Cours de réseaux

M1 Informatique

Faculté Jean Perrin

Plan du cours

Partie 1 : Introduction

Partie 2 : Couche physique

Partie 3 : Couche liaison des données

Partie 4 : Couche Réseau / IPv4

Partie 5 : Couche Réseau / Routage

Partie 6 : Couche Réseau / IPv4, IPv6

Partie 7 : Couche transport : TCP et UDP

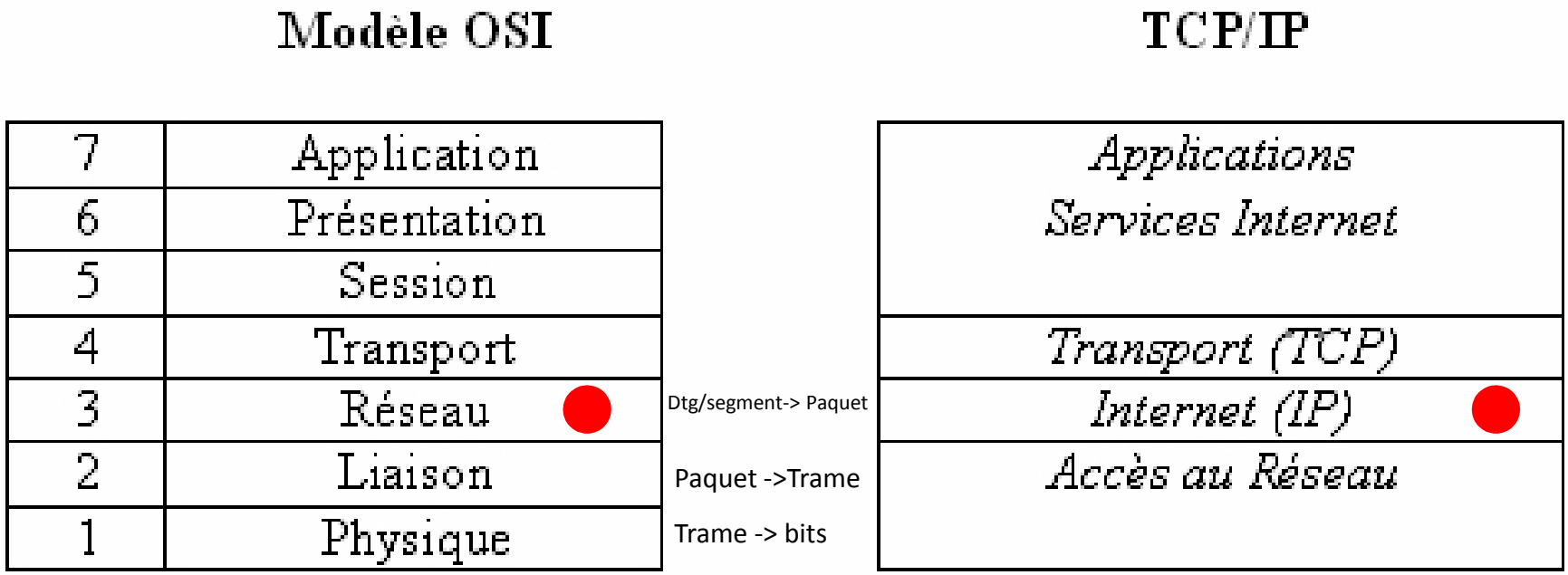
Partie 8 : Couche application

Partie 9 : Couche application / Etude de protocoles

Partie 10 : Notions d'attaques et de sécurité

Partie 4
Couche réseau / IPv4

Vous êtes ici



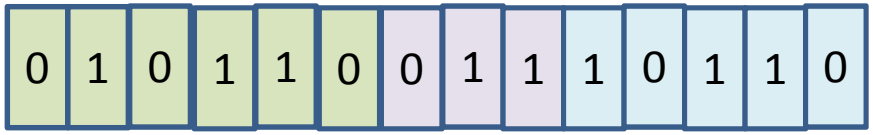
A la fin de ce chapitre…

Nous serons capables de :

- Déterminer le rôle de la couche réseau
- Comprendre le protocole de couche réseau le plus courant (**I**nternet **P**rotocol) et ses caractéristiques pour fournir un service d'acheminement « au mieux » sans connexion
- Comprendre les principes utilisés pour guider la division ou le groupements des périphériques dans le réseaux
- Comprendre l'adressage hiérarchique des périphériques
- Comprendre les notions de base relatives aux routes, aux adresses de tronçon suivant et au transfert de paquets vers un réseau de destination

Vocabulaire – PDU manipulé

Paquet : unité de données des protocoles de couche 3.



