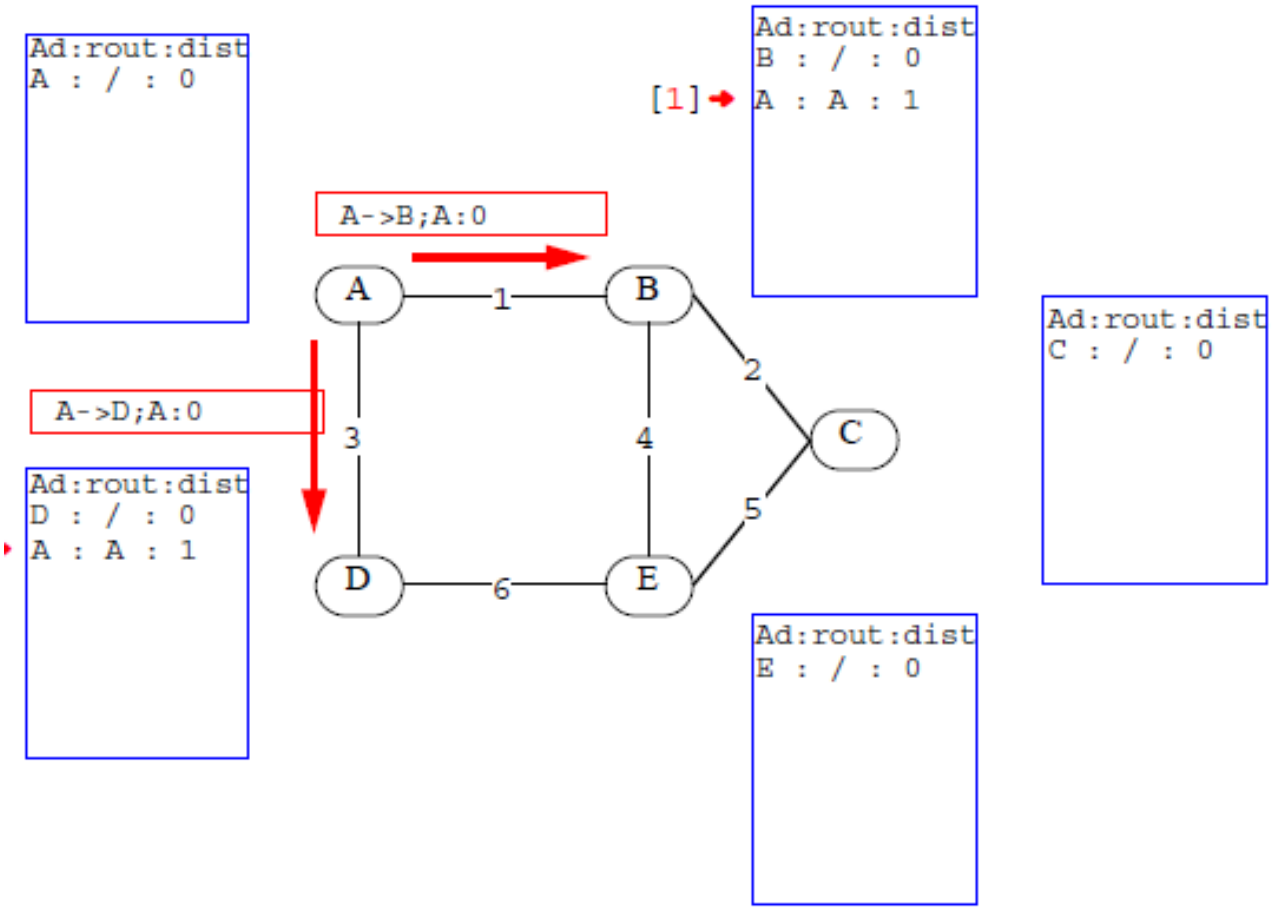
- On met à jour l'entrée : prochain routeur = routeur d'où provient la liste;

distance = distance reçue + 1

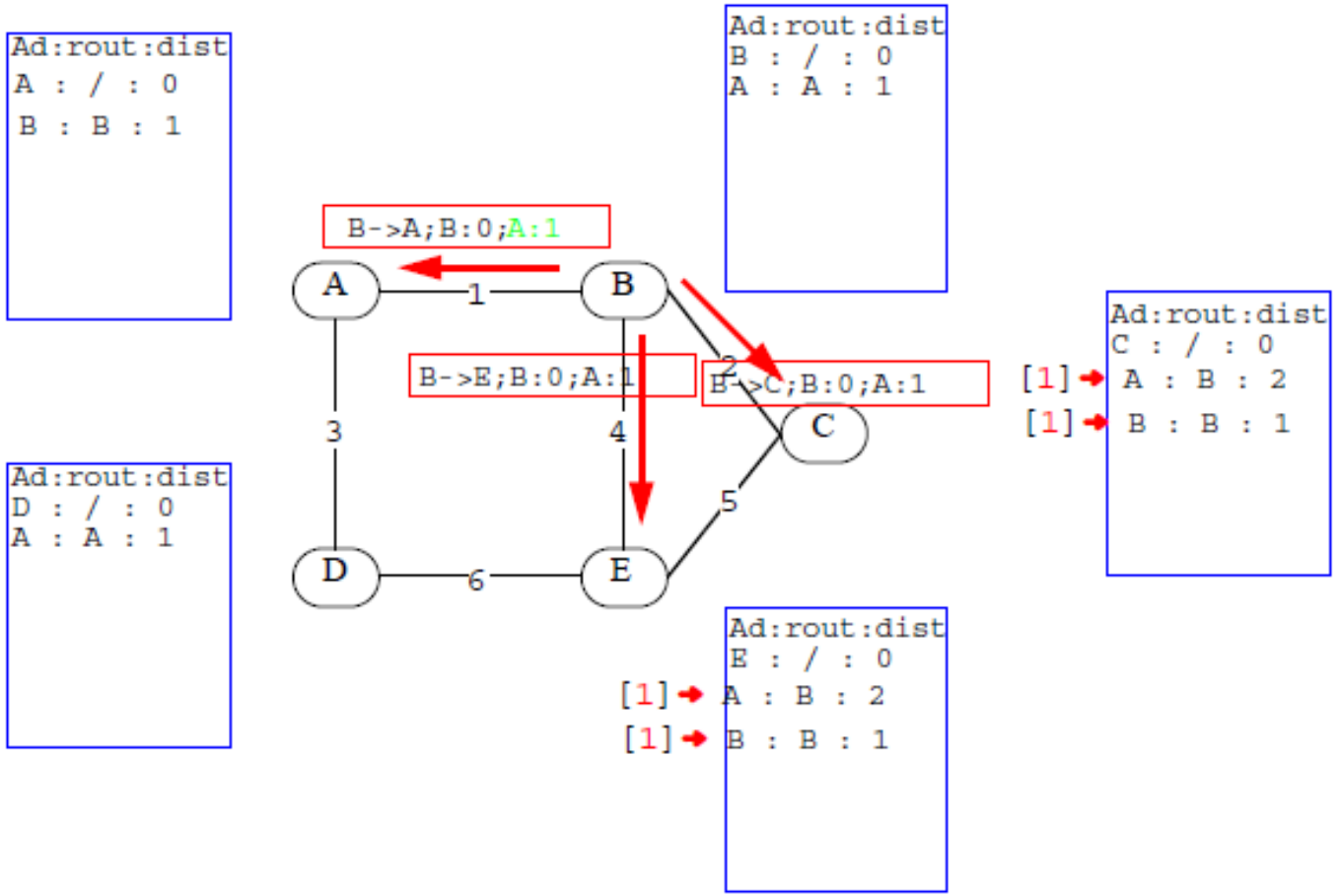
[3] l'entrée existe et son prochain routeur est celui d'où provient la liste:

distance = distance reçue + 1.

