

Protocoles & Réseaux

Couche Réseau

Couche Réseau

- Types de service
- Algorithmes de routage
- Algorithmes de contrôle de congestion
- Interconnexion de réseaux
- Couche réseau dans Internet

Types de service

■ Service en mode datagramme:

- **Connexion:** Pas de connexion préalable
- **Routage:** Chaque paquet a un routage indépendant
- **Adressage:** Chaque paquet contient l'adresse de la source et de la destination
- **Contrôle de congestion:** Difficile et complexe
- **Conséquence d'une défaillance d'un routeur:** Perte des paquets présents dans le routeur défaillant
- **Qualité de service:** Ni contrôle d'erreurs ni contrôle de flux
⇒ travail effectué par l'utilisateur (couche transport) pour alléger la tâche du réseau
- **Analogie:** Service postal



DE

Types de service

■ Service en mode Circuit Virtuel

- **Connexion:** Nécessite une connexion préalable
- **Routage:** Route établie à l'initialisation du CV; chaque paquet utilise cette route
- **Adressage:** Chaque paquet contient le numéro du CV.
- **Contrôle de congestion:** Simple lorsqu'il est possible d'allouer les ressources nécessaires lors de l'établissement de circuit.
- **Conséquence d'une défaillance d'un routeur:** Suppression des circuits traversant le routeur défaillant.
- **Qualité de service:** Garantie.
- **Analogie:** Conversation téléphonique.



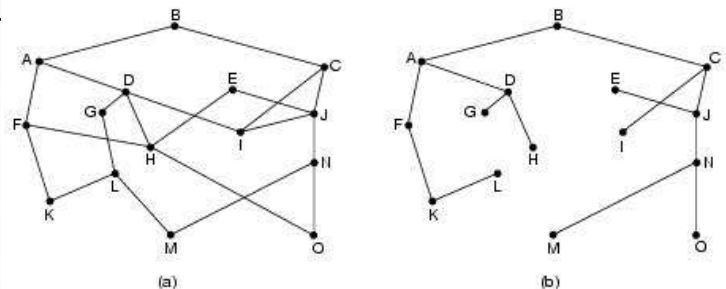
DE

Plan

- Types de service
- **Algorithmes de routage**
- Algorithmes de contrôle de congestion
- Interconnexion de réseaux
- Couche réseau dans Internet

Algorithmes de routage

- Sur quelle ligne retransmettre un paquet entrant ?
- Collaboration des routeurs pour déterminer le meilleur chemin.
- Toutes les routes optimales d'un nœud A vers les autres nœuds forment un arbre collecteur.



- Les routeurs collaborent et établissent l'arbre collecteur pour chaque nœud.

Algorithmes de routage : Classification

➤ Statiques

À l'initialisation, les routes sont pré-calculées et téléchargées dans les routeurs.

Adaptatifs

Les routes dépendent des modifications topologiques du réseau (ajout et/ou élimination des liens et/ou des routeurs) et du trafic.

➤ Centralisés

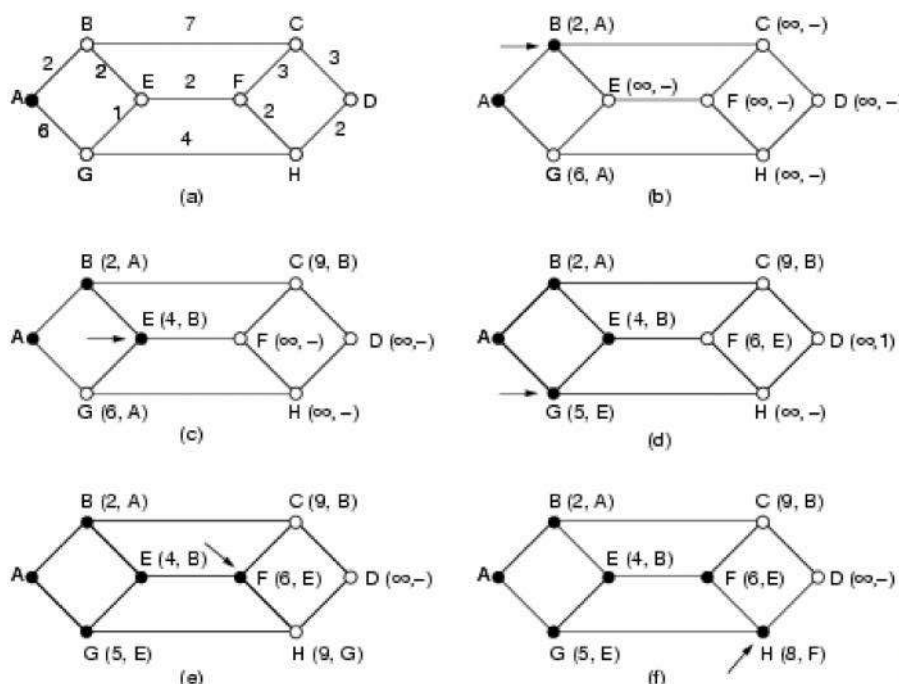
Routes calculées par un centre disposant des informations nécessaires.

➤ Distribués

Collaboration entre routeurs pour déterminer les meilleures routes.

Routage statique : Le plus court chemin (Dijkstra)

À chaque étape, choisir le nœud suivant de coût minimal et ajouter l'arc permettant de l'atteindre.



Routage statique : Inondation (Flooding)

Principe

- Un paquet entrant est retransmis sur toutes les lignes de sortie.
- Paquets dupliqués éliminés à l'arrivée.

Avantages

- Existence d'un meilleur chemin;
- Robuste (tolère la disparition de quelques nœuds intermédiaires).

Inconvénients

- Augmentation de la charge de réseau;
- Paquets dupliqués circulant indéfiniment.

Gestion des paquets dupliqués ?

- Champs compteur indiquant le nombre maximal de nœuds à traverser.
- Décrémentation du compteur à chaque routeur traversé
- Élimination du paquet si le compteur est nul.



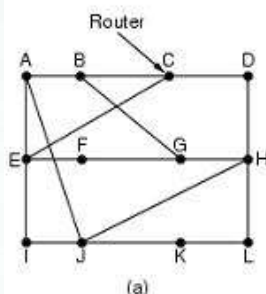
DE

Routage distribué : Routage à vecteur de distance

Principe

Chaque routeur

- Connaît les distances le séparant de ses voisins.
- Transmet, périodiquement, à tous ses voisins son vecteur de routage.
- Recalcule son vecteur de routage en fonction des informations provenant des voisins.



To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	13	7	0	-
K	24	22	22	0	6	K
L	29	33	9	9	15	K

JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6
---------------	----------------	----------------	---------------

Vectors received from J's four neighbors

New routing table for J

(b)

Exemple de tables



DE

Routage distribué : Routage à vecteur de distance

Exemple de métriques

- **Nombre de sauts:** distance entre deux voisins=1.
- **Taille de la file d'attente:** distance= le nombre de paquets dans la file d'attente de la ligne qui le sépare de son voisin.
- **Temps de transmission:** envoi d'un paquet spécial écho retourné par le nœud voisin.

Possibilité de divergence

Réactions face aux modifications: Assez rapide lors du rétablissement d'une ligne, lent si coupure d'une ligne.

Panne du routeur A.