Vocabulaire – Adressage hiérarchique

Adressage hiérarchique : Schéma d'adressage dans lequel les adresses sont formées en suivant des règles de structuration spécifiques (géographique, topologique,…).

s'oppose à **adressage plat** (ou linéaire)

Adressage plat vs adressage hiérarchique

Adressage plat :

- Avantages
- Inconvénients
- Exemple
- Cas d'utilisation

Adressage hiérarchique :

- Avantages
- Inconvénients
- Exemple
- Cas d'utilisation

Adressage plat vs adressage hiérarchique

Adressage plat :

- Pas de problème d'administration
- Pas de perte de place : adresses plus courtes
- Difficile de retrouver une adresse spécifique
- Exemple : adresses MAC

→ Petits réseaux

Adressage hiérarchique :

- Doivent être administrés
- Adresses volumineuses, gaspillage d'adresses
- Localisation aisée d'un destinataire
- Exemple : Réseau Téléphonique Commuté (RTC), adresses IP

→ Grands réseaux

Où en sommes-nous ?

Question

Jusqu'à présent que savons-nous faire ?

Réponse

Envoyer un message sur un réseau local (couche 1 et 2) vers une machine spécifique de ce réseau.

Rôle de la couche réseau

Assure la connectivité de bout en bout.

Permet d'envoyer un message d'un réseau à un autre réseau en trouvant un *meilleur* chemin : **interconnexion** des réseaux.

En général, avant d'atteindre la cible on passe par un tas de réseaux intermédiaires.

Adressage local vs Adressage global

Adressage Local (couche Liaison de données)

Pour aller chez Monsieur Dupont, prendre la première à gauche, au feu tourner à droite.

Adressage global (couche réseau)

Monsieur Dupont habite en France, à Lille au 215 rue Léon Gambetta.

Comment ?

Utilisation de 3 (+1) processus de base :

Adressage : mécanisme d'identification des périphériques finaux dans l'ensemble des réseaux interconnectés : définition d'adresses uniques.

Encapsulation : création de la donnée propre à la couche réseau contenant l'adresse de la destination.

Routage : service permettant de diriger la donnée vers la destination finale en traversant d'autres réseaux.

Décapsulation : au niveau de la destination, récupération du message initial avant encapsulation.

Protocoles de couche réseau

- IPX de Novell
- Apple Talk
- CLNS (Connectionless Network Service) / DECNet
- IP version 4 (IPv4)
- IP version 6 (IPv6)

Le protocole IP

- Internet Protocol
- La version 4 (IPv4) est la version la plus répandue.
- IPv6 est la version du futur
- Conçu pour ne pas surcharger les réseaux
  - Propose uniquement un service de transfert de paquets
  - Pas de gestion de flux
  - Pas de gestion du suivi

Caractéristiques d'IPv4

Sans connexion : aucune connexion n'est établie avant l'envoi de paquets.

Non fiable : ne garantit pas la corruption, la perte, la duplication, l'ordre…

Indépendant des médias

IPv4 : Protocole sans connexion

Pas d'échange initial pour établir la connexion avant le transfert des paquets.

Pas de champ spécifique dans l'en-tête des paquets pour identifier ou maintenir la connexion

→Pas de surcharge inutile du réseau

→Gestion des problèmes (paquets manquants ou dans le désordre) laissée à la couche…

Mais au fait à quelle couche ?

IPv4 : Protocole sans connexion

Pas d'échange initial pour établir la connexion avant le transfert des paquets.

Pas de champ spécifique dans l'en-tête des paquets pour identifier ou maintenir la connexion

→Pas de surcharge inutile du réseau

→Gestion des problèmes (paquets manquants ou dans le désordre) laissée à la couche supérieure.