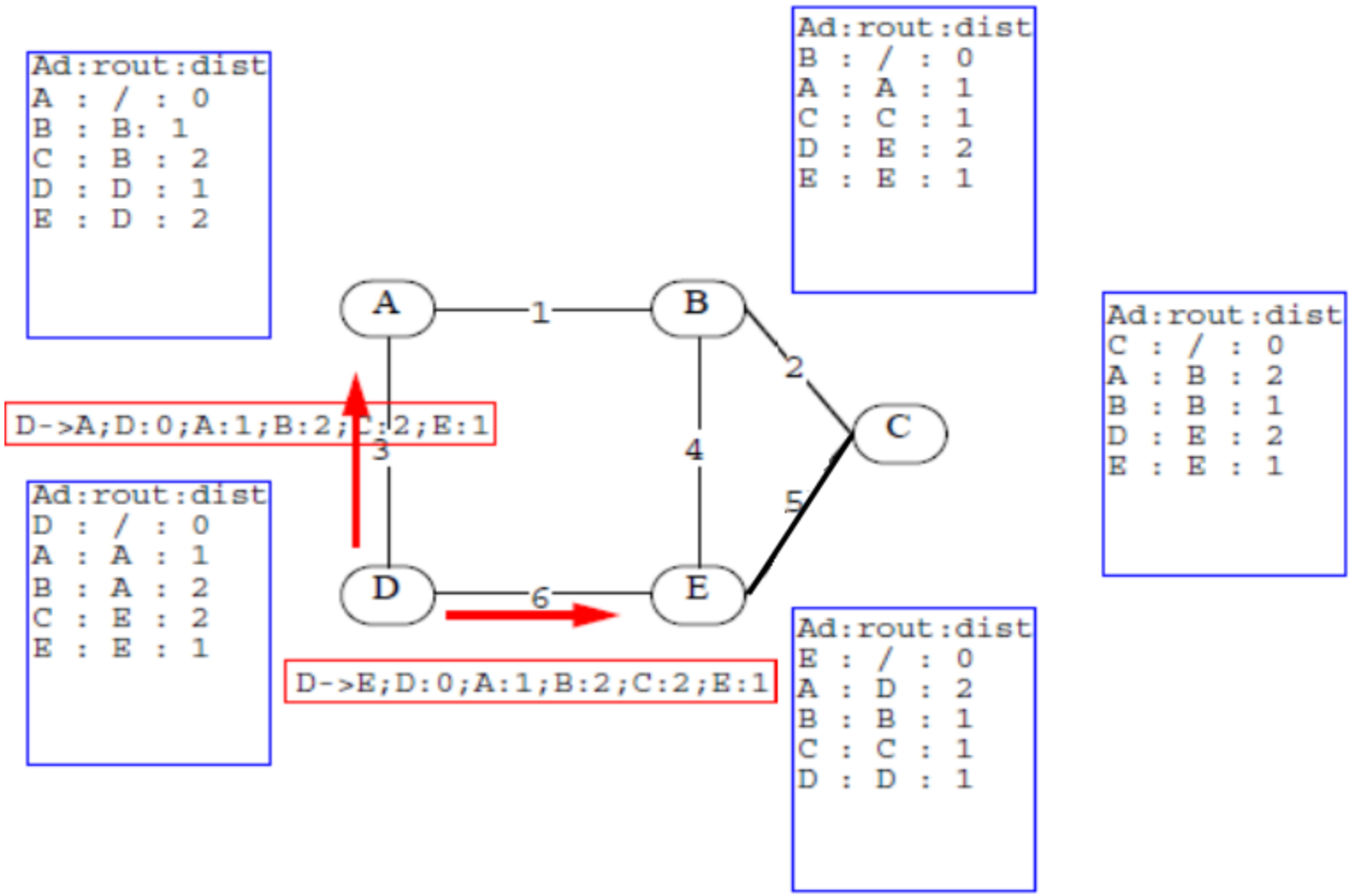
Le protocole RIP - Exemple



Le protocole RIP - Exemple



Le protocole RIP - Exemple



Le protocole RIP - Problèmes

Quelques Problèmes

Convergence Lente (Slow Convergence)

Les changements de topologie ne sont pas immédiatement pris en compte.

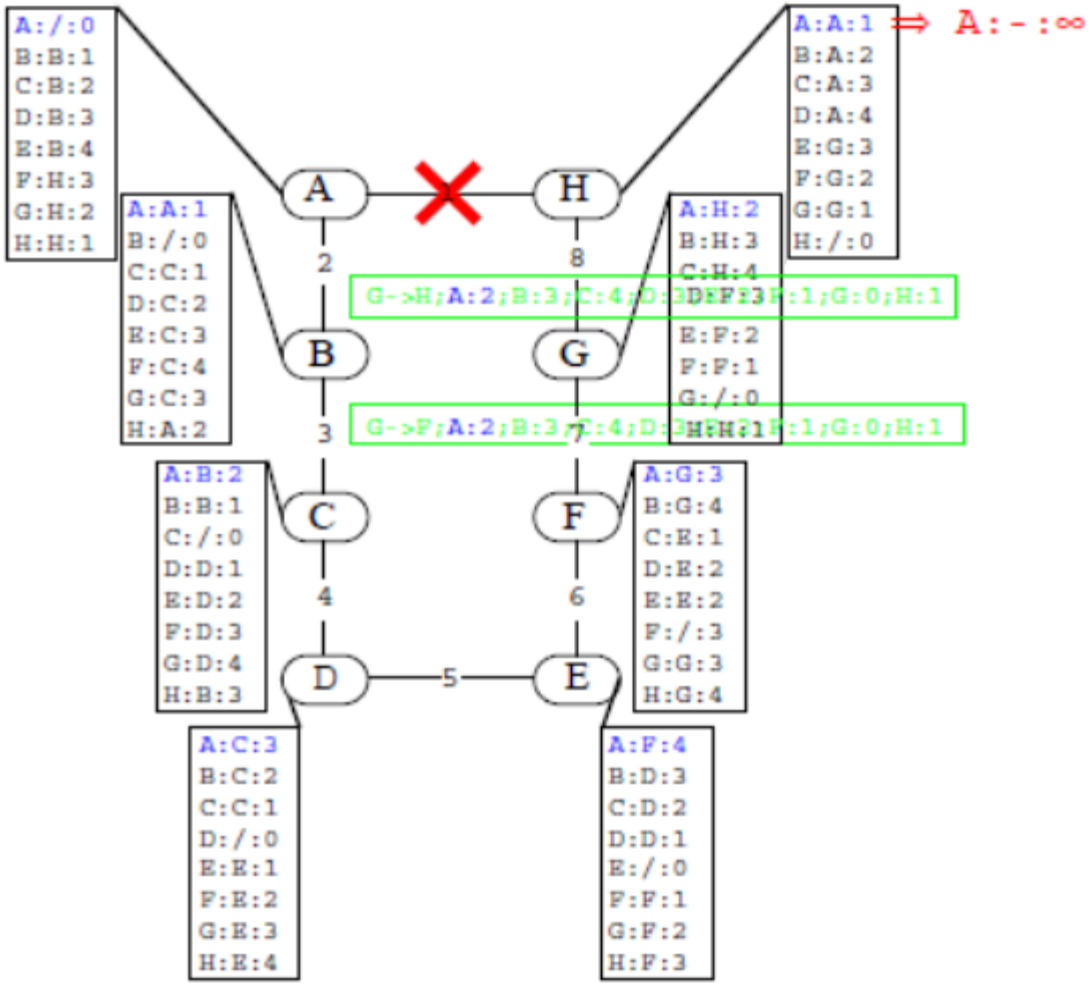
Le Rebond

Des boucles sont créées, des paquets y circulent indéfiniment.

