

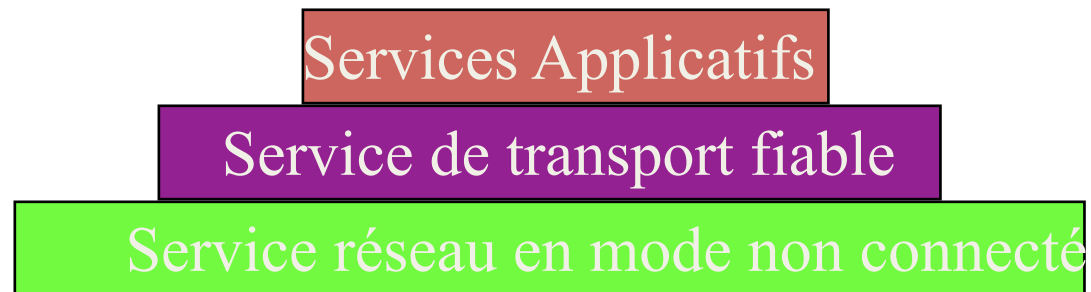
Le protocole IP

Info 0403

Hacène Fouchal

IP : Internet Protocol

- Le protocole Internet (Internet Protocol ou IP) :
 - réalise les fonctionnalités de la couche réseau selon le modèle OSI
 - se situe au coeur de l'architecture TCP/IP qui met en oeuvre un mode de transport fiable (TCP) sur un service réseau en mode non connecté :



- ✦ **Le service offert par le protocole IP est dit non fiable :**
 - remise de paquets non garantie,
 - sans connexion (paquets traités indépendamment les uns des autres),
 - pour le mieux (*best effort*, les paquets ne sont pas éliminés sans raison).

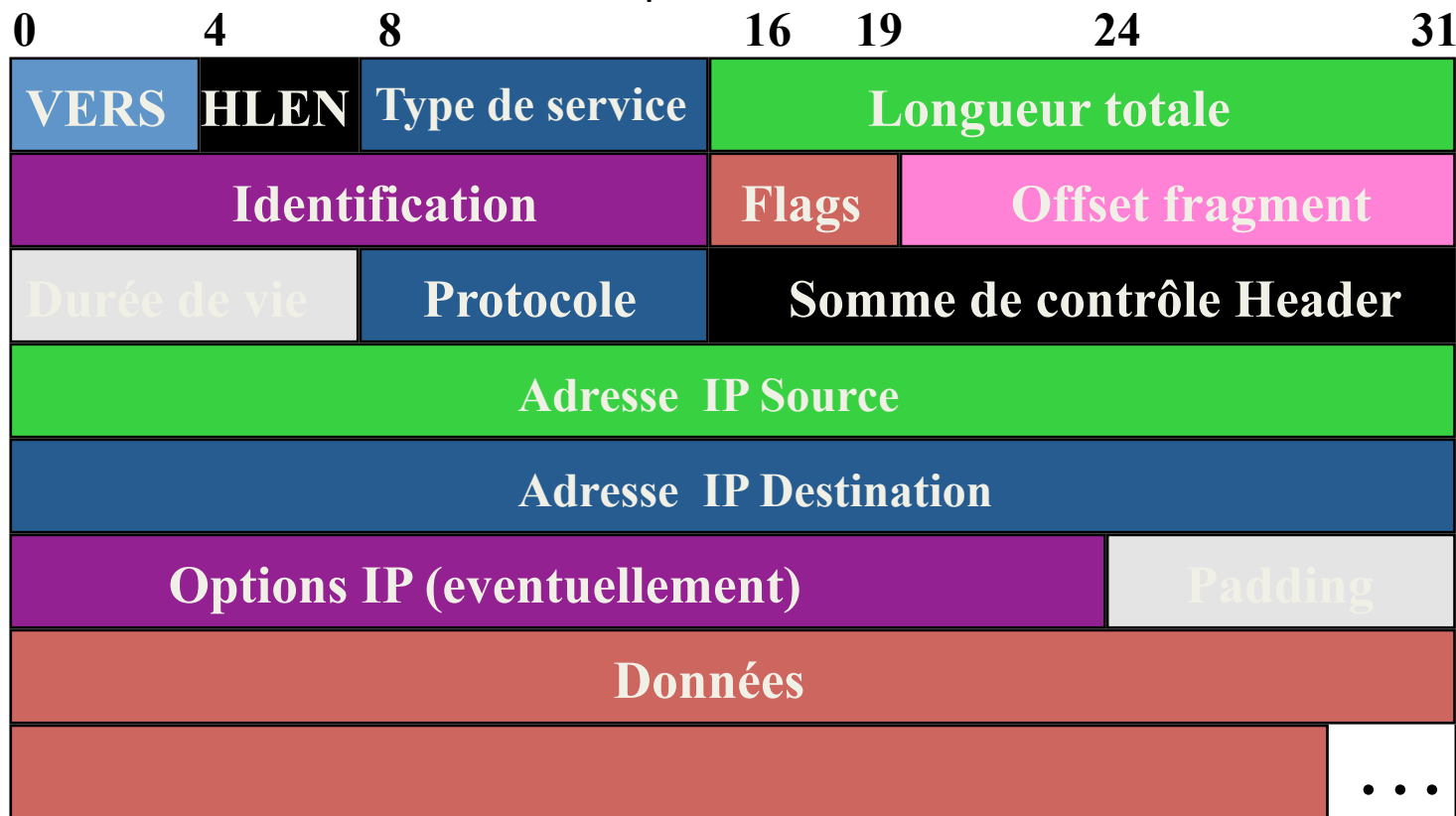
IP : Internet Protocol (suite)