A	B	C	D	E	
∞	∞	∞	∞	∞	Initially
1	∞	∞	∞	∞	After 1 exchange
1	2	∞	∞	∞	After 2 exchanges
1	2	3	∞	∞	After 3 exchanges
1	2	3	4	∞	After 4 exchanges

(a)

A	B	C	D	E	
∞	1	2	3	4	Initially
3	3	2	3	4	After 1 exchange
3	4	4	3	4	After 2 exchanges
5	4	5	5	4	After 3 exchanges
5	6	5	6	6	After 4 exchanges
7	6	7	6	6	After 5 exchanges
7	8	7	8	8	After 6 exchanges
∞	∞	∞	∞	∞	

(b)

Mise sous tension du routeur A



Exercice



DE

Routage distribué : Routage par information à état de liens

Périodiquement chaque routeur effectue les traitements suivants:

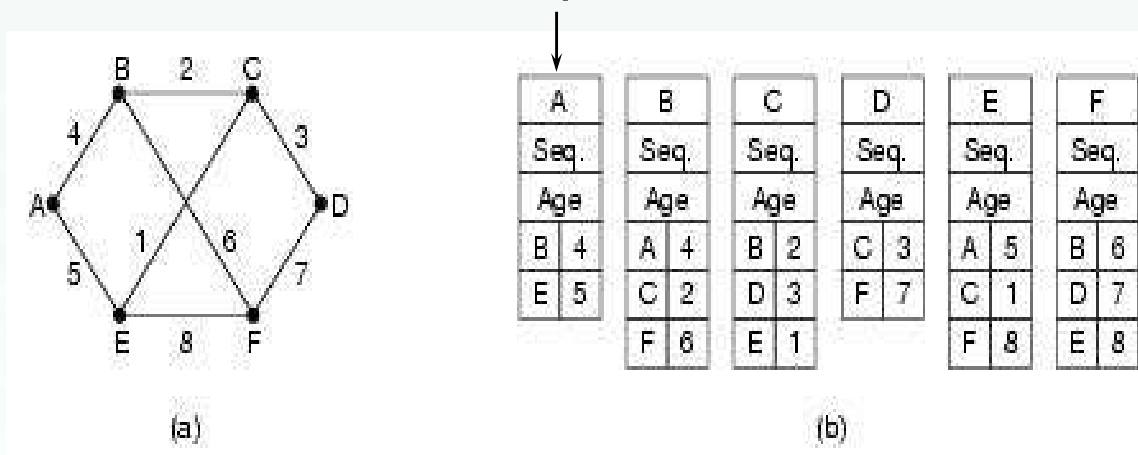
- **Découvrir ses voisins:** Envoyer un paquet (HELLO) sur chaque ligne de sortie. Ses voisins répondront en fournissant leur nom, adresse réseau,...
- **Mesurer la distance vers ses voisins.** Une solution consiste à envoyer un paquet ECHO qui sera estampé et retourné par le nœud voisin. Comme distance, on prendra la moitié du temps aller retour du paquet ECHO.
- **Diffuser les informations collectées:** Construire un paquet d'état de lien contenant les informations collectées (voisin, distance, ...) et le diffuser à tous les nœuds de réseau. (inondation par diffusion).
- **Calculer les plus courts chemins:** (exemple Dijkstra)



DE

Routage

Informations collectées par A et à diffuser aux autres



Exemple de paquets diffusés par les routeurs.

Routage Hiérarchique

Limite des algorithmes de routage

- Inondation $\Rightarrow$ augmente charge du réseau !
- Chaque routeur connaît la topologie du réseau
 - Table de routage volumineuse
 - Nécessité d'espace mémoire et temps de traitement.

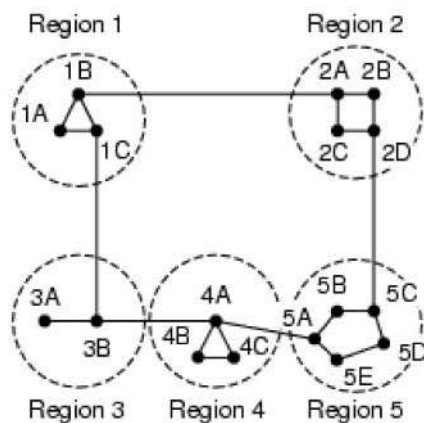
Solution

Routage Hiérarchique $\rightarrow$ Découpage en régions

Chaque routeur connaît

- Les routeurs de sa région (intra-routage);
- Les accès aux autres régions (inter-routage).

Routage Hiérarchique



Exemple

Full table for 1A

Dest.	Line	Hops
1A	—	—
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Hierarchical table for 1A

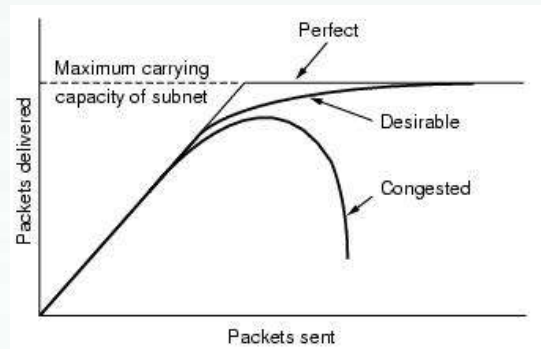
Dest.	Line	Hops
1A	—	—
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Plan

- Types de service
- Algorithmes de routage
- **Algorithmes de contrôle de congestion**
- Interconnexion de réseaux
- Couche réseau dans Internet

Congestion

Dégradation des performances du réseau si le nombre de paquets circulant atteint la capacité limite admissible.



Solutions

- Préventives

- Contrôler le nombre de paquets entrant par unité de temps dans le réseau.

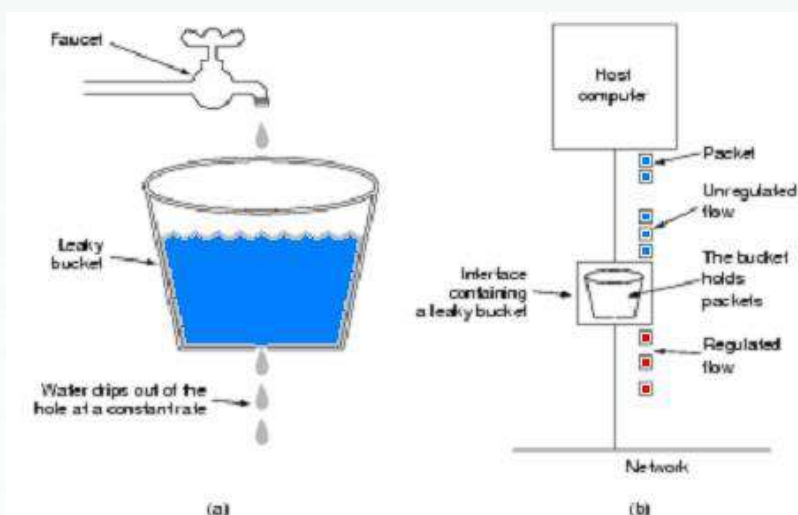
- Correctives

- Ralentir les émissions en avertissant les stations émettrices.