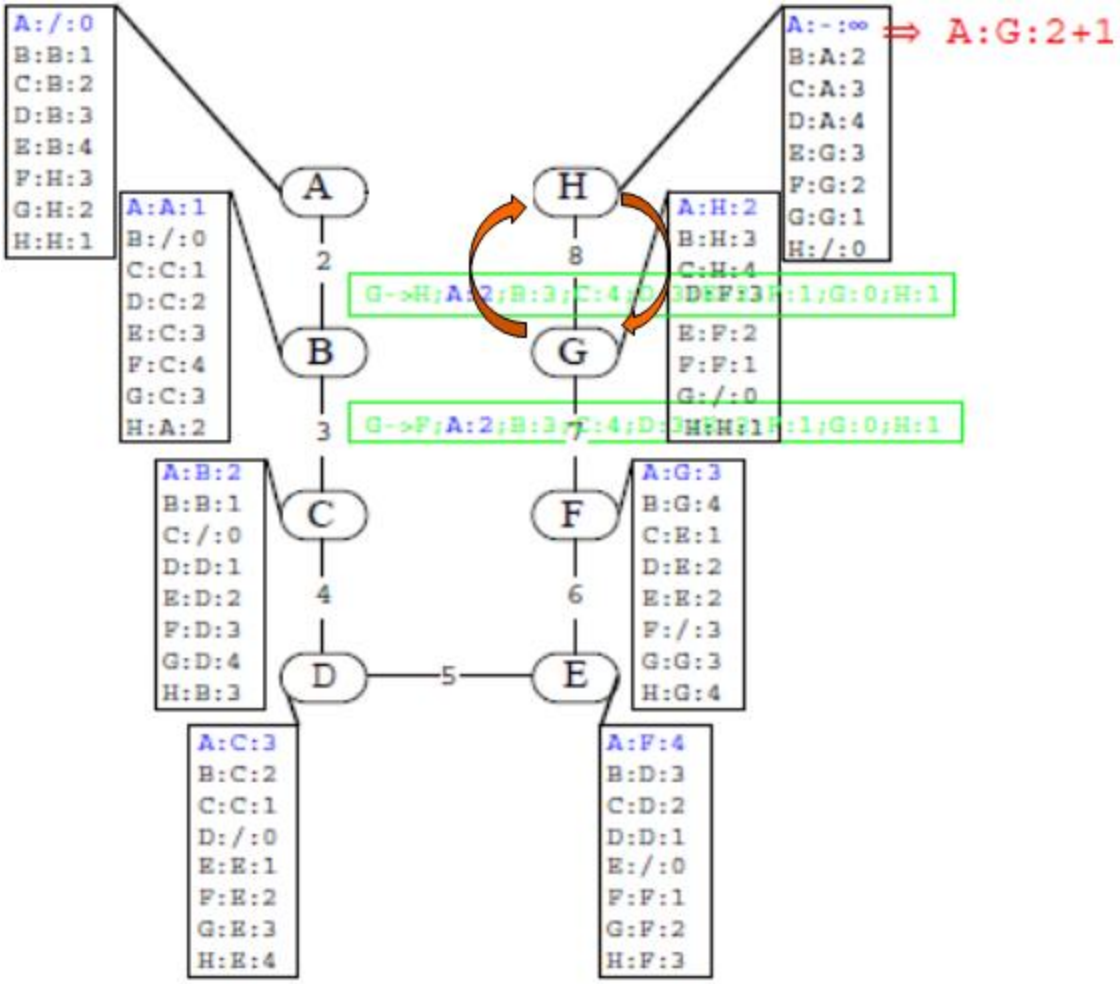
Incrémentation Infinie

Distance des stations inaccessibles incrémentée indéfiniment.

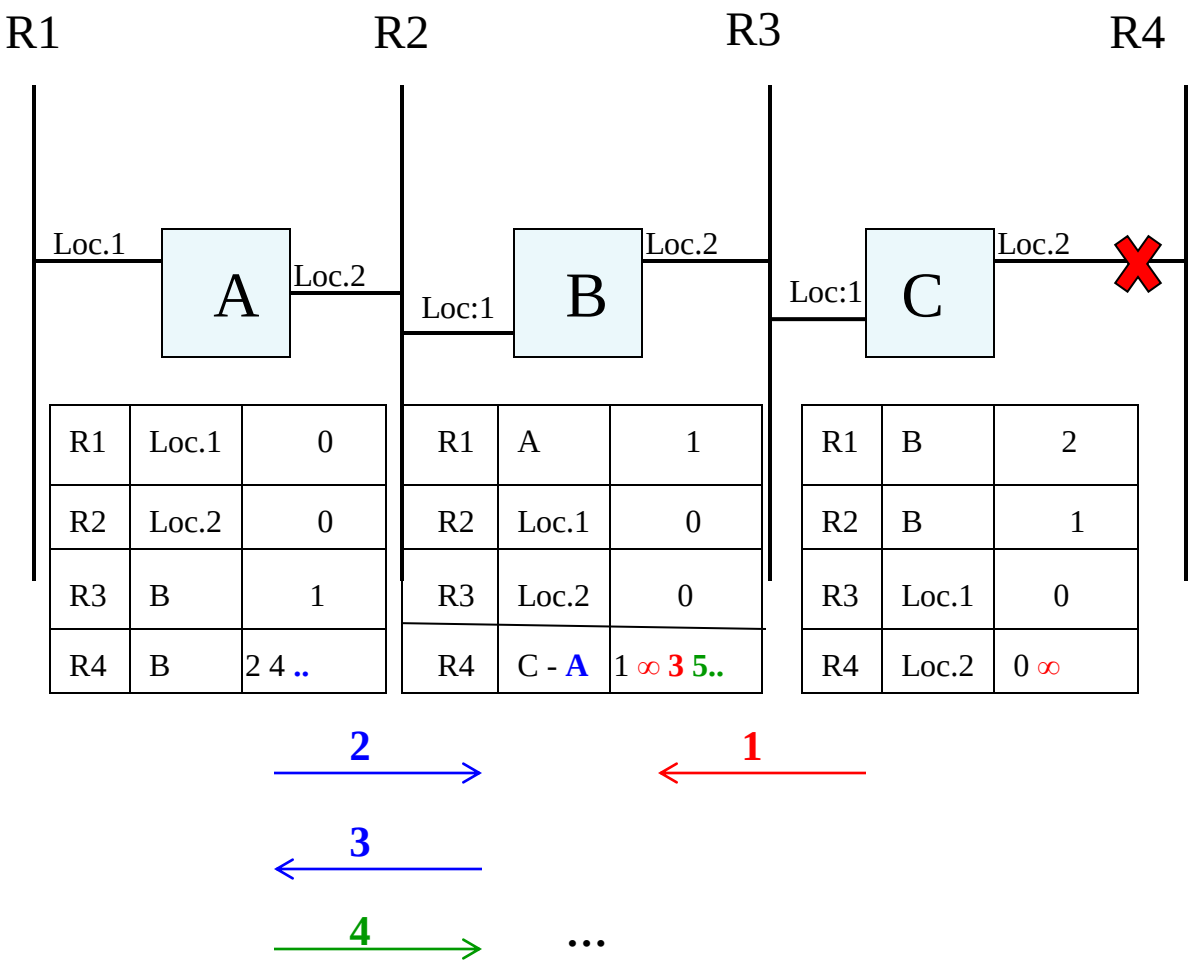
Problème de Rebond



Problème de Rebond



Problème d'Incrémentation Infinie



R1	Loc.1	0
R2	Loc.2	0
R3	B	1
R4	B	2 4 ..

R1	A	1
R2	Loc.1	0
R3	Loc.2	0
R4	C - A	1 ∞ 3 5..

R1	B	2
R2	B	1
R3	Loc.1	0
R4	Loc.2	0 ∞

Le protocole RIP - Solutions

Quelques solutions aux problèmes précédents

Limited Infinity

Distance = 16 destination inaccessible. Cela a pour conséquence de limiter l'étendue du domaine géré par RIP.

Triggered update

- Un message de routage est diffusé dès que la table de routage a été modifiée.
- Prise en compte immédiate des modifications.