- Le protocole IP définit :
 - l'unité de donnée transférée dans les interconnexions (datagramme),
 - la fonction de routage,
 - les règles qui mettent en oeuvre la remise de paquets en mode non connecté (relayage),

IP : Internet Protocol (le datagramme)

- Le datagramme IP

L'unité de transfert de base dans un réseau internet est le datagramme qui est constituée d'un en-tête et d'un champ de données:



IP : Internet Protocol (le datagramme)

Signification des champs du datagramme IP :

- **VERS** : numéro de version de protocole IP, actuellement version 4,
- **HLEN** : longueur de l'en-tête en mots de 32 bits, généralement égal à 5 (pas d'option),
- **Longueur totale** : longueur totale du datagramme (en-tête + données)
- **Type de service** : indique comment le datagramme doit être géré :



- **PRECEDENCE (3 bits)** : définit la priorité du datagramme; en général ignoré par les machines et passerelles (pb de congestion).
- **Bits D, T, R** : indiquent le type d'acheminement désiré du datagramme, permettant à une passerelle de choisir entre plusieurs routes (si elles existent) : D signifie délai court, T signifie débit élevé et R signifie grande fiabilité.

IP : Internet Protocol

(le datagramme)

- FRAGMENT OFFSET, FLAGS, IDENTIFICATION : les champs de la fragmentation.
 - Sur toute machine ou passerelle mettant en oeuvre TCP/IP une unité maximale de transfert (*Maximum Transfert Unit* ou MTU) définit la taille maximale d'un datagramme véhiculé sur le réseau physique correspondant
 - lorsque le datagramme est routé vers un réseau physique dont le MTU est plus petit que le MTU courant, la passerelle fragmente le datagramme en un certain nombre de fragments, véhiculés par autant de trames sur le réseau physique correspondant,
 - lorsque le datagramme est routé vers un réseau physique dont le MTU est supérieur au MTU courant, la passerelle route les fragments tels quels (rappel : les datagrammes peuvent emprunter des chemins différents),
 - le destinataire final reconstitue le datagramme initial à partir de l'ensemble des fragments reçus; la taille de ces fragments correspond au plus petit MTU emprunté sur le réseau. Si un seul des fragments est perdu, le datagramme initial est considéré comme perdu : la probabilité de perte d'un datagramme augmente avec la fragmentation.

IP : Internet Protocol

(le datagramme)

- FRAGMENT OFFSET : indique le déplacement des données contenues dans le fragment par rapport au datagramme initial. C'est un multiple de 8 octets; la taille du fragment est donc également un multiple de 8 octets.
- chaque fragment a une structure identique à celle du datagramme initial, seul les champs FLAGS et FRAGMENT OFFSET sont spécifiques.

IP : Internet Protocol (le datagramme)



En-tête datagramme

EF1 et EF2 ont le bit More (M) positionné.
Le déplacement (depl) est relatif au datagramme initial.

EF1 600 octets

EF2 600 octets

EF3 200 oct.

En-tête fragments: M=0; depl=1200

En-tête fragments: M=1; depl=600

En-tête fragments: M=1; depl=00

EF1 600 octets

EF2 600 octets

EF3 200 oct.

IP : Internet Protocol

(le datagramme)

- **Longueur totale** : taille du fragment et non pas celle du datagramme initial, à partir du dernier fragment (TOTAL LENGTH, FRAGMENT OFFSET et FLAGS) on peut déterminer la taille du datagramme initial.
- **IDENTIFICATION** : entier qui identifie le datagramme initial (utilisé pour la reconstitution à partir des fragments qui ont tous la même valeur).
- **FLAGS** contient un bit appelé "*do not fragment*" (01X)
- un autre bit appelé "*More fragments*" (FLAGS = 001 signifie d'autres fragments à suivre) permet au destinataire final de reconstituer le datagramme initial en identifiant les différents fragments (milieu ou fin du datagramme initial)
- les passerelles doivent accepter des datagrammes dont la taille maximale correspond à celle du MTU le plus grand, des réseaux auxquels elle est connectée.
- les passerelles doivent accepter sans les fragmenter, les datagrammes de longueur 576 octets.

IP : Internet Protocol (le datagramme)

- Durée de vie

- Ce champ indique en secondes, la durée maximale de transit du datagramme sur l'internet. La machine qui émet le datagramme définit sa durée de vie.
- Les passerelles qui traitent le datagramme doivent décrémenter sa durée de vie du nombre de secondes (1 au minimum) que le datagramme a passé pendant son séjour dans la passerelle; lorsque celle-ci expire le datagramme est détruit et un message d'erreur est renvoyé à l'émetteur.

- Protocole

Ce champ identifie le protocole de niveau supérieur dont le message est véhiculé dans le champ données du datagramme :

- 6 : TCP,
- 17 : UDP,
- 1 : ICMP.

IP : Internet Protocol

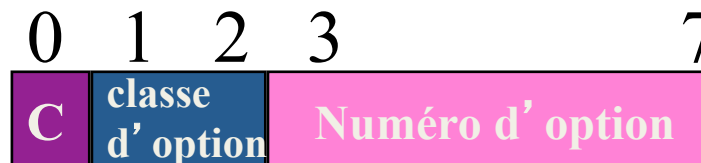
(le datagramme)

- Somme de contrôle de l'en-tête
 - Ce champ permet de détecter les erreurs survenant dans l'en-tête du datagramme, et par conséquent l'intégrité du datagramme.
 - Le total de contrôle d'IP porte sur l'en-tête du datagramme et non sur les données véhiculées. Lors du calcul, le champ HEADER CHECKSUM est supposé contenir la valeur 0

IP : Internet Protocol (le datagramme)