Congestion : Algorithme du seau percé

- Éviter les surprises: réguler le trafic entrant dans le réseau
- Serveur avec un temps de service constant
- La file d'attente du serveur est de taille limitée

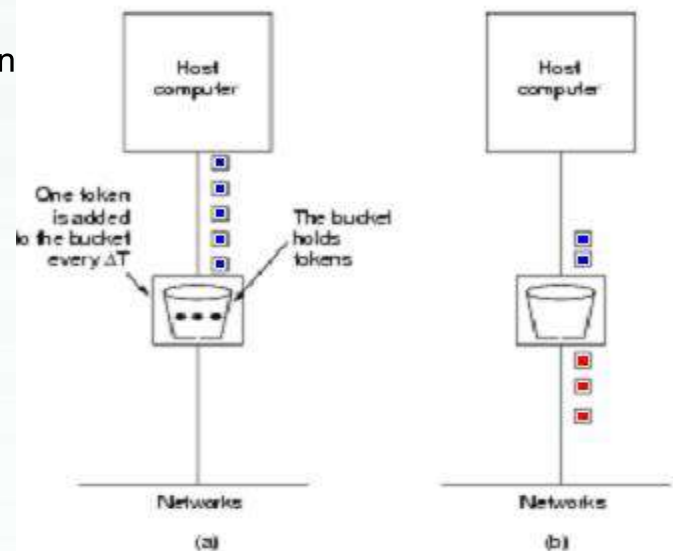
Possibilité de perdre des paquets



Congestion : Algorithme du seau percé à jetons

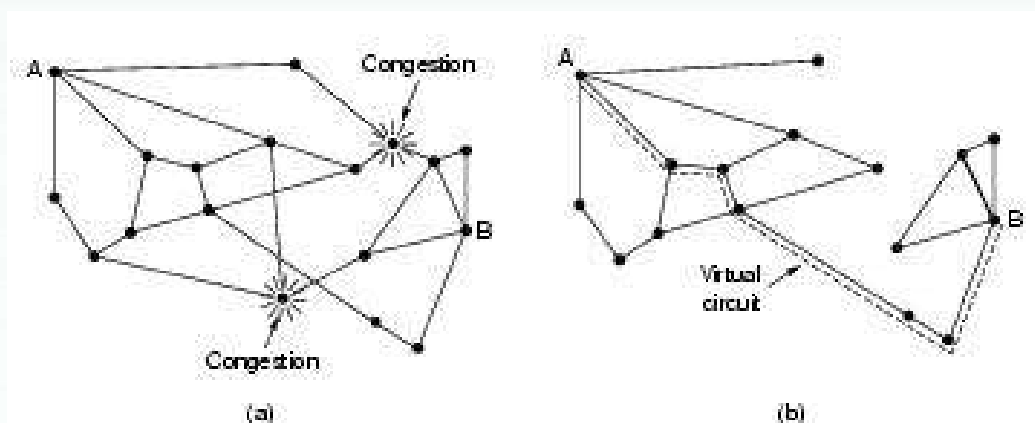
- Introduire plus de flexibilité par rapport à l'algorithme précédent
- Périodiquement, un nouveau jeton est généré

- k paquets arrivent et disposent de i jeton
 - **Si $k \leq i$ alors** transmettre k paquets
 - Sinon** transmettre i paquets
(k-i restent dans le file d'attente).



Congestion : Circuit virtuel

- Avant d'établir un circuit, s'assurer qu'il n'y aura pas de congestion
- Choisir des routes non congestionnées.
- Refuser l'établissement de circuit, si cela n'est pas possible

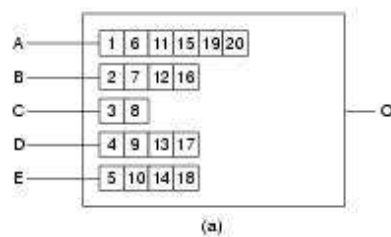


Congestion : Technique des paquets d'engorgement

- Envoyer des paquets d'engorgement aux émetteurs quand les performances du réseau commencent à se dégrader.
- Si les files d'attentes de sorties du routeur commencent à saturer, celui-ci envoie des paquets d'engorgement aux émetteurs.
- Les émetteurs sont supposés être coopératifs

L'utilisation de l'algorithme du temps équitable évite de pénaliser les émetteurs non-coopératifs.

- **Une file d'attente pour chaque émetteur**
- **Un algorithme de type round robin pour le service.**



Packet	Finishing time
C	8
B	16
D	17
E	18
A	20

(b)

Plan

- Types de service
- Algorithmes de routage
- Algorithmes de contrôle de congestion
- **Interconnexion de réseaux**
- Couche réseau dans Internet

Interconnexion de réseaux

Comment interconnecter des réseaux hétérogènes

➤ Physiquement ?

Logiquement ?

Imposer une solution ? (non réaliste !)

- Insérer une boîte noire en frontière de plusieurs réseaux hétérogènes;
- La boîte noire transparente se charge de l'interconnexion.
- Nom et fonction de la boîte dépendent de la couche où s'effectuent les conversions.



DE

Interconnexion de réseaux

Éléments d'interconnexion (boîtes noires):

Répéteur : Couche Physique - Copier des bits en transit entre deux segments de câble.

Pont : Couche Liaison : Copier et faire suivre des trames entre LAN.

Routeur : Couche Réseau : Copier et faire suivre des paquets entre réseaux.

Passerelle de transport : Mettre en relation les flux d'un protocole de couche transport.

Passerelle d'application : Interconnecter des applications de couche supérieure.



DE

Interconnexion de réseaux

Point de différences entres les réseaux

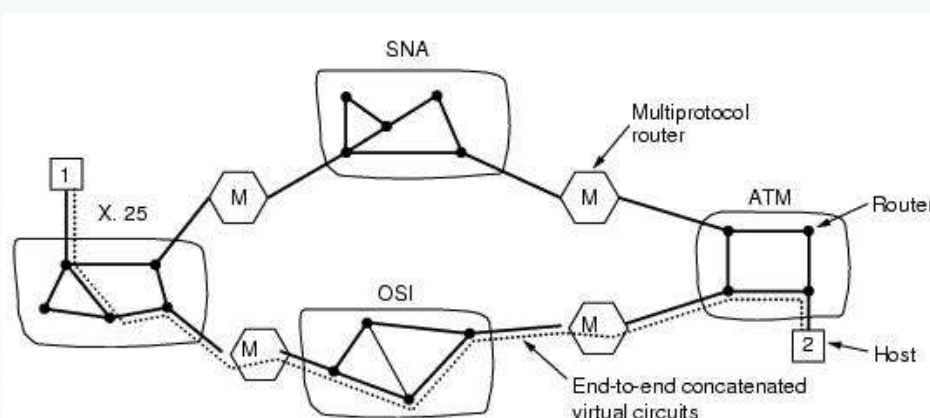
Issue	Differences
Service offered (*)	Connection-oriented vs connectionless
Protocols (*)	IP, IPX, CLNP, AppleTalk, etc.
Addressing	Flat (802) vs hierarchical
Multicasting	Present versus absent
Packet size (*)	Network-specific maximum
Quality of Service	None versus a lot versus who knows
Error handling	Reliable, (un)ordered delivery
Flow control	Sliding window, rate control, etc.
Congestion control	Leaky bucket, choke packets, etc.
Security	Privacy rules, encryption, etc.
Parameters	Timeouts, flow specs, etc.
Accounting	Connect time, packets, bytes, none

Interconnexion de réseaux : Modèle circuit virtuel

Hypothèses : Soient deux machines (1) et (2) reliées par des réseaux physiques hétérogènes et connectés par des routeurs multiprotocoles.

Si ces réseaux disposent du mode circuit virtuel

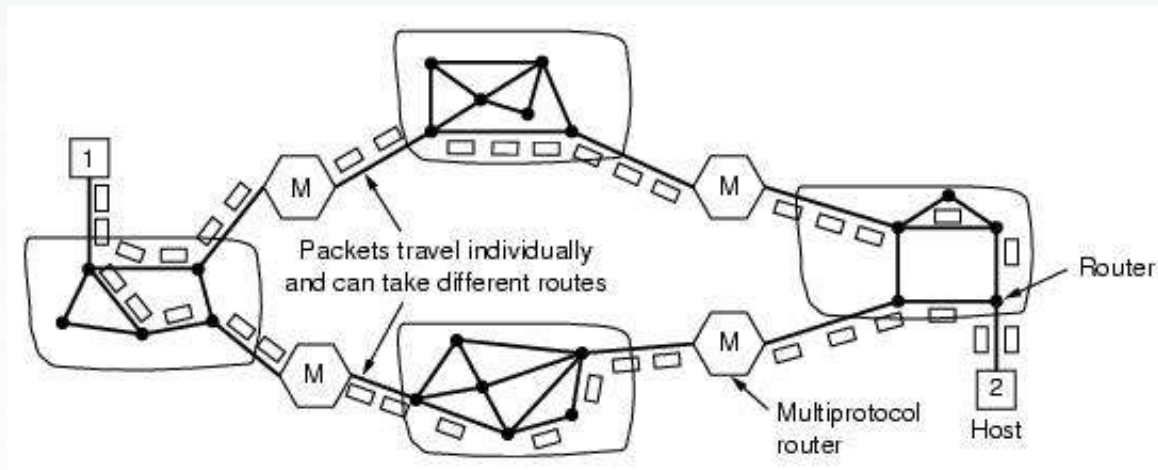
Alors un circuit virtuel pourra s'établir par concaténation des segments de circuits offerts par les différents réseaux.