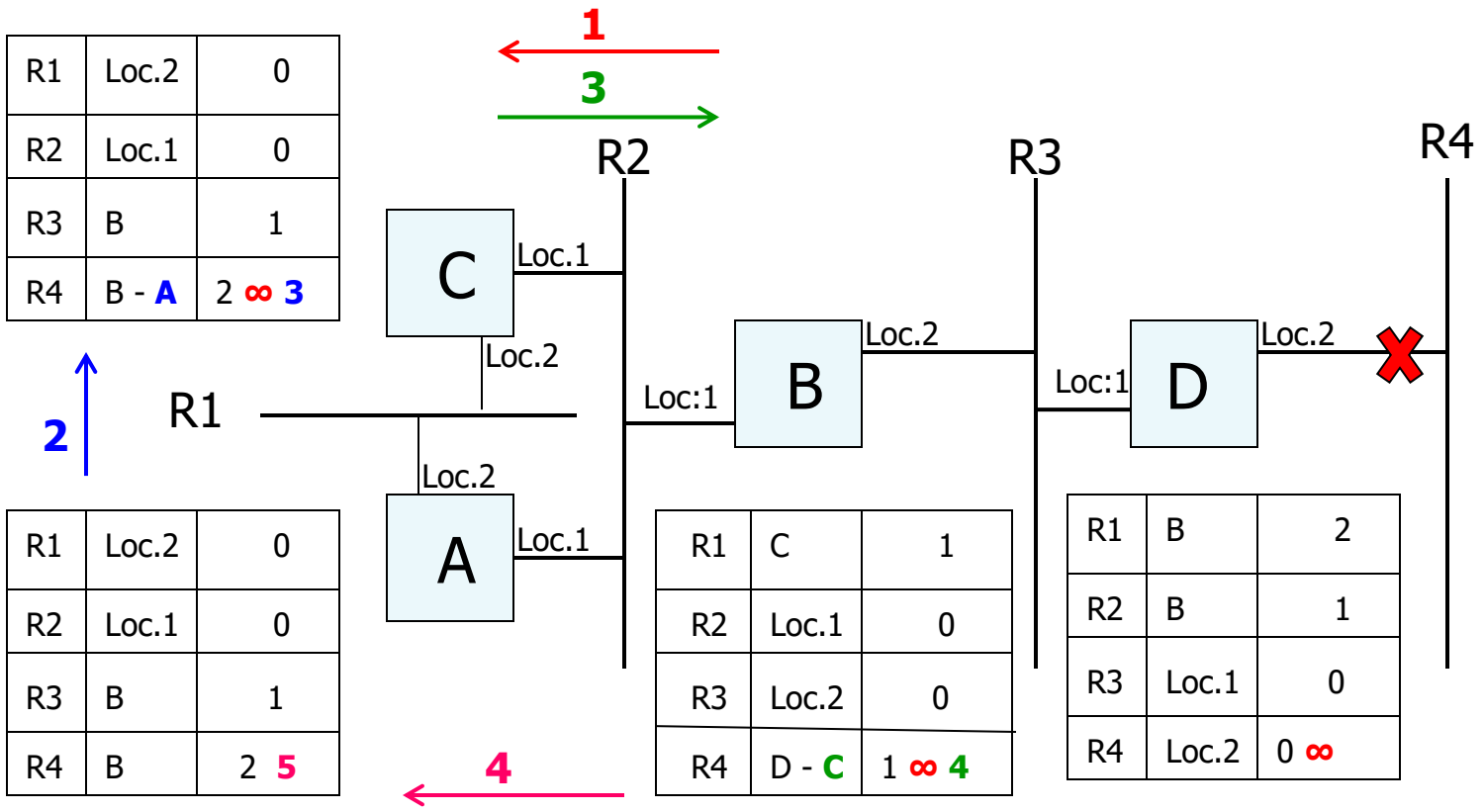
Horizon Coupé (Split Horizon)

- But: Eviter le problème de rebond en forçant un sens pour la propagation de l'information de routage.

- Dans le cas de l'exemple précédent, Interdire à A d'émettre vers B l'information qu'il peut atteindre R3 ou R4 car les routes passent par B saut prochain.

- Cela ne résout pas complètement le problème du rebond. Cette solution n'est pas efficace pour les topologies réseaux non linéaires.

Problème avec l'Horizon Coupé



A et C n'envoient pas des informations vers B à propos de R4 (Split Horizon).
A envoie à C que R4 est accessible avec coût 2.
C modifie sa table de routage et l'envoie à B.
Problème: Boucle créée entre A, B et C.

Le protocole RIP - Solutions

Route time-out

Détection des destinations inaccessibles. Toute destination dont on n'a plus de nouvelles pendant 3 minutes est considérée inaccessible.

Hold down (Compteur de Retenue)

- Les destinations qui ne sont plus accessibles, distance = 16, sont enregistrées dans la table de routage. Cette valeur est conservée pendant 4 périodes de mise à jour, 2 minutes, le temps que l'information se propage dans le réseau.

-Après cette période, des messages de routage relatives à ces destinations peuvent être considérées.

Poison reverse

Diffuser les destinations qui deviennent inaccessibles aux voisins. Pour une destination donnée, un coût 16 est annoncé au routeur voisin à travers lequel le routage est fait pour atteindre cette destination.

Le Routing Information Protocol

- Utilisé avec UDP comme protocole de transport.

- Diffusion des messages de routage toutes les 30s.

- Délai aléatoire de diffusion immédiate compris entre zéro et 5 secondes.

- Durée de validité d'une entrée 3 minutes: Si aucun message de routage n'est reçu d'un routeur au bout de 180s, il est considéré comme inaccessible.

- Utilise les techniques « Hold down », « Split Horizon » et « Poison Reverse » pour résoudre le problème de rebond.

- Utilise « Triggered Update » pour accélérer la convergence.

Le protocole RIP

Le champ "command" (8 bits): code le type du message

1 = demande d'information

demande d'informations de routage.

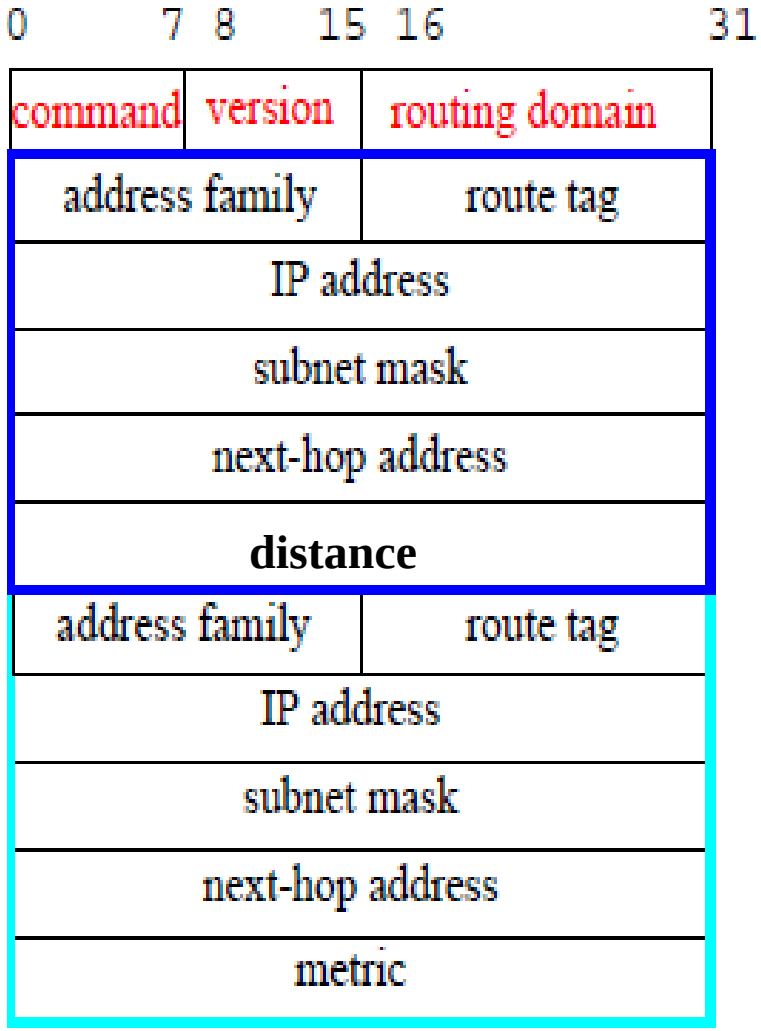
2 = réponse

suite à une demande, envoi périodique d'un message de routage sous forme de (destination, distance).

Le champ "version" (8 bits)

Indique le numéro de version du protocole RIP.