- **OPTIONS**

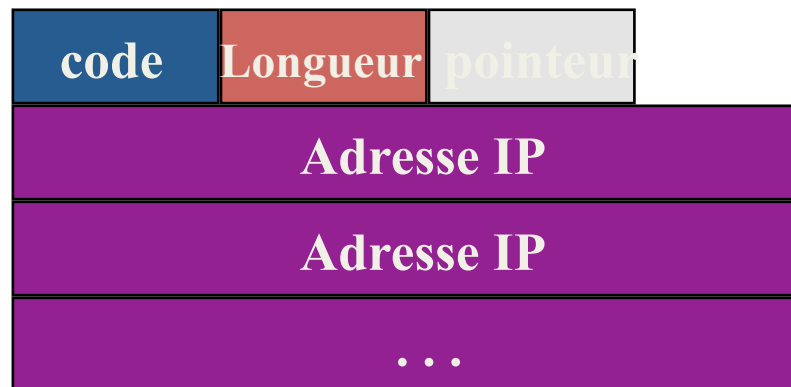
- Le champ OPTIONS est facultatif et de longueur variable. Les options concernent essentiellement des fonctionnalités de mise au point. Une option est définie par un champ octet :



- **copie (C)** indique que l'option doit être recopiée dans tous les fragments (c=1) ou bien uniquement dans le premier fragment (c=0).
- les bits **classe d'option** et **numéro d'option** indiquent le type de l'option et une option particulière de ce type :

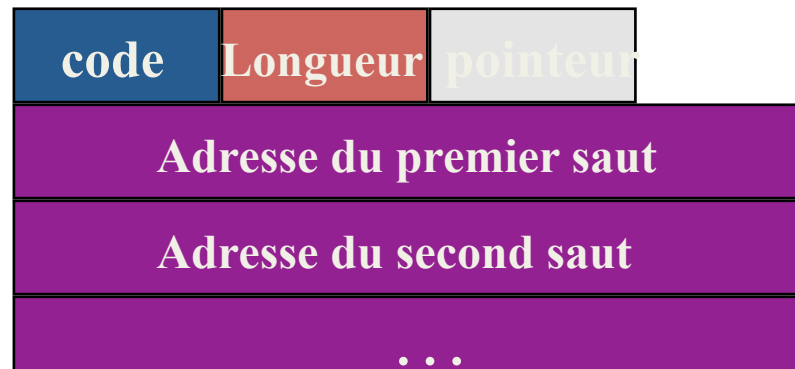
IP : Internet Protocol (le datagramme)

- Enregistrement de route (classe = 0, option = 7) : permet à la source de créer une liste d'adresse IP vide et de demander à chaque passerelle d'ajouter son adresse dans la liste.



IP : Internet Protocol (le datagramme)

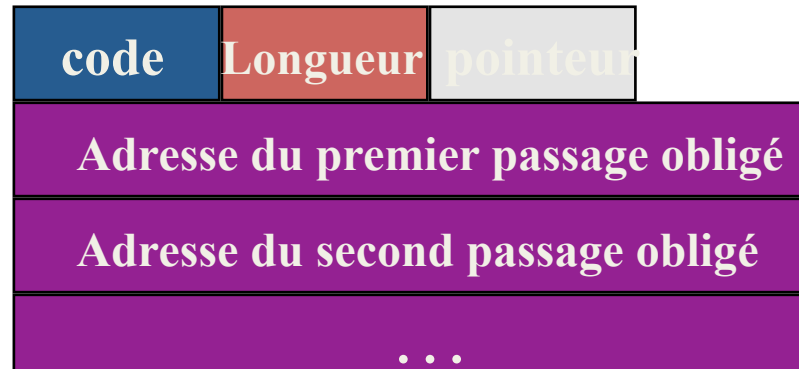
- Routage strict prédéfini par l'émetteur (classe = 0, option = 9):
prédéfini le routage qui doit être utilisé dans l'interconnexion en indiquant la suite des adresses IP dans l'option :



- ♦ **Le chemin spécifié ne tolère aucun autre intermédiaire; une erreur est retournée à l'émetteur si une passerelle ne peut appliquer le routage spécifié.**
- ♦ **Les passerelles enregistrent successivement leur adresse à l'emplacement indiqué par le champ *pointeur*.**

IP : Internet Protocol (le datagramme)

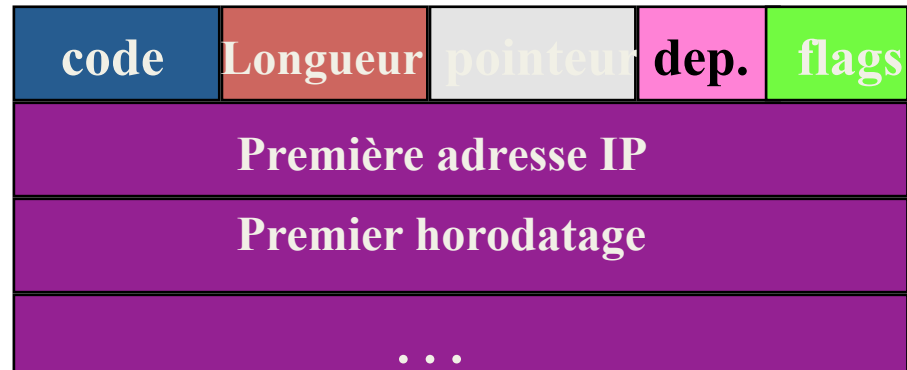
- Routage lâche prédéfini par l'émetteur (classe = 0, option = 3):
Cette option autorise, entre deux passages obligés, le transit par d'autres intermédiaires :



IP : Internet Protocol

(le datagramme)

- Horodatage (classe = 2, option = 4) : cette option permet d'obtenir les temps de passage (*timestamp*) des datagrammes dans les passerelles. Exprimé en heure et date universelle.