Interconnexion de réseaux : Modèle circuit datagramme

Interconnexion de réseaux hétérogènes

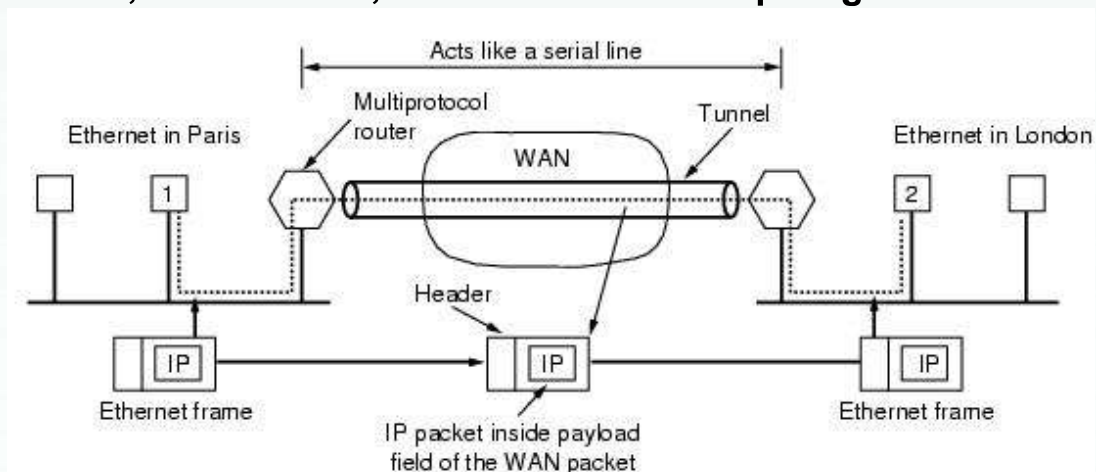
- Techniques d'adressage différentes
- Utiliser un protocole routé de couche réseau universel : IP.



Interconnexion de réseaux : Tunnel

Cas simple d'interconnexion :

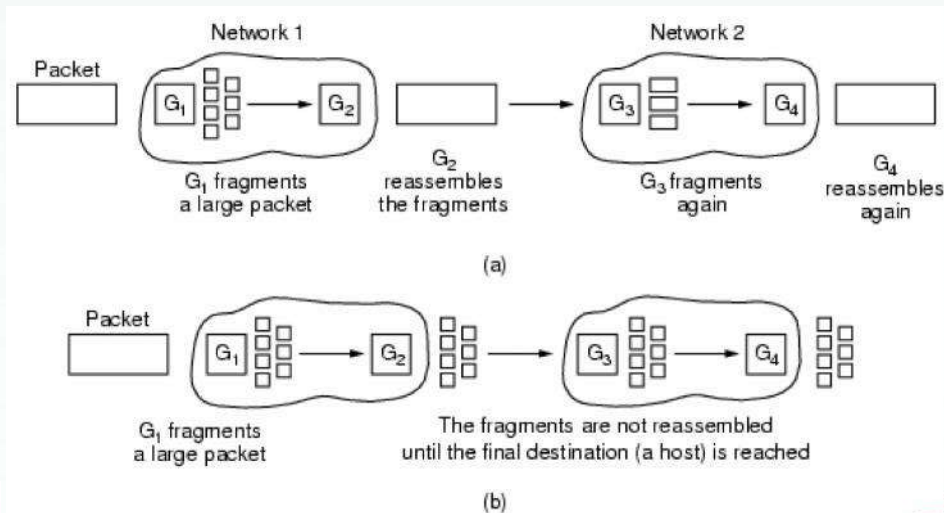
- Source et destination sont sur un même type de réseau, séparé par un (ou plusieurs) sous-réseau (x).
- Le sous-réseau intermédiaire est considéré comme un tunnel, sous-réseau, constitué d'une simple ligne de



Interconnexion de réseaux : Fragmentation

Les réseaux utilisent des paquets de tailles différentes

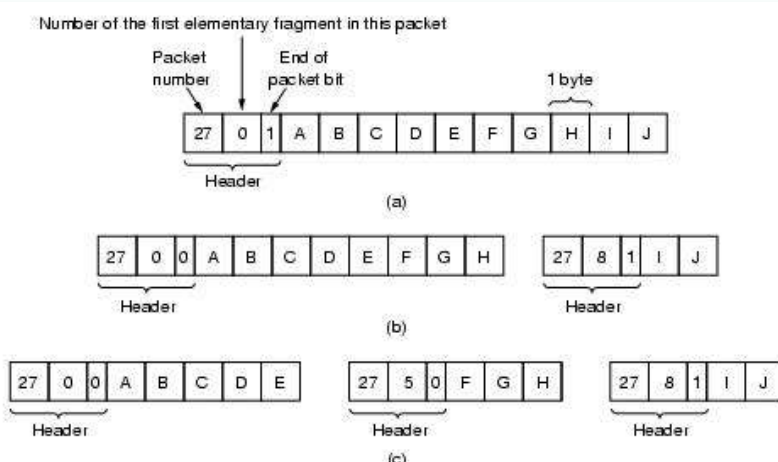
- Fragmenter un paquet en plusieurs sous-paquets
- La fragmentation peut être transparente ou non.



Interconnexion de réseaux : Réassemblage

Défragmenter un paquet IP en un ou plusieurs fragments ?

⇒ Définir un champ pour localiser le fragment à l'intérieur du paquet !



Paquet original de 10 octets

(b) Fragments obtenus dans un réseau où la taille Maximale est de 8 octets

(c) Fragments obtenus après passage des paquets de (b) par un réseau où la taille maximale est de 5 octets

Plan

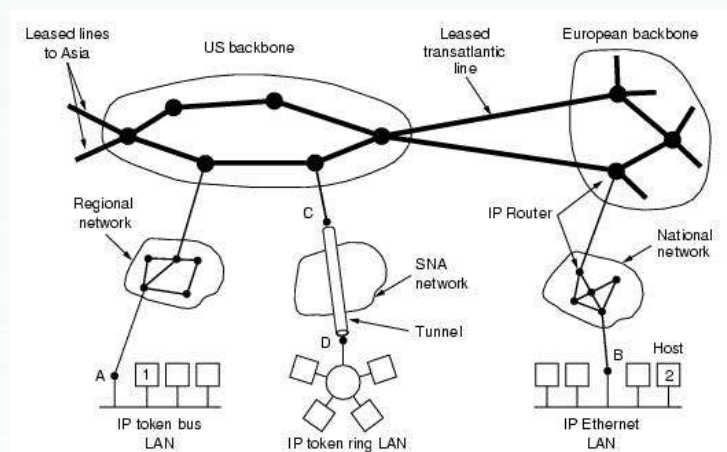
- Types de service
- Algorithmes de routage
- Algorithmes de contrôle de congestion
- Interconnexion de réseaux
- **Couche réseau dans Internet**

Couche réseau dans Internet

Internet

Ensemble de **systèmes autonomes** (sous-réseaux) connectés par des **épines dorsales**

(réseaux fédérateurs)



Couche réseau dans Internet

Protocole IP (Internet Protocol)

Protocole de convergence: masque les différences entre les réseaux.
L'utilisateur ne voit qu'un seul réseau virtuel homogène.