IPv4 : Protocole sans connexion

L'expéditeur ne sait pas :

- si le destinataire est présent
- si le paquet est arrivé
- si le destinataire peut lire le paquet

Le destinataire ne sait pas :

- Quand un paquet arrive

Analogie avec l'envoi de courrier postal

IPv4 : Protocole non fiable

Dans l'en-tête, pas de champs spécifiques contrôlant la fiabilité, pas de reçu, pas de contrôle d'erreur: c'est l'**acheminement « au mieux »**.

Impossibilité de récupérer, corriger ou retransmettre des paquets perdus ou corrompus.

La fiabilité est laissée (éventuellement) à la couche transport (TCP ou UDP)

→ adaptabilité aux besoins

IPv4 : Protocole indépendant des médias

Tout paquet IP peut être transmis sur n'importe quel type de média (via la couche de liaison)

Prise en compte de la MTU (unité de transmission maximale) de la couche de liaison pour un média donné → détermine la taille de création des paquets.

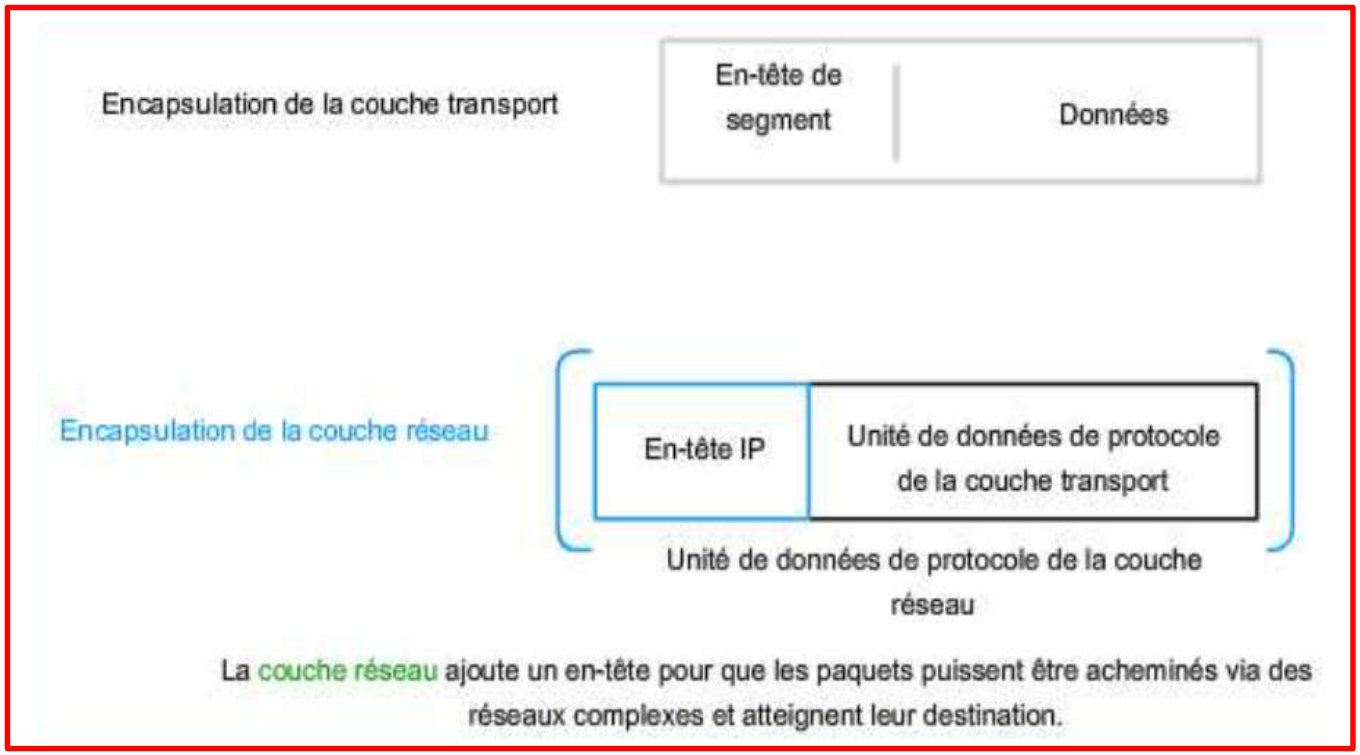
Fragmentation des données

Un paquet IP transite par de nombreux réseaux de types différents (ethernet, tokenRing, FDDI, etc) dont les caractéristiques sont différentes et le MTU aussi.