- Une liste de couples (adresse IP - horodatage) est réservée par l'émetteur; les passerelles ont à charge de remplir un champ lors du passage du datagramme.

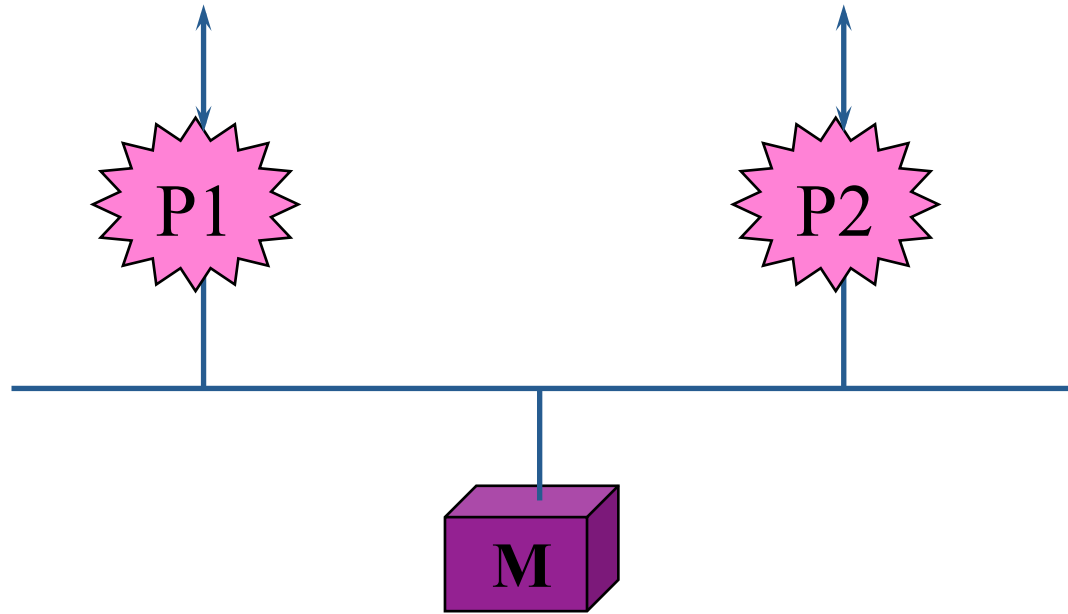
IP : Internet Protocol (le datagramme)

- Le champ dépassement de capacité (dep.) comptabilise les passerelles qui n'ont pu fournir les informations requises (liste initiale était trop petite).
- Le champ FLAGS indique si les passerelles doivent renseigner uniquement l'horodatage (FLAGS = 0), ou bien l'horodatage et l'adresse IP (FLAGS=1). Si les adresses IP sont prédéfinies par l'émetteur (FLAGS=3), les passerelles n'indiquent l'horodatage que si l'adresse IP pointée par le champ *pointeur* est identique à leur adresse IP.
- Les horodatages, bien qu'exprimés en temps universel, ne constituent qu'une estimation sur le temps de passage car les horloges des machines situées sur les réseaux ne sont pas synchronisées.

Routage des datagrammes

- Le routage est le processus permettant à un datagramme d'être acheminé vers le destinataire lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur.
- Le chemin parcouru est le résultat du processus de routage qui effectue les choix nécessaires afin d'acheminer le datagramme.
- Les routeurs forment une structure coopérative de telle manière qu'un datagramme transite de passerelle en passerelle jusqu'à ce que l'une d'entre elles le délivre à son destinataire. Un routeur possède deux ou plusieurs connexions réseaux tandis qu'une machine possède généralement qu'une seule connexion.
- Machines et routeurs participent au routage :
 - les machines doivent déterminer si le datagramme doit être délivré sur le réseau physique sur lequel elles sont connectées (routage direct) ou bien si le datagramme doit être acheminé vers une passerelle; dans ce cas (routage indirect), elle doit identifier la passerelle appropriée.
 - les passerelles effectuent le choix de routage vers d'autres passerelles afin d'acheminer le datagramme vers sa destination finale.

Routage des datagrammes (suite)



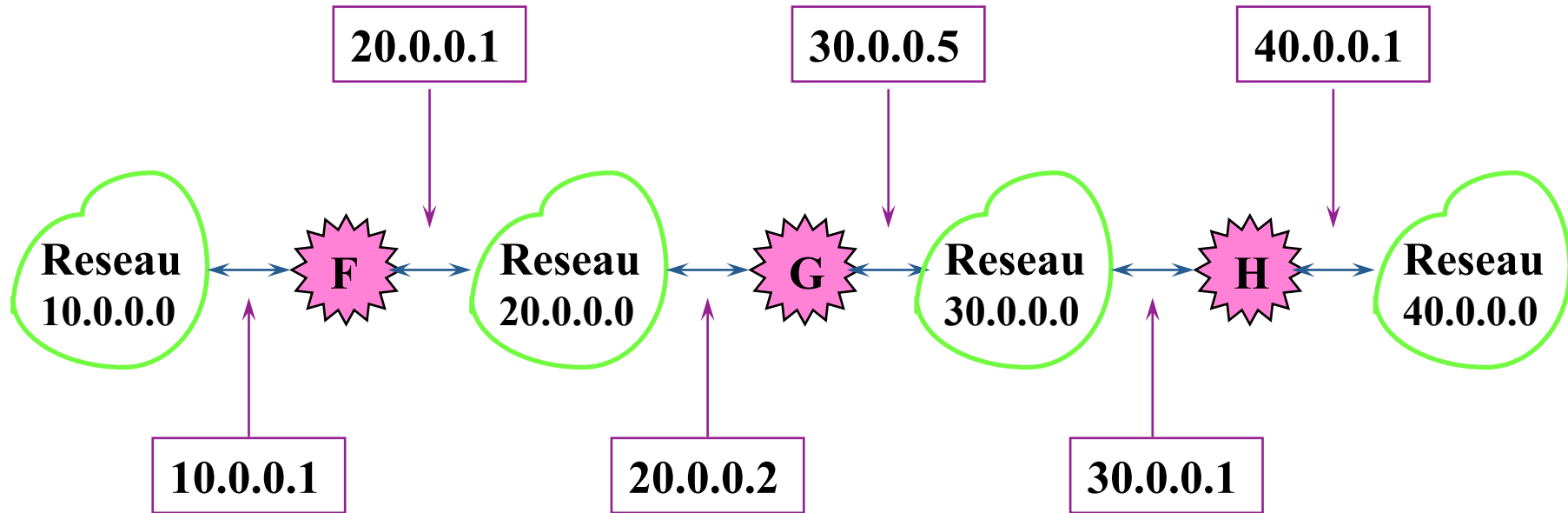
M est mono-domiciliée et doit acheminer les datagrammes vers une des passerelles P1 ou P2; elle effectue donc le premier routage. Dans cette situation, aucune solution n'offre un meilleur choix.