IP fonctionne au dessus de différents réseaux :

- une connexion physique/liaison: SLIP, PPP, ...
- un Réseau local: Ethernet, Token-Ring, WiFi...
- ATM, X25, MPLS...

IP ne nécessite qu'un service d'émission/ réception sans aucune garantie.

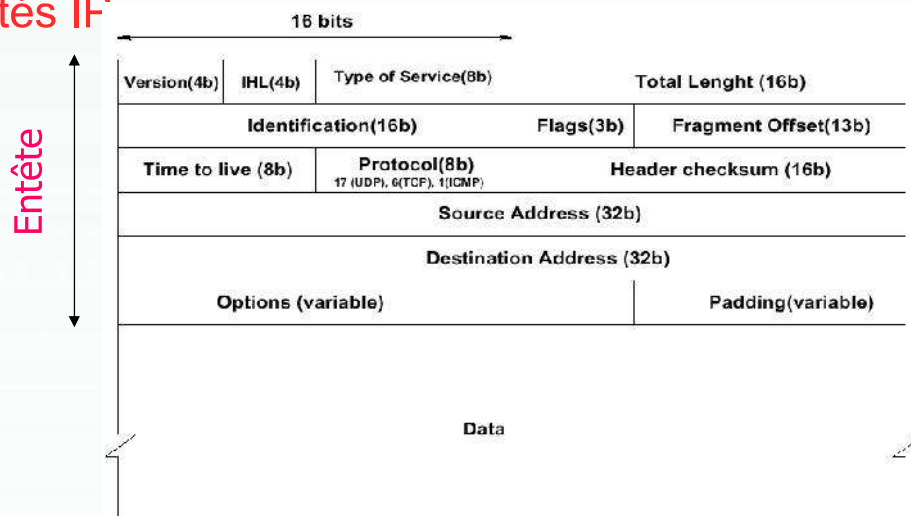
☐ **IPV4: adressage sur 4 octets (32 bits)**

☐ **IPV6: adressage sur 6 octets (128 bits)**



Protocole IP V4 Datagramme

Datagramme: Unité de données échangée par des entités IF



Protocole IP V4 Datagramme (suite)

Description

Version : Indique la version IP (IPv4, IPv6) du datagramme

Internet Header Length (IHL) : Longueur de l'entête multiple de mots de 32 bits (au moins 5 mots)

Type of Service (TOS) : Type de service souhaité

Priorité: de 0 à 7

0: priorité normale (0 par défaut)

7: priorité maximale (pour la supervision du réseau)

0	1	2	3	4	5	6	7
priorité	D	T	R	C			inutilisé

- D=1 : minimiser le délai d'acheminement
- T=1 : maximiser le débit de transmission
- R=1 : assurer une plus grande fiabilité
- C=1 : minimiser les coûts de transmission



Protocole IP V4 Datagramme

Total length :

Longueur (octets) du fragment IP incluant l'entête

Espace réservé pour ce champ : 2 octets; longueur ≤ 65535

Identifiant : Datagramme Unique.



Flags :

☐ DF (Don't Fragment) = 1

datagramme non fragmenté (segmentation interdite)

☐ MF (More Fragment) = 1

datagramme avec d'autres fragments



Protocole IP V4 Datagramme



MTU choisie divisible par 8

Données 1400 octets

En-tête datagramme

EF1 et EF2 positionnent le bit More (MF).
Le déplacement (D) est relatif au datagramme initial.

EF1 600 octets

EF2 600 octets

EF3 200 oct.

En-tête fragments: M=0; D =1200

En-tête fragments: M=1; D =600

En-tête fragments: M=1; D =00

EF1 600 octets

EF2 600 octets

EF3 200 oct.

Protocole IP V4 Datagramme

Checksum : Code détecteur d'erreur (ne s'applique qu'à l'entête)

Time to live : Durée de vie restante (nombre de routeurs à traverser)
Initialisée à N par la station émettrice, décrémenté d'une unité par le routeur récepteur.

➤ **Comment éviter qu'un datagramme ne séjourne indéfiniment dans un internet ?** Un routeur qui reçoit un datagramme de TTL nul, détruit ce dernier et avertit l'expéditeur à l'aide d'un message ICMP.

Protocol : Identification du protocole client (IP → 4, 17 → UDP, 6 → TCP, 1 → ICMP): pour remettre les données au protocole adéquat.

Options : Sécurité, enregistrement de route, horaire, routage strict, ...

Padding : Bourrage (permet à l'entête d'occuper un nombre entier de mots de 32 bits).

Protocole IP V4 : Adressage

4 octets (32 bits)

2^{32} = 4,2 milliards d'adresses possibles.

Notation «décimale pointé»:

A.B.C.D

Ex: 194.2.204.17 (www.efrei.fr); 131.108.0.0 Réseau Cisco

Deux parties:

❑ **Identifiant de réseau (*network id*):**

assigné par une autorité (NIC: *Network Information Center*).

❑ **Identifiant de la machine (*host id*):**

assigné par l'administrateur de réseau.



DE

Protocole IP V4 : Adressage

Une adresse IP doit être unique au monde

Il n'existe pas deux machines munis d'une même adresse

Un ordinateur connecté à plusieurs réseaux possède plusieurs adresses IP.

❑ Une adresse différente sur chacun des réseaux (interfaces) .

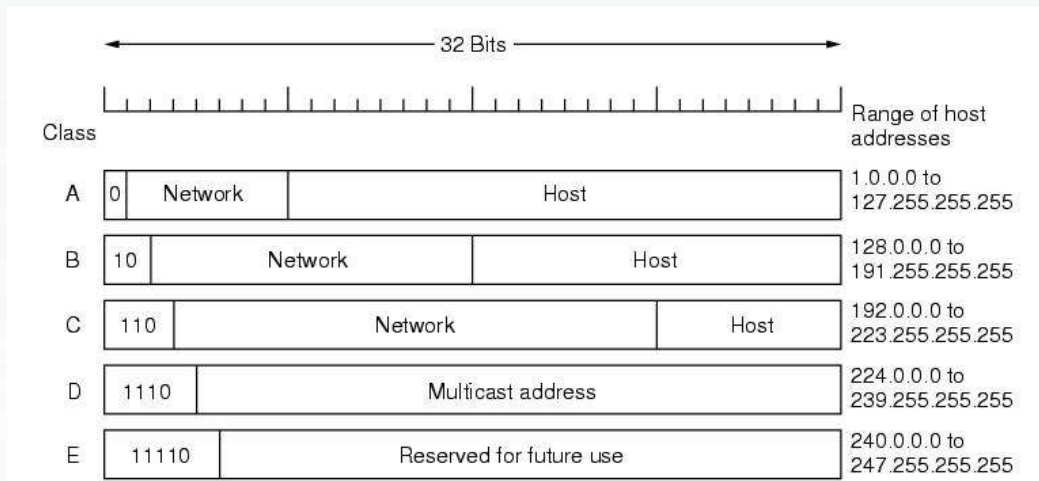
Exemple : Routeur

Une adresse n'identifie pas une machine, mais un point d'accès (interface) à un réseau.