La transmission d'un paquet d'un média à un autre (via un routeur) peut entrainer la **fragmentation** du paquet si la MTU du second média est inférieure à celle du premier.

Encapsulation par IPv4 (empaquetage)

Ajout d'un en-tête aux données de la couche transport



En-tête IPv4

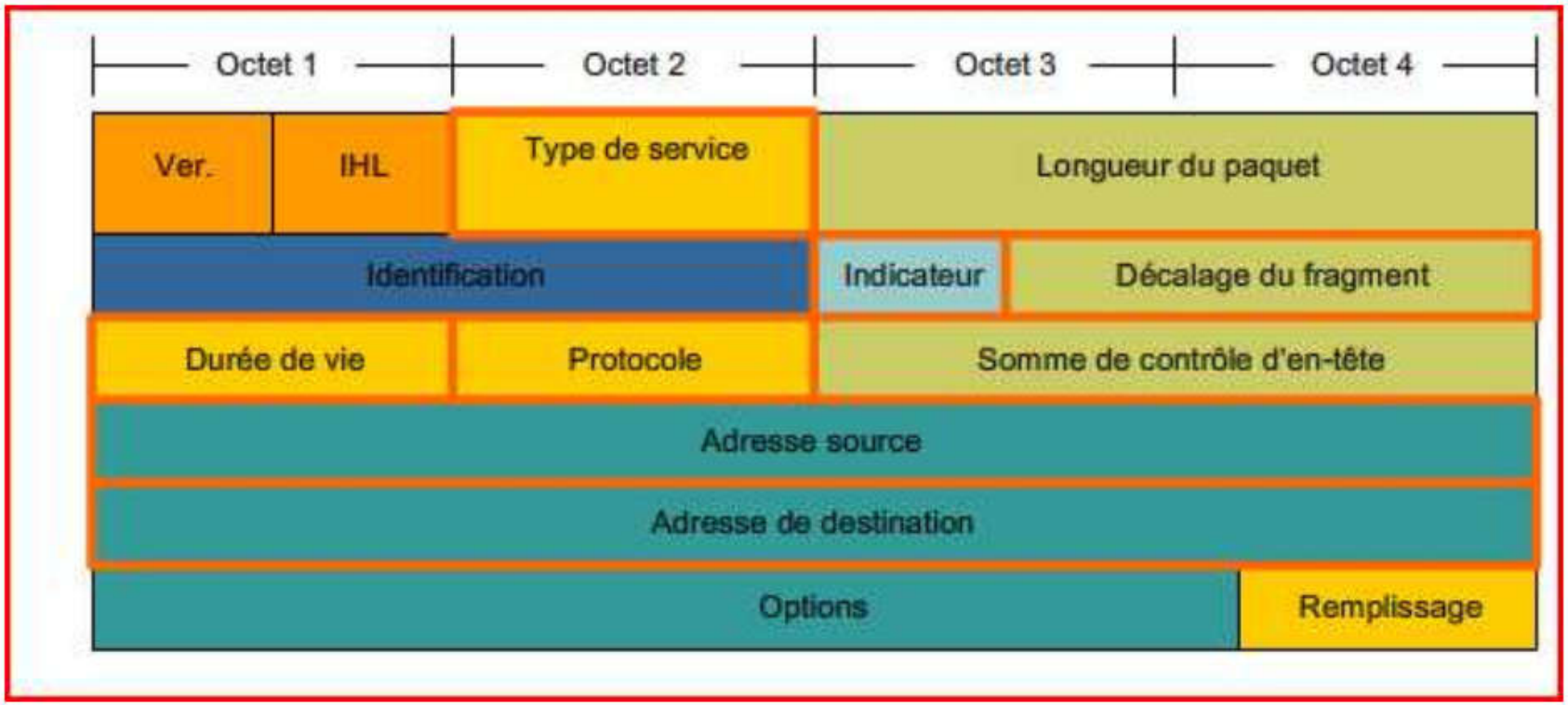
Nombreux champs contenant des valeurs binaires

On utilise souvent le terme **datagramme** pour parler d'un **paquet** dans le protocole IP.