Le champ "routing domain" (16 bits)



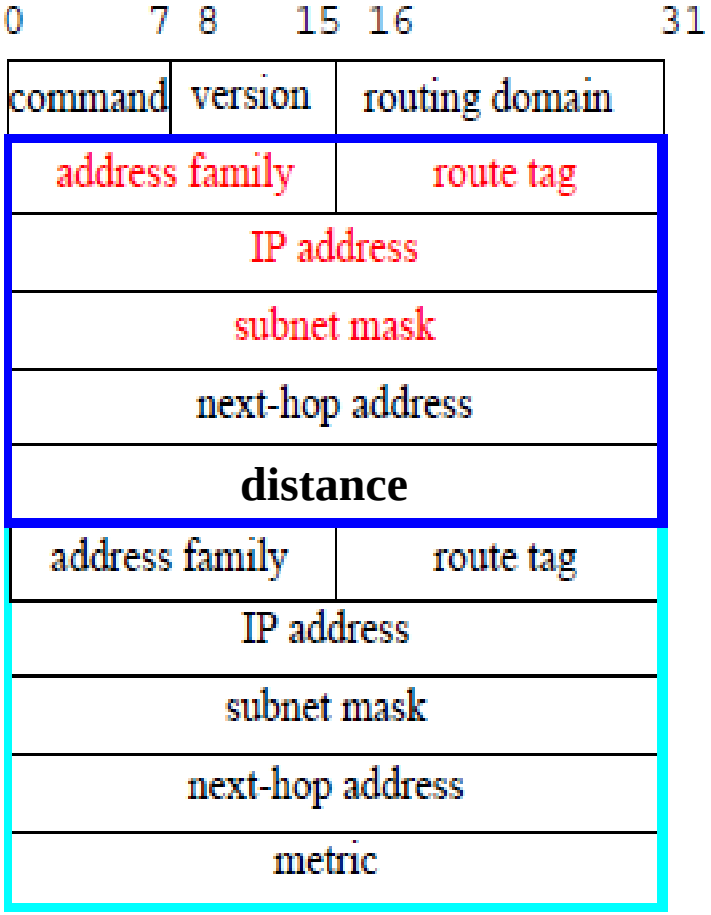
Le protocole RIP

"address family" (16 bits): code le format d'adressage
Valeur 2 correspond au protocole IP.

Le champ "route tag" (16 bits)

Le champ "IP address" (32 bits): l'adresse de destination
Adresse IP d'un réseau

Le champ "subnet mask" (32 bits)
- L'adresse masque du réseau IP



Le protocole RIP

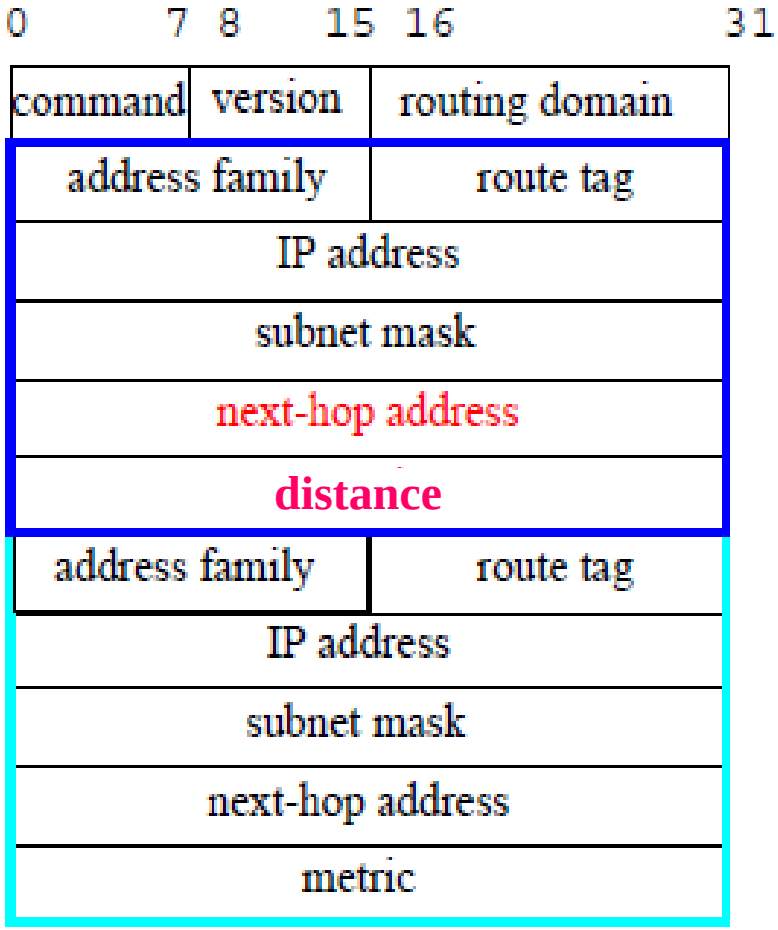
Le champ "next-hop address" (32 bits):

Contient l'adresse du routeur suivant qui est associé à l'adresse destination.

Le champ « distance» (32 bits):

Distance en nombre de sauts entre la destination indiquée par "IP address".

16 = distance infinie, c'est-à-dire destination inaccessible.



Le Protocole OSPF

- OSPF (RFC 2328) Routage à état de liens

- Utilise une topologie hiérarchique

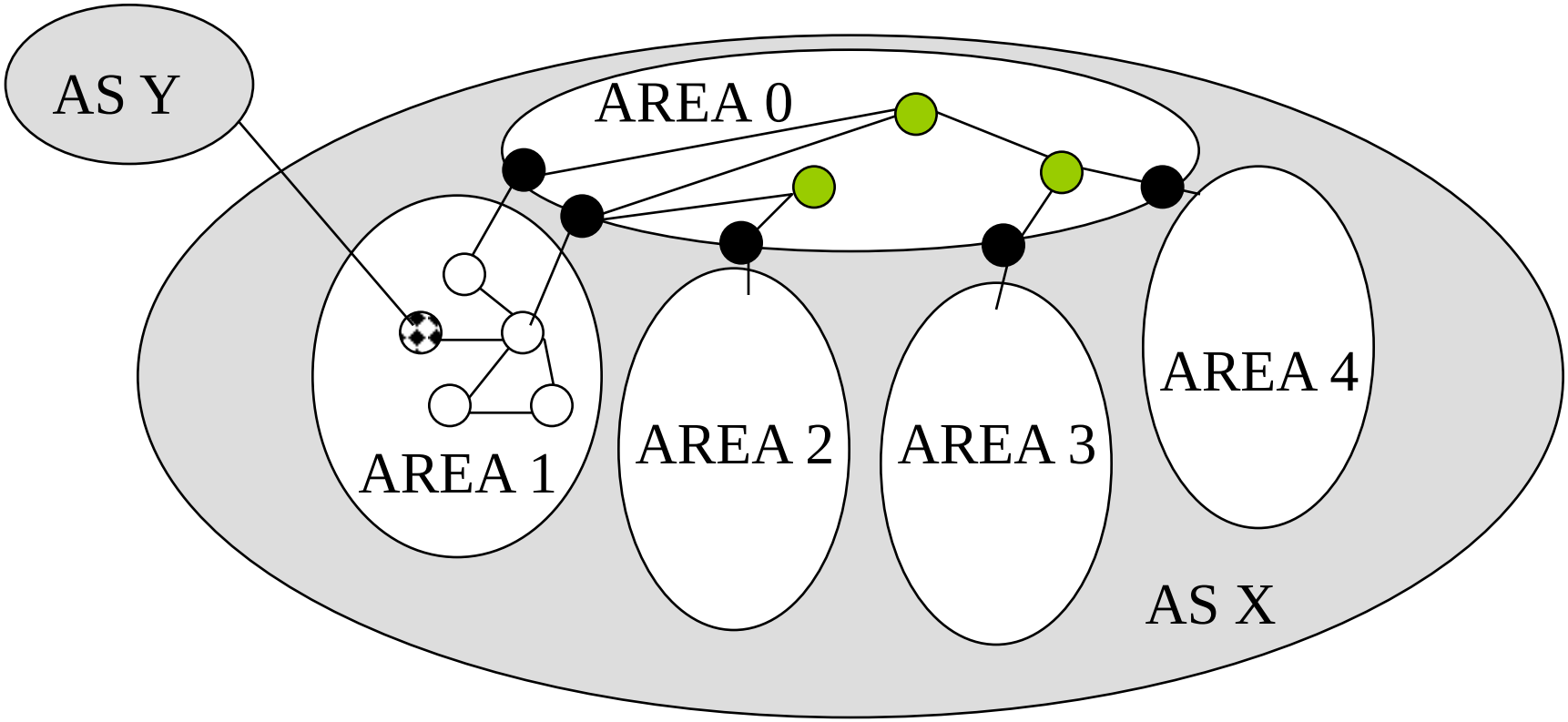
- Un système autonome AS est découpé en zones ou aires «Areas».