DE

Protocole IP V4 : Adressage



Class	Max. networks	Max. hosts/network
A	126	16,777,214
B	16,382	65,536
C	2,097,150	254

Protocole IP V4 : Adressage

Classe A:



➤ 7 bits pour l'identifiant réseau

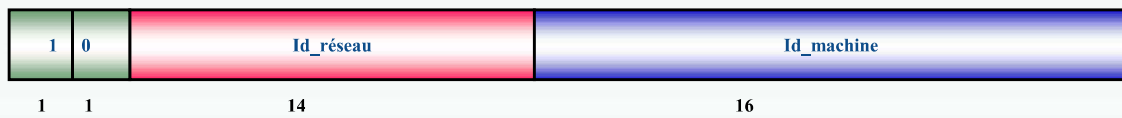
- 1.0.0.0 à 126.0.0.0
- 0.0.0.0 et 127.0.0.0 sont réservées

➤ 24 bits pour l'identifiant de la machine

→ Destinée aux Réseaux de grande taille

Protocole IP : Adressage

Classe B



➤ **14 bits pour l'identifiant réseau**

- 128.0.0.0 à 191.255.0.0

➤ **16 bits pour l'identifiant de la machine**

→ **Destinée aux Réseaux de taille moyenne**

Protocole IP : Adressage

Classe C



➤ **21 bits pour l'identifiant réseau**

192.0.1.0 à 233.255.255.0

➤ **8 bits pour l'identifiant de la machine**

→ **Destinée aux petits Réseaux**

Protocole IP : Adressage

Classe D



Adresse *multicast*: exemple vidéo-conférence

Pas de structuration, utilisée d'une manière spéciale, sans contrainte d'unicité, sans organisme gérant leur attribution

Classe E



Réservée



Protocole IP : Adressage

Adresses particulières:

127.X.X.X : bouclage (*lookback*, *lookhost*): utilisées pour les tests des logiciels, communications *inter-processus* sur la même station.

0.0.0.0 : Cette machine ! Une machine ne disposant pas d'adresse (station sans disque utilisant RARP).

Tous les bits de la partie machine sont à 0 : Désigne le réseau.

Tous les bits de la partie machine sont à 1

Désigne une diffusion sur un réseau. 132.203.255.255

Tous les bits de la partie réseau sont à 0

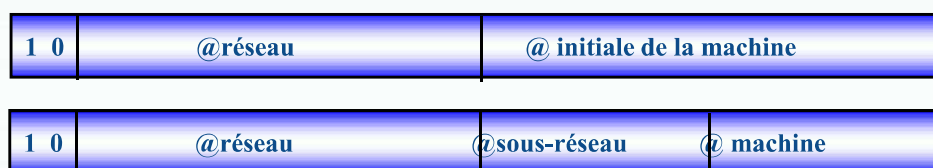
Désigne une machine sur le réseau. 0.0.128.50



Protocole IP : Adressage - Sous-réseaux

Découpage logique d'un réseau en sous-réseaux

- ☐ Géré par l'administrateur du réseau
- ☐ Segmenter le réseau, une partie des bits clients est attribuées aux réseaux.
- ☐ Meilleure structuration du réseau, amélioration du routage interne



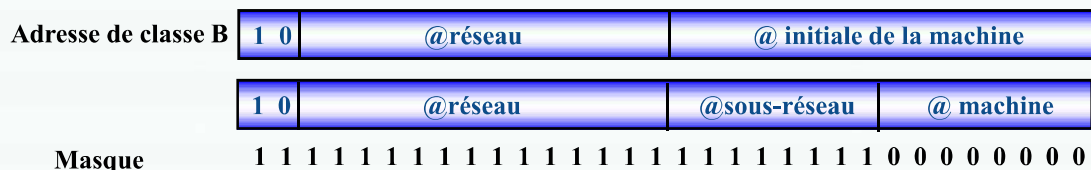
Adresse de classe B



DE

Protocole IP : Adressage - Sous-réseaux

Le découpage invisible de l'extérieur est utilisé pour le routage interne.
Tous les équipements (station, serveur, routeur, etc.) interne au réseau doivent utiliser la notion de sous-réseau.



Utilisation de masque de sous-réseau pour déterminer l'adresse:

- du sous_réseau **@IP & masque_sous_réseau = @réseau + @sous_réseau**
- de la machine **@IP & masque_sous_réseau = @machine**



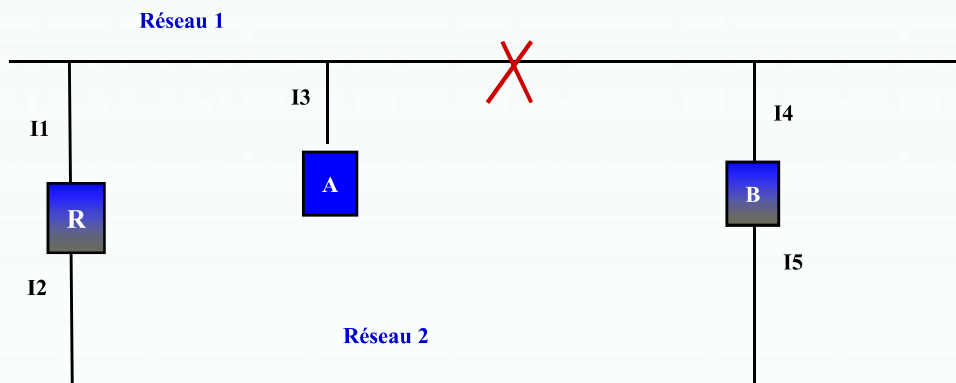
DE

Protocole IP : Adressage - Faiblesse

Mobilité: Changer de réseau $\Rightarrow$ changer d'adresse.
Changer de classe $\Rightarrow$ changer toutes les adresses.

Choix de route: Le chemin suivi par un datagramme vers un host multi-domiciliés dépend de l'adresse utilisée.

Si la ligne directe entre A et B est hors usage, alors A ne pourra plus communiquer avec B en spécifiant l'adresse I4.



Protocole IP : Protocoles de contrôle d'Internet

Internet : Réseau décentralisé

- Pas de superviseur global du réseau
- Chaque routeur fonctionne de manière autonome

Comment contrôler et gérer Internet?

$\Rightarrow$ Protocoles complémentaires : Contrôle et Gestion du réseau

ICMP, ARP, RARP.

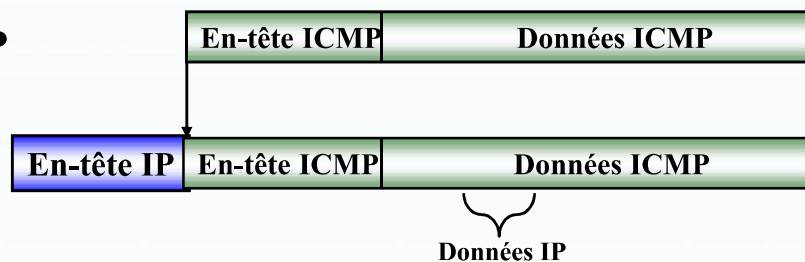
Protocole IP : ICMP (Internet Control Message Protocol)

Diagnostic du réseau Internet

- Routeurs détectent les erreurs et/ou des circonstances exceptionnelles
- Messages ICMP encapsulés dans des paquets IP

Message ICMP

Datagramme



Protocole IP : Format ICMP

Type :

Spécifie le type de message

1 octet	1 octet	2 octets
Type	Code	Somme de contrôle d'erreurs
Paramètres		
Données (optionnelles)		

Code: Informations supplémentaires sur le type de message

Somme de contrôle d'erreur : Calculé sur tout le message ICMP

Paramètres :

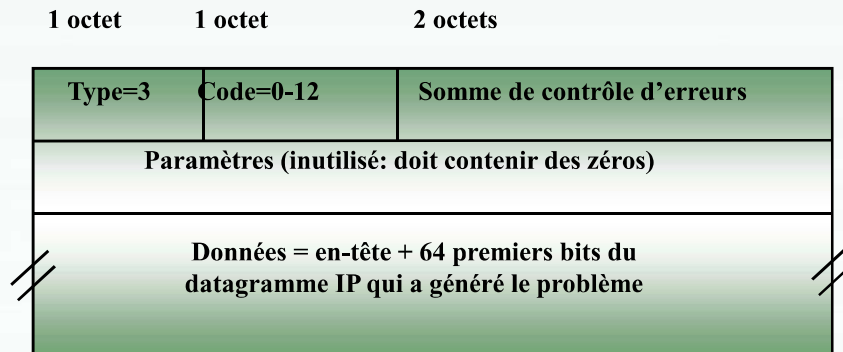
Utilisé pour indiquer l'identificateur et le numéro de séquence du message (utile lorsqu'on attend une réponse)

Données: Utilisé pour envoyer des informations additionnelles

Protocole IP : Format ICMP - Exemple de message ICMP

Destination inaccessible:

Envoyé lorsqu'un routeur ne peut délivrer un datagramme



☐ Code = 0

⇒ Réseau inaccessible.