Le routage indirect repose sur une table de routage IP, présente sur toute machine et passerelle, indiquant la manière d'atteindre un ensemble de destinations.

Routage des datagrammes (suite)

- Les tables de routage IP, pour des raisons évidentes d'encombrement, renseignent seulement les adresses réseaux et non pas les adresses machines.
- Typiquement, une table de routage contient des couples (R, P) où R est l'adresse IP d'un réseau destination et P est l'adresse IP de la passerelle correspondant au prochain saut dans le cheminement vers le réseau destinataire.
- La passerelle ne connaît pas le chemin complet pour atteindre la destination.
- Pour une table de routage contenant des couples (R, P) et appartenant à la machine M, P et M sont connectés sur le même réseau physique dont l'adresse de niveau réseau (partie Netid de l'adresse IP) est R.

Routage des datagrammes (suite)



Pour atteindre les machines du réseau	10.0.0.0	20.0.0.0	30.0.0.0	40.0.0.0
Router vers	20.0.0.1	direct	direct	30.0.0.1

Table de routage de G

Routage des datagrammes (suite)

`Route_Datagramme_IP(datagramme, table_de_routage)`

- Extraire l'adresse IP destination, ID, du datagramme,
- Calculer l'adresse du réseau destination, IN.
- Si IN correspondant à une adresse de réseau directement accessible,
envoyer le datagramme vers sa destination, sur ce réseau.
- sinon si dans la table de routage, il existe une route vers ID
router le datagramme selon les informations contenues dans la table de routage.
- sinon si IN apparaît dans la table de routage,
router le datagramme selon les informations contenues dans la table de routage.
- sinon s'il existe une route par défaut
router le datagramme vers la passerelle par défaut.
- sinon déclarer une erreur de routage (quasiment impossible).

Routage des datagrammes (suite)

- Après exécution de l'algorithme de routage, IP transmet le datagramme ainsi que l'adresse IP déterminée, à l'interface réseau vers lequel le datagramme doit être acheminé.
- L'interface réseau détermine alors l'adresse physique associée à l'adresse IP et achemine le datagramme sans l'avoir modifié (l'adresse IP du prochain saut n'est sauvegardée nulle part).
- Si le datagramme est acheminé vers une autre passerelle, il est à nouveau géré de la même manière, et ainsi de suite jusqu'à sa destination finale.

Routage des datagrammes (suite)

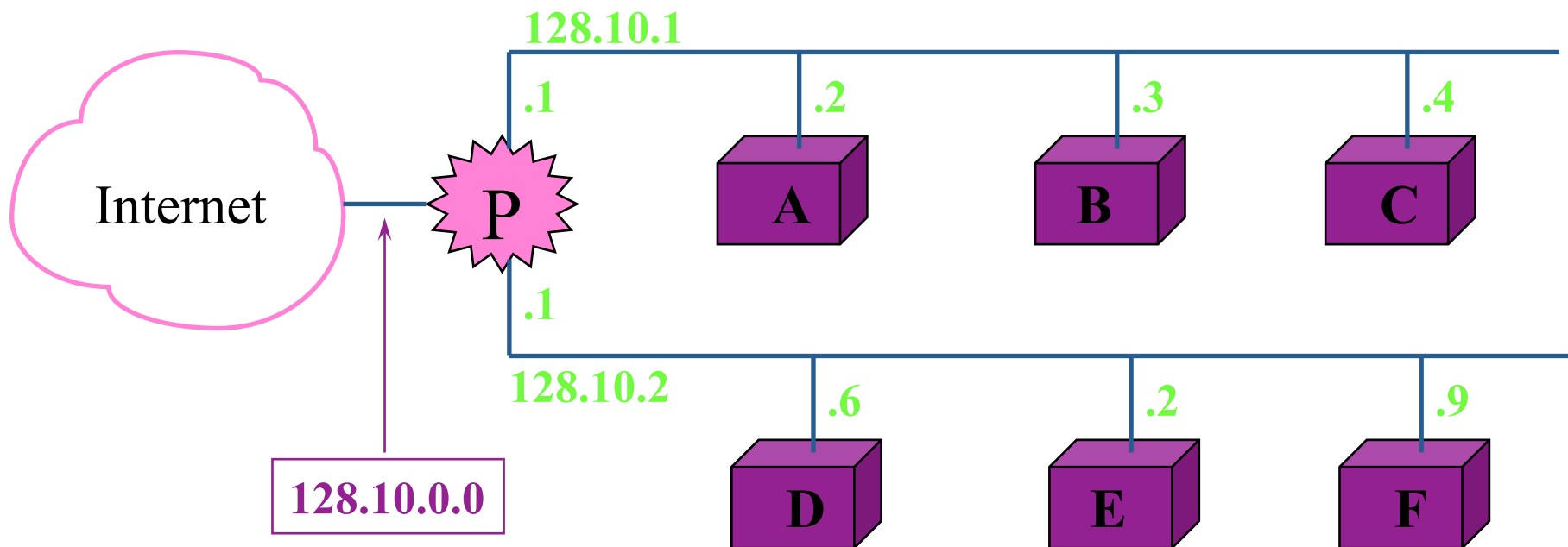
- Les datagrammes entrants sont traités différemment selon qu’ il sont reçus par une machine ou une passerelle :
- machine : le logiciel IP examine l’ adresse destination à l’ intérieur du datagramme
 - si cette adresse IP est identique à celle de la machine, IP accepte le datagramme et transmet son contenu à la couche supérieure.
 - sinon, le datagramme est rejeté; une machine recevant un datagramme destiné à une autre machine ne doit pas router le datagramme.
- passerelle : IP détermine si le datagramme est arrivé à destination et dans ce cas le délivre à la couche supérieure. Si le datagramme n’ a pas atteint sa destination finale, il est routé selon l’ algorithme de routage précédemment décrit.