- Une zone (Area) = ensemble de réseaux contigus.

- La zone 0 est la dorsale d'un système autonome.

- On distingue entre routage intra zone et inter zone.

Le Protocole OSPF: Hiérarchie



○ Routeur interne «**Internal Router**» **IR**

● Routeur interne dans la zone zéro «**Backbone Router**» **BR**

● Routeur à la frontière de deux ou plusieurs zones «**Area Border Router**» **ABR**

⚽ Routeur inter systèmes autonomes «**Autonomous System Boundary Router**» **ASBR**

Le Protocole OSPF

Routage intra-zone

La source et la destination dans la même zone.

Routage inter-zone

La source et la destination dans des zones différentes.

- Aller de la source vers la zone dorsale.
- Transiter à travers la dorsale jusqu'à la zone de destination.
- Transiter dans la zone destination jusqu'à la destination.

Bases de données enregistrées dans un routeur :

« **Adjacency Database** »

« **Topology Database** »

« **Forwarding Database** »

Le Protocole OSPF

Chaque routeur :

- découvre ses voisins par envoi périodique de message HELLO.

- mesure les coûts vers chacun de ses voisins.

- construit un message **LSA** (Link State Advertisment) traduisant l'état des liens, contenant adresse du routeur source, la liste des voisins et les coûts associés.

- diffuse ce message LSA à tous les autres routeurs de la zone.

- construit une base de données d'états de liens et calcule **l'arbre SPF** en appliquant l'algorithme de Dijkstra.

Le Protocole OSPF

A l'intérieur d'une zone

- Chaque routeur dispose d'une base de données topologique contenant des informations sur les états des liens.

- Au moins un routeur est connecté à la zone dorsale.

- Si un routeur est connecté à deux zones, il doit exécuter l'algorithme du plus court chemin pour les deux zones séparément**.**

Identification d'un routeur

- Un routeur est identifié, de façon unique par un identifiant appelé **RID** (Router IDentifier).

- Un routeur choisira comme ID la plus grande adresse IP de ses interfaces opérationnelles.

- Si une nouvelle interface est activée dans le routeur, le RID ne pourra changer qu'après redémarrage du routeur.

OSPF: Routeurs désignés

Élection des DR et BDR

- Pour diminuer le trafic réseaux entre tous les routeurs, un **routeur désigné DR** est élu dans chaque réseau.

- Chaque routeur possède une priorité.

- Le routeur qui envoie un message Hello avec la plus grande priorité OSPF est élu DR, sinon celui avec la plus grande adresse IP.

- Ainsi, tous les échanges de messages LSA dans ce réseau ne se font qu'avec ce routeur désigné. Dans un réseau à n routeurs et sans DR, n*(n-1)/2 messages LSA sont échangés → Avec un DR, uniquement (n-1)/2 messages.

- Un routeur de secours BDR **Backup Designated Router** est aussi choisi. Généralement, le routeur avec la 2ème plus grande priorité ou 2ème plus grande adresse devient BDR.

- Si le DR est en panne, le BDR devient DR et un nouveau BDR est élu.

- Si le BDR est en panne, un nouveau BDR est élu.

Le Protocole OSPF

Messages de Routage

Le DR envoie un message DBD (« Database Description ») qui représente un résumé de l'état des liens.

Le routeur à la réception acquitte les paquets DBD (« Link State Acknowledgment ») et envoie un message DBD.

Le DR acquitte les paquets DBD.

Après l'échange des messages DBD, si un routeur constate que certaines entrées sont moins récentes, il envoie une requête LSR « Link State Request » à laquelle répond le routeur adjacent (ayant l'info. La plus récente) par un message LSU « Link State Update ».

Un routeur envoie un LSU (« Link State Update ») quand l'état d'un lien change ou toutes les 30 minutes.

Le Protocole OSPF

Il existe 5 types de messages LSA (Link State Announcement)

- **Type 1** « **router link** »: états des liens des routeurs et réseaux adjacents au routeur de la zone, message envoyé par routeur interne.

- **Type 2** « **network link** »: liste des routeurs appartenant à un réseau de la zone.

- **Type 3** « **Summary link** »: destinations en dehors de la zone (mais dans le même AS), message envoyé par routeur **ABR.**

- **Type 4** « **AS border router link** »: routeurs ASBR, message envoyé par routeur **ABR.**

- **Type 5** « **AS external link** » : destinations en dehors du AS, message envoyé par routeur **ASBR.**

Exemple OSPF: Système autonome sans découpage en aires

Légende :