☐ Code = 4

⇒ Fragmentation nécessaire et bit DF positionné

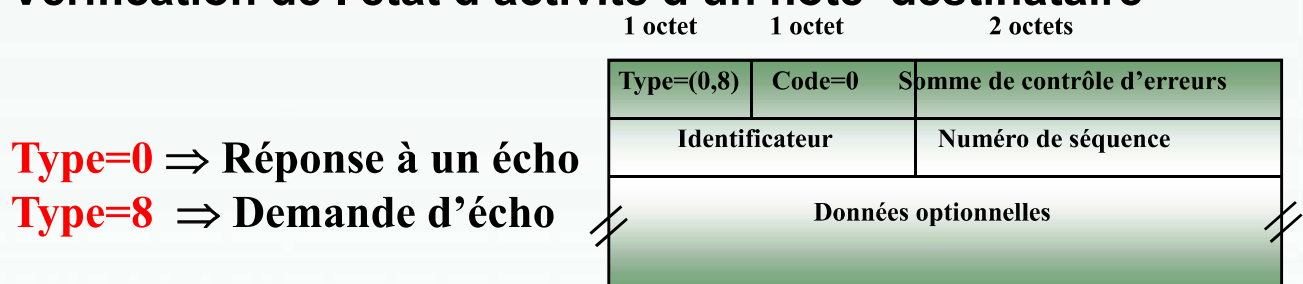


DE

Protocole IP : Format ICMP - Exemple de message ICMP

Message d'écho :

Vérification de l'état d'activité d'un hôte destinataire



Type=0 ⇒ Réponse à un écho

Type=8 ⇒ Demande d'écho

Identificateur, Numéro de séquence permettent à l'expéditeur d'associer les réponses reçues avec ses propres demandes

Tout ordinateur recevant une demande d'écho répondra à l'expéditeur.



DE

Protocole IP : Format ICMP - Exemple de message ICMP

Message d'horodate

Identique au message écho (heure d'arrivée et de retour de message seront inscrites dans la réponse).

ping

Envoie d'un message écho, pour mesurer le temps d'aller retour.

Temps expiré

envoyé lorsqu'un datagramme est détruit (TTL = 0)

traceroute (Unix) se base sur ce message pour trouver un chemin entre une source et une destination.



DE

Protocole IP : Format ICMP - Exemple de message ICMP

```
C:\> ping www.cisco.com
```

```
Pinging [198.133.219.25] with 32 bytes of data:  
Reply from 198.133.219.25: bytes=32 time=181ms TTL=232  
Reply from 198.133.219.25: bytes=32 time=160ms TTL=232  
Reply from 198.133.219.25: bytes=32 time=181ms TTL=232  
Reply from 198.133.219.25: bytes=32 time=170ms TTL=232
```

```
Ping statistics for 198.133.219.25:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 160ms, Maximum = 181ms, Average = 173ms
```



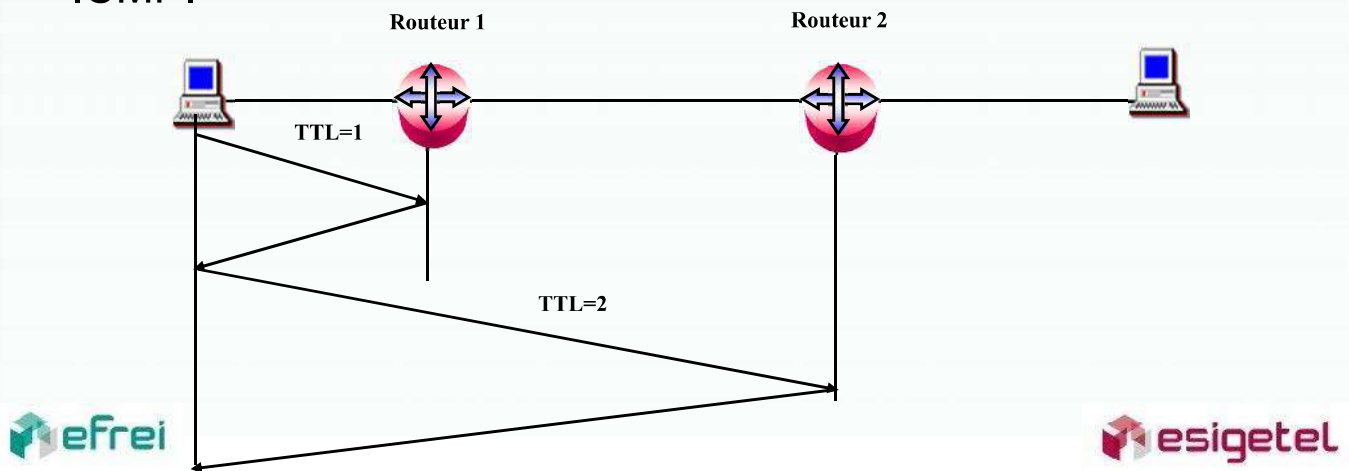
DE

Protocole IP : Format ICMP - Exemple de message ICMP

Exemple 1 : **traceroute**

1^{er} Paquet IP avec TTL=1: Le routeur 1 retourne un message ICMP indiquant le dépassement du TTL.

2^{eme} Paquet IP avec TTL=2: le routeur 2 retourne un message ICMP.



DE

Protocole IP : Format ICMP - Exemple de message ICMP

Exemple 2 : **traceroute**

c:\> Tracert www.cisco.com (windows) ⇔ traceroute sous Linux ou Unix

Extrait !!

Tracing route to www.cisco.com [198.133.219.25] over a maximum of 30 hops:

```

3  <10 ms  <10 ms  <10 ms  Efrei-GW.efrei.fr [194.2.204.254]
4   20 ms   30 ms   30 ms  217.ATM4-0.GW1.Vincennes.OLEANE.NET [194.2.2.161]
5   20 ms   30 ms   90 ms  FastEth0-0.GW2.Vincennes.OLEANE.NET [194.2.1.34]
6   20 ms   20 ms   40 ms  ATM-10-0-0-
    2.AUB7.Aubervilliers.raei.francetelecom.net [194.51.173.245]
11  20 ms   20 ms   20 ms  193.251.126.54
12  20 ms   30 ms   30 ms  P1-0.PASCR1.Pastourelle.opentransit.net
    [193.251.243.30]

```

```

23  181 ms  190 ms  180 ms  sjck-sdf-ciod-gw2.cisco.com [128.107.239.102]
24  171 ms  210 ms  270 ms  www.cisco.com [198.133.219.25]

```

Trace complete.

DE

Protocole IP : ARP (Address Resolution Protocol) & Proxy ARP

Nécessité de l'@MAC pour communiquer !

Relation entre adressage IP et MAC non bijective !