Le sous-adressage

- Le sous-adressage est une extension du plan d'adressage initial
- Devant la croissance du nombre de réseaux de l'Internet, il a été introduit afin de limiter la consommation d'adresses IP qui permet également de diminuer :
 - la gestion administrative des adresses IP,
 - la taille des tables de routage des passerelles,
 - la taille des informations de routage,
 - le traitement effectué au niveau des passerelles.
- Principes
 - A l'intérieur d'une entité associée à une adresse IP de classe A, B ou C, plusieurs réseaux physiques partagent cette adresse IP.
 - On dit alors que ces réseaux physiques sont des sous-réseaux (*subnet*) du réseau d'adresse IP.

Le sous-adressage (suite)

Les sous-réseaux **128.10.1.0** et **128.10.2.0** sont notés seulement avec le **NetId**, les machines seulement avec le **Hostid** ; exemple IP(F) = **128.10.2.9**



Un site avec deux réseaux physiques utilisant le sous-adressage de manière à ce que ses deux sous-réseaux soient couverts par une seule adresse IP de classe B.
La passerelle P accepte tout le trafic destiné au réseau 128.10.0.0 et sélectionne le sous-réseau en fonction du troisième octet de l'adresse destination.

Le sous-adressage (suite)

- Le site utilise une seule adresse pour les deux réseaux physiques.
- A l'exception de P, toute passerelle de l'internet route comme s'il n'existait qu'un seul réseau.
- La passerelle doit router vers l'un ou l'autre des sous-réseaux ; le découpage du site en sous-réseaux a été effectué sur la base du troisième octet de l'adresse :
 - les adresses des machines du premier sous-réseau sont de la forme 128.10.1.X,
 - les adresses des machines du second sous-réseau sont de la forme 128.10.2.X.
- Pour sélectionner l'un ou l'autre des sous-réseaux, P examine le troisième octet de l'adresse destination : si la valeur est 1, le datagramme est routé vers réseau 128.10.1.0, si la valeur est 2, il est routé vers le réseau 128.10.2.0.

Le sous-adressage (suite)

- Conceptuellement, la partie locale dans le plan d'adressage initial est subdivisée en “partie réseau physique” + “identification de machine (hostid) sur ce sous-réseau” :