RT : routeur

N : sous réseau

H : machine hôte

I : interface

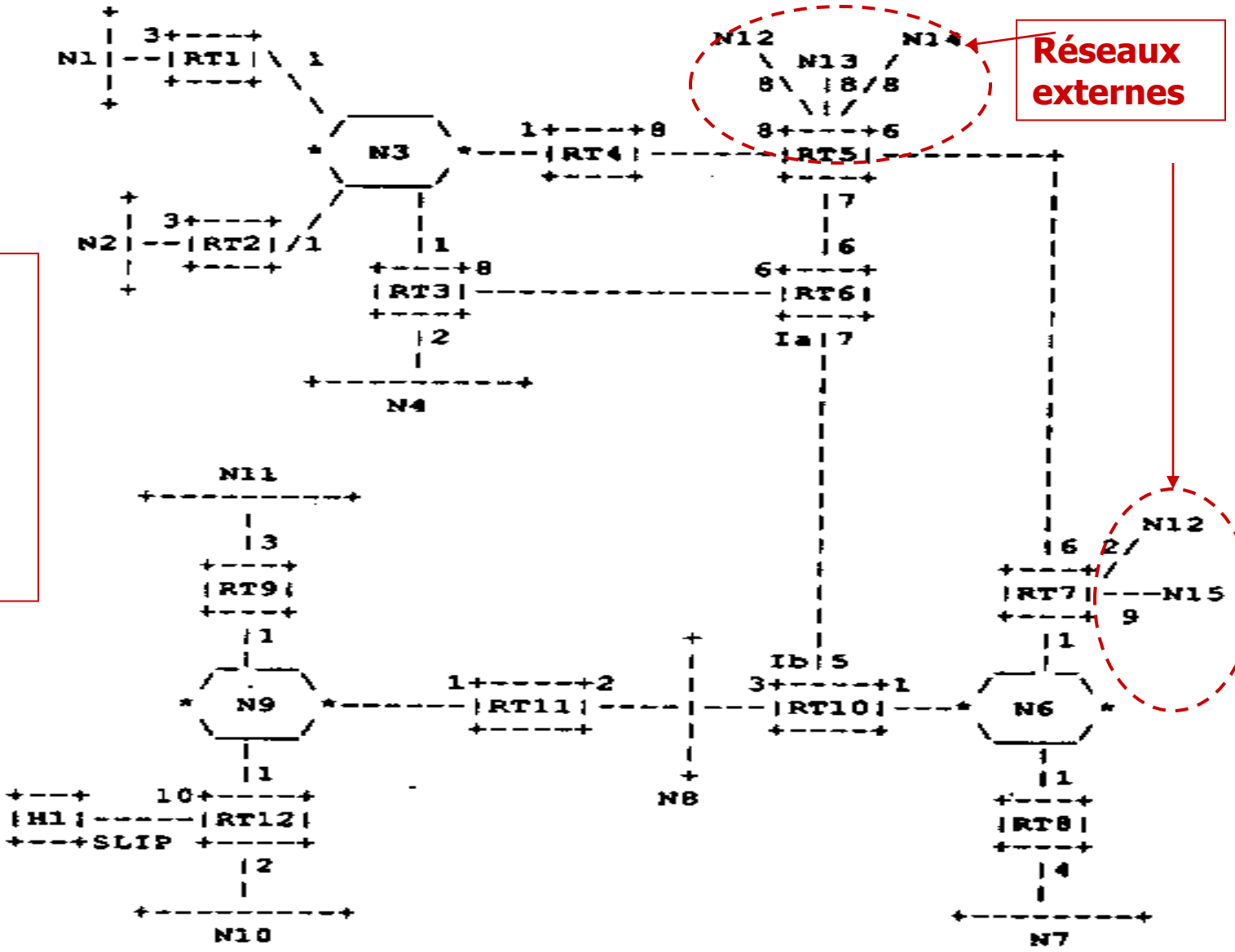


Figure 2: A sample Autonomous System

Exemple OSPF: Système autonome sans découpage en aires

La table suivante représente la **matrice d'adjacence** du graphe précédent avec coût de liens.

Etant donné cette matrice d'adjacence, chaque routeur calcule les plus courts chemins vers toutes les destinations possibles (routeurs et sous réseaux).

From

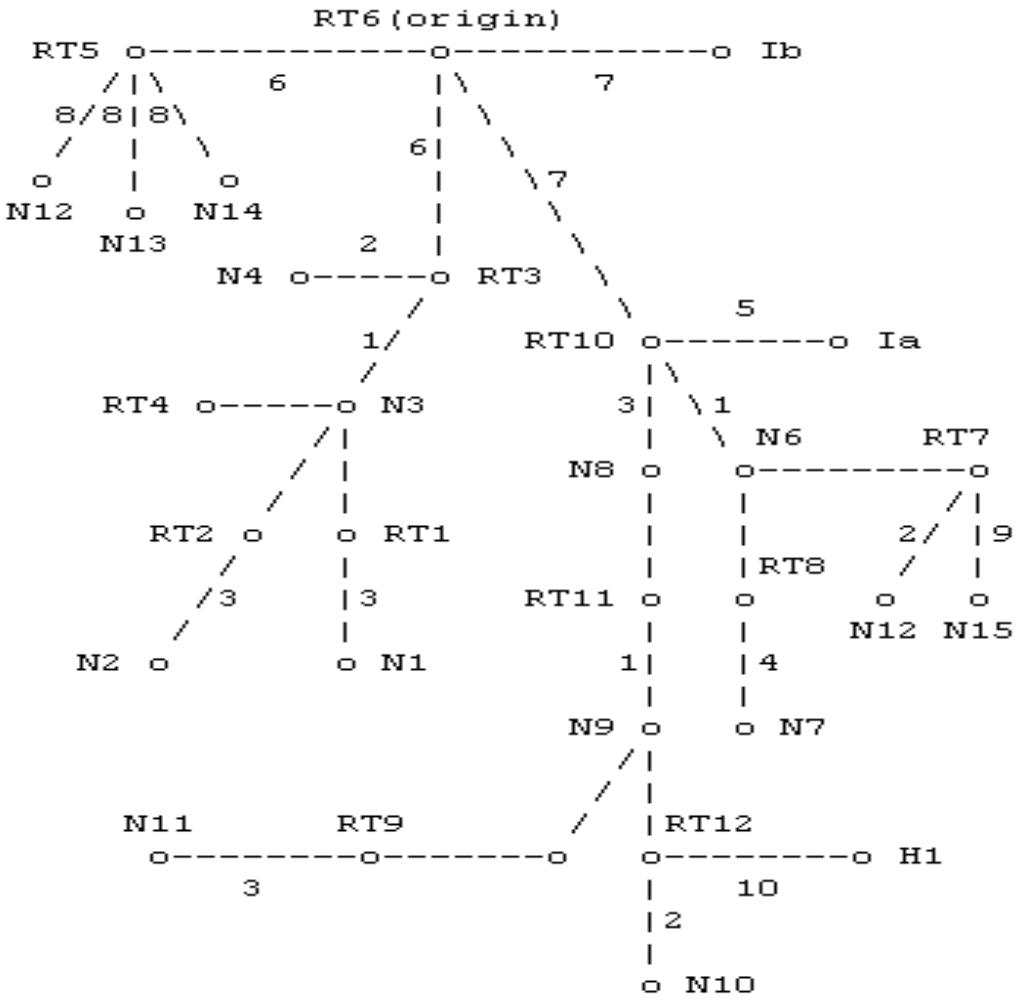
		RT1	RT2	RT3	RT4	RT5	RT6	RT7	RT8	RT9	RT10	RT11	RT12	N3	N6	N8	N9
	RT1													0			
	RT2													0			
	RT3					6								0			
	RT4				8									0			
	RT5			8		6	6										
	RT6		8		7						5						
	RT7				6										0		
*	RT8														0		
*	RT9																0
T	RT10					7									0	0	
O	RT11															0	0
*	RT12																0
*	N1	3															
	N2		3														
	N3	1	1	1	1												
	N4		2														
	N6						1	1		1							
	N7							4									
	N8									3	2						
	N9								1		1	1					
	N10											2					
	N11								3								
	N12				8		2										
	N13				8												
	N14				8												
	N15						9										
	H1												10				

The resulting directed graph

Exemple OSPF: Système autonome sans découpage en aires

L'ensemble des meilleurs chemins entre un routeur et toutes les destinations peut être modélisé sous forme d'un arbre de plus courts chemins.

L'exemple suivant correspond à l'arbre calculé par le routeur R6.



The SPF tree for Router RT6

Exemple OSPF: Système autonome sans découpage en aires

Table de Routage du routeur R6

Destination	Next Hop	Distance
N1	RT3	10
N2	RT3	10
N3	RT3	7
N4	RT3	8
Ib	*	7
Ia	RT10	12
N6	RT10	8
N7	RT10	12
N8	RT10	10
N9	RT10	11
N10	RT10	13
N11	RT10	14
H1	RT10	21
RT5	RT5	6
RT7	RT10	8