**L'Émetteur connaît l'@IP du destinataire,
mais ignore l'@MAC de ce dernier!**



DE

Protocole IP : ARP (Address Resolution Protocol) & Proxy ARP

Machines sur :

- un même Réseau

Solution statique:

Chaque machine sauvegarde toutes les @ IP et les @ MAC correspondantes.

Nombre élevé de machines

- Quantité énorme d'information
- Traitements importants

Solution dynamique: Protocole ARP

- des réseaux différents

Solution statique: ne convient pas

Solution dynamique: Proxy ARP



DE

Protocole IP : ARP (Address Resolution Protocol) Principes

ARP

Une machine diffuse une requête sur le réseau local: { @IP=W.X.Y.Z, @MAC=? }.

Seule la machine dont l'@IP= W.X.Y.Z répond à la requête en joignant son @MAC

Proxy ARP

Une machine utilise le protocole ARP et diffuse une requête sur le réseau local:

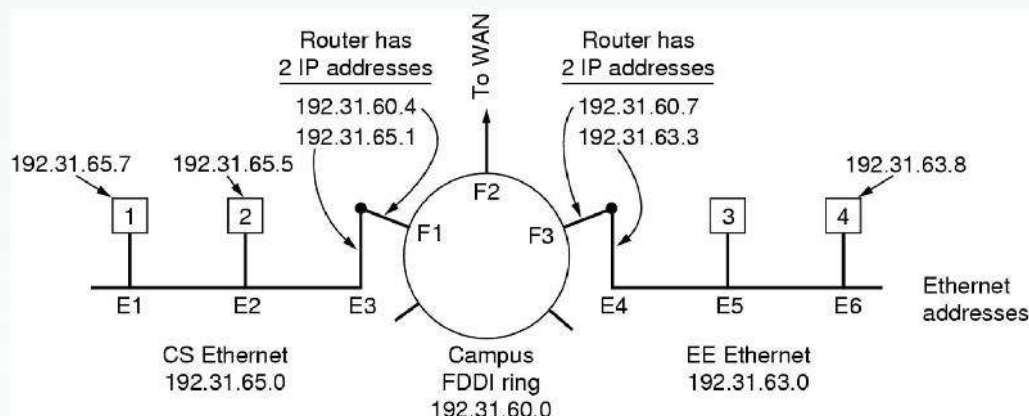
{ @IP= W.X.Y.Z, @MAC=? }

Résolution @IP $\Leftrightarrow$ @MAC ?



DE

Protocole IP : ARP (Address Resolution Protocol)



L'utilisation d'une mémoire cache améliore les performances!



DE

Protocole IP : RARP (Reverse Address Resolution Protocol)

Comment une machine sans disque dur pour sauvegarder son adresse IP, peut-elle récupérer une adresse au démarrage ?

Diffusion d'une requête RARP

{ mon @MAC= W.X.Y.Z, qui connaît mon @IP }

Un serveur RARP gérant une table {@MAC, @IP} pour les machines sans disque répond à la requête.



DE

Protocole IP : Protocoles de routage

A l'intérieur d'un Systèmes Autonome (SA ou AS) et entre Systèmes Autonomes

Routage intra-système (Interior Gateway Routing)

- Router les paquets d'une source à une destination de manière optimale
- OSPF (Open Shortest Path First)

Routage inter-system (Exterior Gateway Routing)

- Routage effectué en respectant des politiques de sécurité :
- Certains paquets ne doivent pas transiter par certains SA !!!

Exemple:

- Les paquets envoyés par Microsoft ne traverseront pas les réseaux (SA) de Cisco et réciproquement.
- BGP (Border Gateway Protocol)



DE

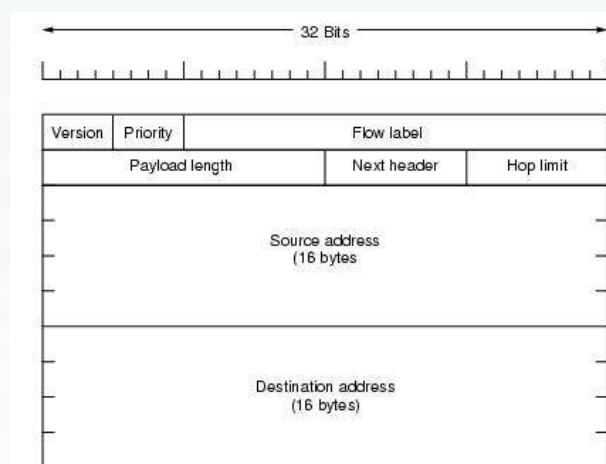
Protocole IP : IPV 6

Protocoles IPv6 pour résoudre les problèmes de IPv4

- Supporter un nombre exponentiel de machines
- Réduire la taille des tables de routage
- Simplifier le protocole pour accélérer le routage
- Augmenter la sécurité: authentification, intégrité, confidentialité, etc.
- Mieux supporter les types de services, notamment les services temps réel.
- Faire cohabiter IPv4, IPv6 ; permettre au protocole une évolution future.



Protocole IP : IPV 6 - Format en-tête



Protocole IP : IPV 6 - En-tête

- **Version (4 bits):** Identifie le numéro de la version du protocole IP
- **Priority (4 bits):**
 - 0 à 7 sont affectées aux sources capables de ralentir leur débit en cas de congestion (1 pour les *news*, 4 pour *ftp*, 6 pour *telnet*, etc.)
 - 8 à 15 sont assignées aux trafics temps réel (audio, vidéo, etc.)
- **Flow label (24 bits):** Utilisé par une source pour marquer les paquets afin de bénéficier d'un service particulier.
- **Payload Length (16 bits):** La longueur des données (en octets) après l'en-tête IPv6
- **Next Header (8 bits):** Indique le type d'en-tête suivant immédiatement l'en-tête IPv6 (TCP=6, UDP=17, ICMP=1, ...)
- **Source Address (128 bits):** @émetteur initial du paquet
- **Destination Address(128 bits):** @destination (peut être différente de l'@ de destination finale si l'option « Routing Header» est présente)



Protocole IP : IPV 6 - Format en-tête

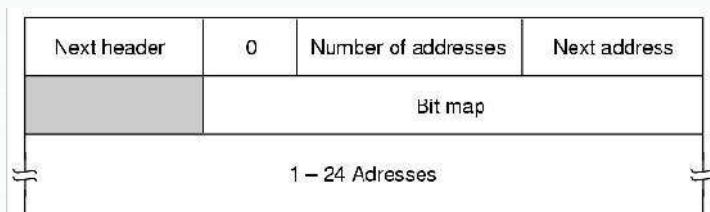
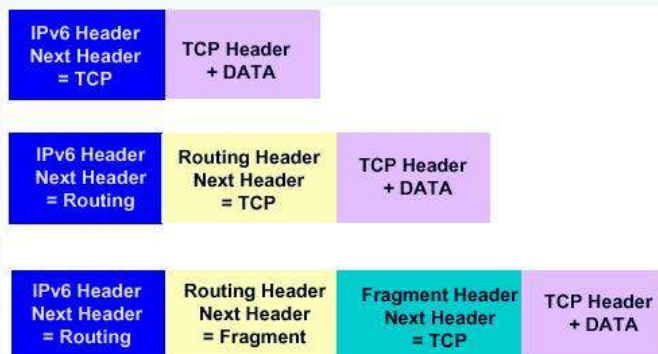
- **En-tête de base**
 - En-tête simplifiée: sans checksum, ni fragmentation.
 - Éliminer les champs occasionnels en les reportant dans la partie optionnelle.
- **En-têtes optionnelles**

Ext. header	Description
Hop-by-hop options	Information for routers
Routing	Full or partial route to follow
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted payload	Info on the encrypted contents
Destination options	Additional info for destination



Protocole IP : IPV 6 - Format en-tête

En-têtes optionnelles



Ex : Option de routage.