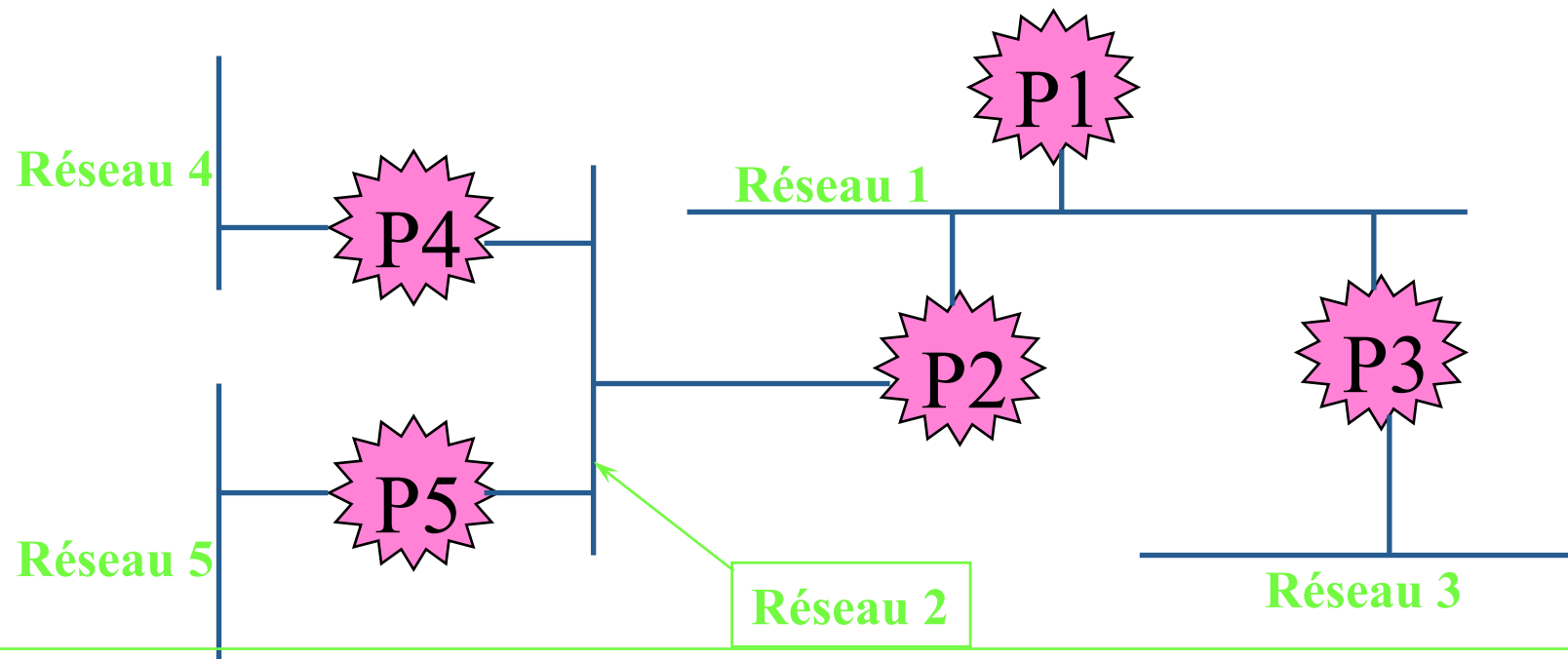


- ✦ «Partie Internet» correspond au NetId (plan d'adressage initial)
- ✦ «Partie locale» correspond au hostid (plan d'adressage initial)
- ✦ les champs «Réseau physique» et «identifieur Machine» sont de taille variable; la longueur des 2 champs étant toujours égale à la longueur de la «Partie locale».

Le sous-adressage (suite)

Structure du sous-adressage

- Structuration souple : chaque site peut définir lui-même les longueurs des champs réseau physique et identificateur de machine.
- Flexibilité indispensable pour adapter la configuration réseau d'un site:



Ce site a cinq réseaux physiques organisés en trois niveau : le découpage rudimentaire en réseau physique et adresse machine peut ne pas être optimal.

Le sous-adressage (suite)

- Le choix du découpage dépend des perspectives d'évolution du site:
 - Exemple [Classe B](#) : 8 bits pour les parties réseau et machine donnent un potentiel de 256 sous-réseaux et 254 machines par sous-réseau, tandis que
3 bits pour la partie réseau et 13 bits pour le champ machine permettent 8 réseaux de 8190 machines chacun.
 - Exemple [Classe C](#) : 4 bits pour la partie réseau et 4 bits pour le champ machine permettent 16 réseaux de 14 machines chacun.
- Lorsque le sous-adressage est ainsi défini, toutes les machines du réseau doivent s'y conformer sous peine de dysfonctionnement du routage ==> configuration rigoureuse.

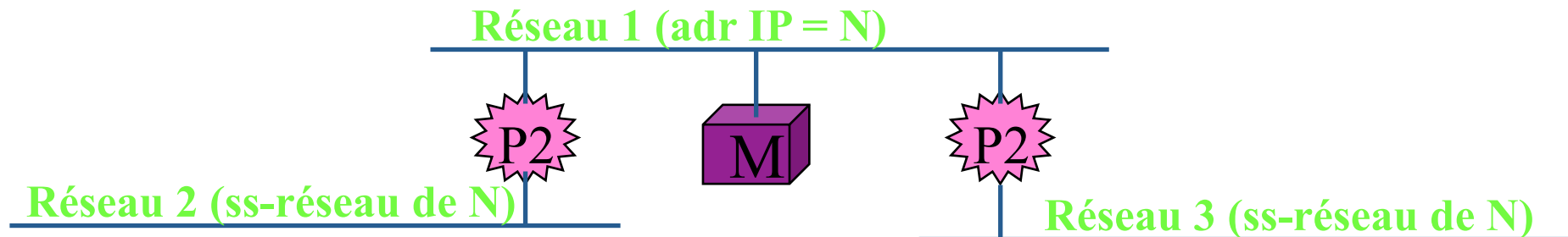
Le sous-adressage (suite)

- Utilisation de masques
- Le sous-adressage ==> masque de 32 bits associé au sous-réseau.
- Bits du masque de sous-réseau (*subnet mask*) :
 - positionnés à 1 : partie réseau,
 - positionnés à 0 : partie machine
- 11111111 11111111 11111111 00000000
==> 3 octets pour le champ réseau, 1 octet pour le champ machine
- Les bits du masque identifiant sous-réseau et machine peuvent ne pas être contigus : 11111111 11111111 00011000 01000000
- Les notations suivantes sont utilisées :
 - décimale pointée; exemple : 255.255.255.0
 - triplet : { <ident. réseau>, <ident. sous-réseau> <ident. machine> } ; cette notation renseigne les valeurs mais pas les champs de bits; exemple { -1, -1, 0 }, { 128.10, 27, -1 }.
 - adresse réseau/masque : 193.49.60.0/27 (27=# bits contigus du masque)

Le sous-adressage (suite)

Routage avec sous-réseaux

- Le routage IP initial a été étendu à l'adressage en sous-réseaux;
- l'algorithme de routage obtenu doit être présent dans les machines ayant une adresse de sous-réseau, mais également dans les autres machines et passerelles du site qui doivent acheminer les datagrammes vers ces sous-réseaux.



M doit utiliser le routage de sous-réseaux pour décider si elle route vers les passerelles P1 ou P2 bien qu'elle même soit connectée à un réseau (Réseau 1) n'ayant pas de sous-adressage

Le sous-adressage (suite)

Le routage unifié : Une entrée dans la table de routage =
(masque de sous-réseau, adresse sous-réseau, adresse de la passerelle)

Algorithme de routage unifié :

- `Route_IP_Datagram(datagram, routing_table)`
- Extraire l'adresse ID de destination du datagramme,
- Calculer l'adresse IN du réseau destination,
- Si IN correspond à une adresse réseau directement accessible
envoyer le datagramme sur le réseau physique correspondant,
- Sinon
 - Pour chaque entrée dans la table de routage,
 - $N = (ID \& \text{masque de sous-réseau de l'entrée})$
 - Si N est égal au champ adresse réseau de l'entrée
router le datagramme vers la passerelle correspondante,
 - Fin_Pour
- Si aucune entrée ne correspond, déclarer une erreur de routage.