Exemple OSPF: Système autonome avec 3 aires

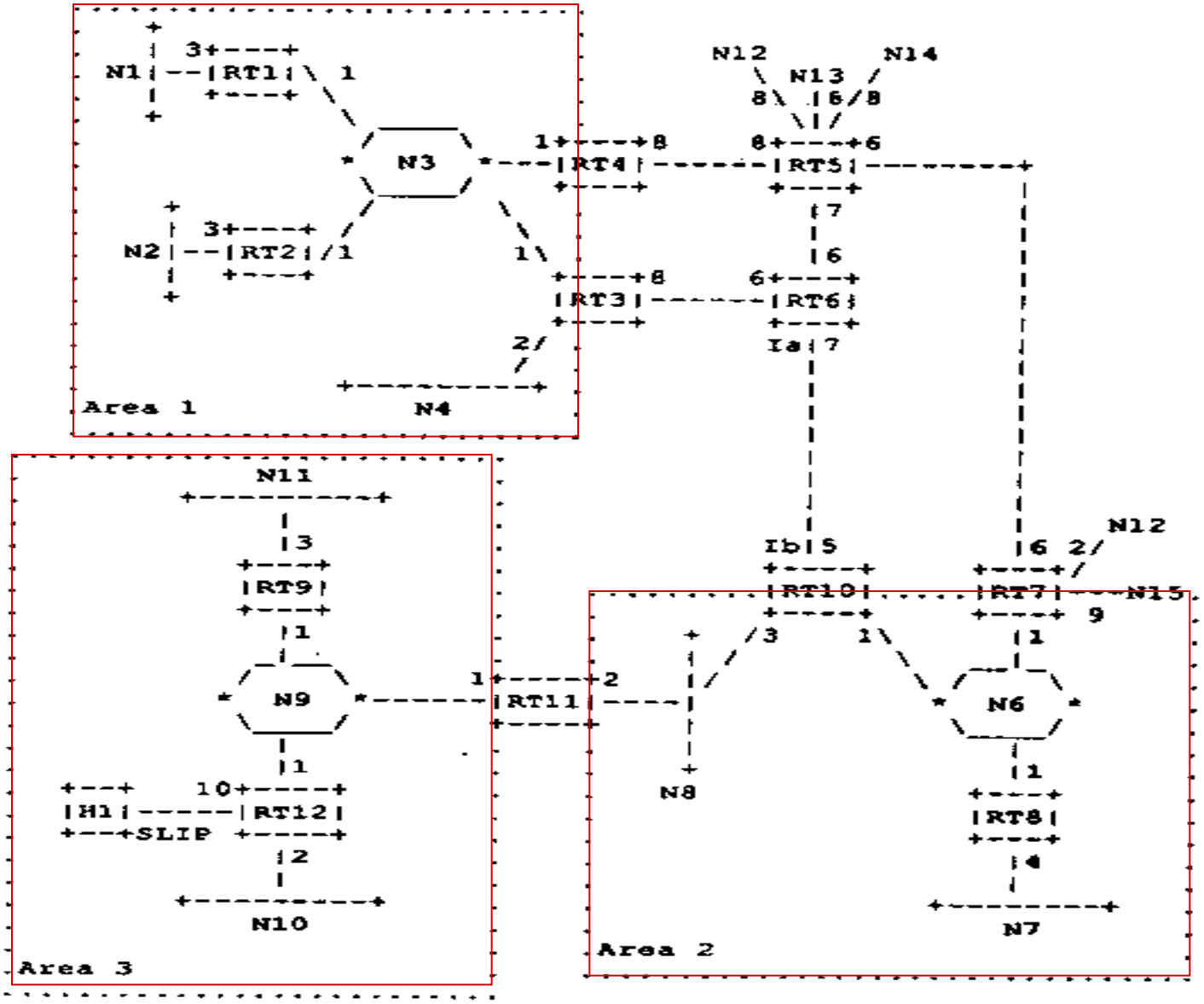


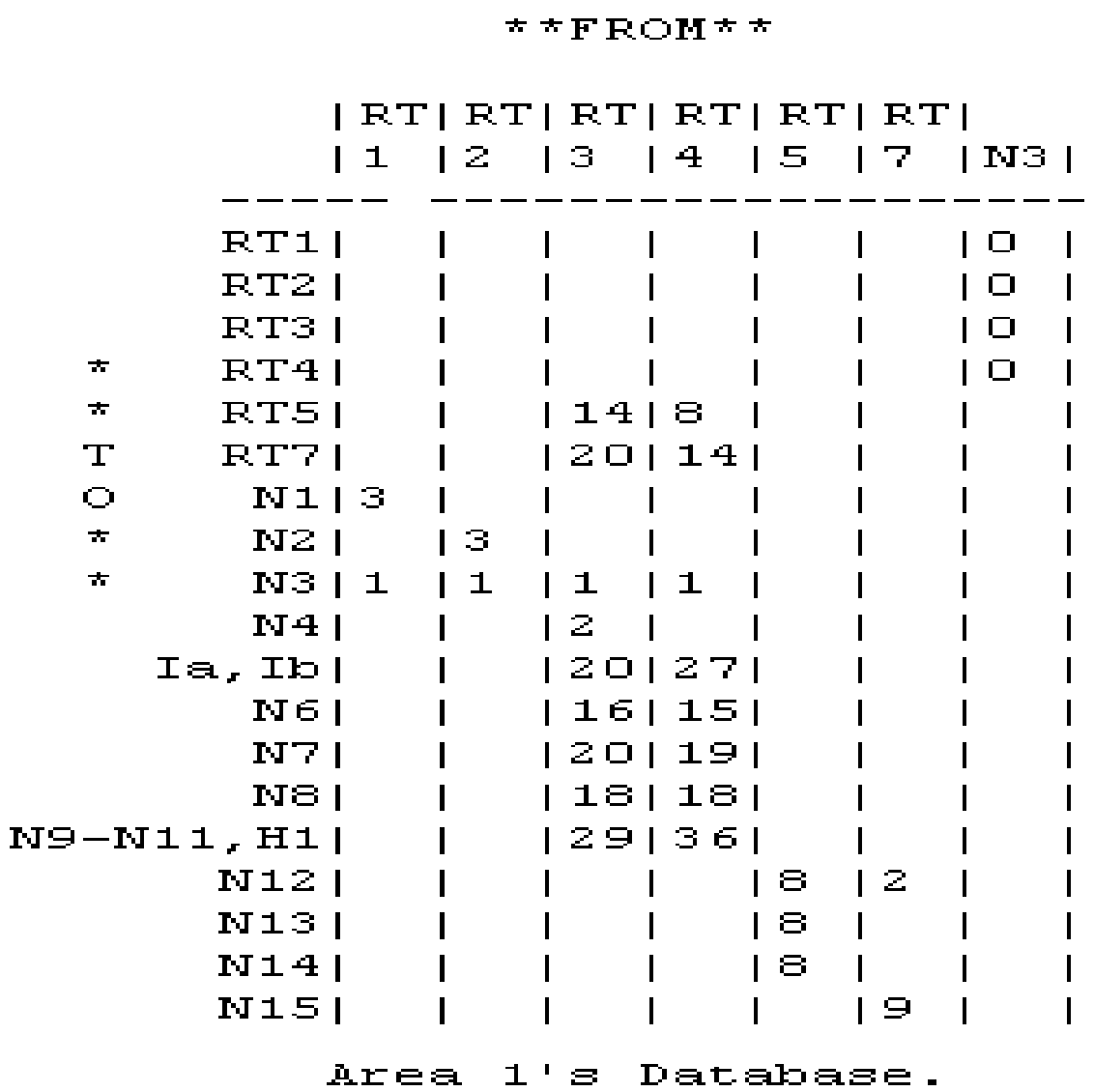
Figure 6: A sample OSPF area configuration

Exemple OSPF: Système autonome avec 3 aires

		FROM RT3	RT4	RT5	RT6	RT7	RT10	RT11
	RT3				6			
	RT4			8				
	RT5		8		6	6		
	RT6	8		7			5	
	RT7			6				
*	RT10				7			2
*	RT11						3	
T	N1	4	4					
O	N2	4	4					
*	N3	1	1					
*	N4	2	3					
	Ia						5	
	Ib				7			
	N6					1	1	3
	N7					5	5	7
	N8					4	3	2
N9-N11,H1								11
	N12			8		2		
	N13			8				
	N14			8				
	N15					9		

The backbone's database.

Exemple OSPF: Système autonome avec 3 aires



FROM

		RT1	RT2	RT3	RT4	RT5	RT7	N3
	RT1							O
	RT2							O
	RT3							O
*	RT4							O
*	RT5			14	8			
T	RT7			20	14			
O	N1	3						
*	N2		3					
*	N3	1	1	1	1			
	N4			2				
	Ia, Ib			20	27			
	N6			16	15			
	N7			20	19			
	N8			18	18			
	N9-N11, H1			29	36			
	N12					8	2	
	N13					8		
	N14					8		
	N15						9	

Area 1's Database.

Chapitre II: La Couche Réseau

- Le Concept d'Interconnexion
- Architecture Internet
- Adressage (IP, OSI)
- IP et protocoles associés (ICMP, ARP, RARP)
- Fragmentation et Réassemblage
- Routage: Généralités
- Algorithmes de Routage (LSR, DVR)
- Protocoles de RTG Internet I (RTG intra-domaine: RIP, OSPF)
- Protocoles de RTG Internet II (RTG inter-domaine: BGP)

Le Protocole BGP (Border Gateway Protocol)

- BGP est l'EGP utilisé par Internet.

- Utilisé pour le routage entre différents systèmes autonomes.

- Adapté à des topologies maillées telles que Internet.

- Utilise une stratégie de routage différente de celle utilisée par les protocoles IGP, comme il n'est pas basé sur le choix de plus courts chemins.