Le sous-adressage (suite)

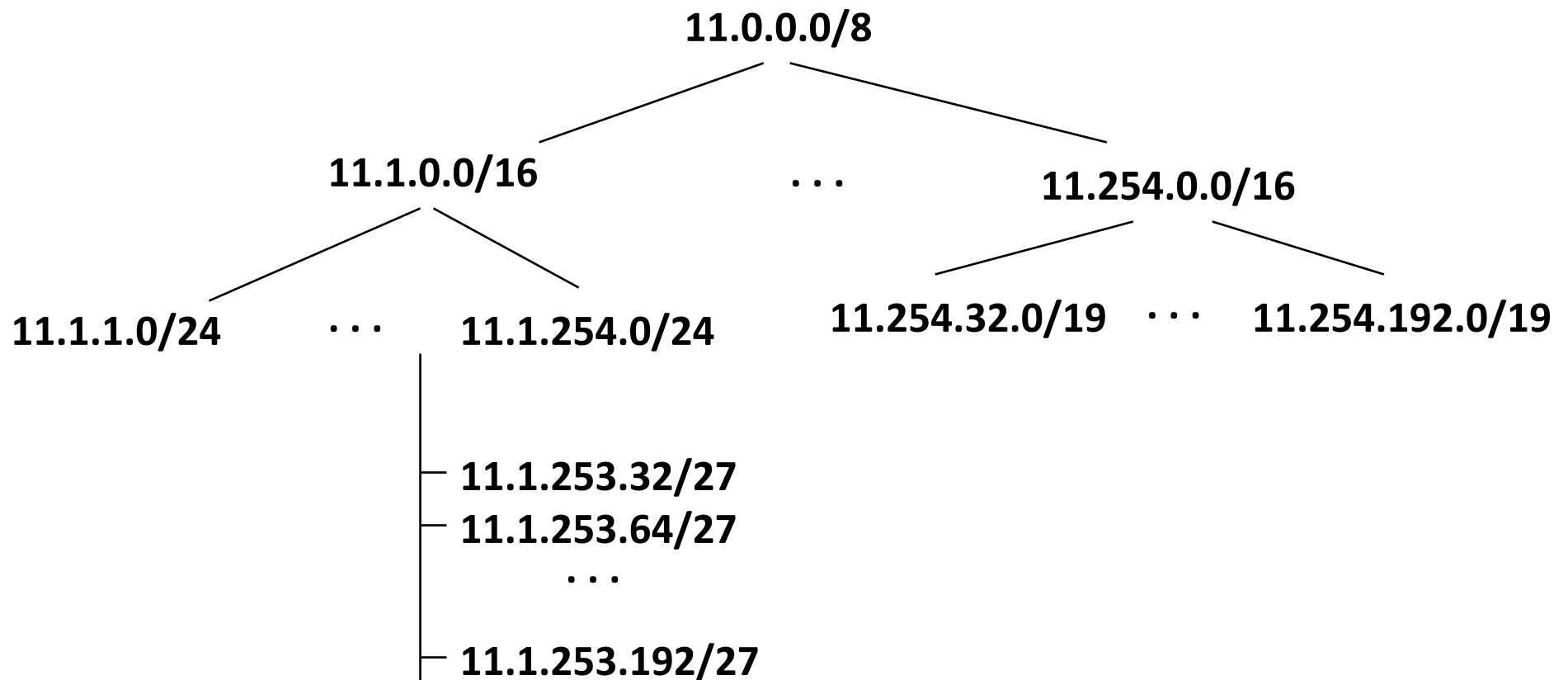
- Diffusion sur les sous-réseaux
- Elle est plus complexe que dans le plan d'adressage initial.
- Dans le plan d'adressage Internet initial, Hostid = 11..1, ==> diffusion vers toutes les machines du réseau.
- D'un point de vue extérieur à un site doté de sous-réseaux, la diffusion n'a de sens que si la passerelle qui connaît les sous-réseaux propage la diffusion à tous ses réseaux physiques : { réseau, -1, -1 }.
- Depuis un ensemble de sous-réseau, il est possible d'émettre une diffusion sur un sous-réseau particulier : { réseau, sous-réseau, -1 }.

Le sous-adressage variable (VLSM)

- RFC 1009 : un réseau IP peut posséder plusieurs masques différents; ==> réseau de type VLSM (Variable Length Subnet Masks)
- Evite la rigidité du masque fixe qui impose :
 - le nombre de sous-réseaux
 - le même nombre de machines par sous-réseau
 - Exemple : 130.5.0.0/22 ==> 64 sous-reseaux et 1022 machines / sous-réseau
 - inadapté pour des petits sous-réseaux de quelques machines; exemple 30 machines sur un sous-réseau ==> 992 adresses IP perdues
- Permet l'adaptation de l'adressage IP a la taille des sous-réseaux
 - Exemple précédent : cohabitation de grands et petits sous-réseaux
 - 130.5.0.0/22 (64 sous-reseaux et 1022 machines / sous-réseau)
 - 130.5.0.0/26 (1024 sous-réseaux de 62 machines / sous-réseau)

VLSM : agrégation de routes

- Division d'un espace IP en sous-réseaux successifs
- Permet de masquer les informations de routage entre groupes de sous-réseaux



Autre technique : CIDR