6 champs particuliers :

- Adresse source IP
- Adresse destination IP
- Durée de vie (TTL)
- Type de service (ToS)
- Protocole
- Décalage du fragment (fragment offset)

En-tête IPv4


Octet 1
Octet 2
Octet 3
Octet 4
Ver.
IHL
Type de service
Longueur du paquet
Identification
Indicateur
Décalage du fragment
Durée de vie
Protocole
Somme de contrôle d'en-tête
Adresse source
Adresse de destination
Options
Remplissage

Les champs « adresse IP »

Chaque champ adresse contient une valeur binaire (32 bits) représentant l'adresse « couche réseau »

- du destinataire du paquet
- de l'émetteur du paquet

Champ « durée de vie »

Aussi appelé TTL : Time to live

Valeur binaire de 8 bits décrémentée de 1 à chaque saut : *i.e.* à chaque traitement par un routeur.

Pourquoi ?

Champ « durée de vie »

Aussi appelé TTL : Time to live

Valeur binaire de 8 bits décrémentée de 1 à chaque saut : *i.e.* à chaque traitement par un routeur.

Permet d'éviter que les paquets ne pouvant pas atteindre leur destination ne soient transférés indéfiniment sur le réseau : évite les **boucles de routage**

Champ « protocole »

Valeur binaire de 8 bits

Indique le type des données utiles (i.e venant de la couche transport) transportées par le paquet

Permet de transmettre de manière adaptée ces données au « bon » protocole de la couche supérieure.

Exemple : ICMP (01), TCP (06), UDP (17)

Champ « type de service »

Aussi appelé ToS : Type of Service

Valeur binaire de 8 bits

Permet de définir différentes priorités sur les paquets et ainsi définir différentes qualités de service (QoS).

Les routeurs peuvent être configurés de manière à transmettre en priorité les paquets ayant tel ou tel ToS

Exemple : Données vocales de téléphonie

Fragmentation : champ « **fragment offset**»

Valeur binaire de 16 bits

Utilisé lorsqu'un routeur fragmente le paquet

Indique le numéro d'ordre du fragment pour la reconstruction du paquet

Utilisation d'un flag **MF** (**m**ore **f**ragment) qui indique si d'autres fragments vont suivre.

Fragmentation

L'utilisation des champs « fragment offset» et « more fragment » est-elle suffisante pour la gestion de la fragmentation ?

Réponse : NON

Fragmentation : champs numéro d'identification

Il faut également être capable d'identifier les fragments provenant d'un même paquet.

C'est le rôle du champ « numéro d'identification » sur 2 octets.

Fragmentation

Question : Qui réassemble les fragments pour reconstituer le paquet initial ?

Réponse : c'est toujours la station de destination (finale)

Fragmentation : Flag « DF »

Indicateur sur 1 bit

Indique que le paquet ne doit pas être fragmenté (**D**on't **f**ragment)

Si un routeur ne peut transmettre un tel paquet (DF=1) sans le fragmenter, il est rejeté.

Autres champs

- **Version** : numéro de version de IP (IPv **4)**
- **IHL** (Internet Header Length) : longueur de l'en-tête (4 bits)
- **Longueur** : longueur totale du paquet (incluant l' en-tête) donnée en octets
- **Somme de contrôle d'en-tête** : vérifie l'absence d'erreurs dans l'en-tête

Séparation des hôtes en groupes communs

Constat :

A mesure que le nombre d'hôtes augmente, la gestion et l'adressage du réseau devient de plus en plus difficile.

Solution :

Regrouper les hôtes en réseaux plus petits (sous-réseaux) en fonction de différents critères.

Séparation des hôtes en groupes communs

Facteurs de regroupement possibles

- Emplacement géographique
- Objectif
- Propriété

Regroupement géographique

Création des sous-réseaux en fonction des emplacements géographiques.

Exemples :

- Les différents bâtiments d'un campus
- Les différents étages d'un bâtiment

Regroupement par objectifs spécifiques

Les hôtes ayant des tâches similaires sont regroupés sur le même sous-réseaux.

Permet de mettre à dispositions des ressources communes, des outils, des logiciels de manière plus efficace -> réduction du trafic

Regroupement par propriété

Les sous-réseaux sont créés en fonction de l'organisation (ex. services, filiales,…)

Permet de mieux gérer les frontières pour la gestion des sous-réseaux et la mise en place de la sécurité.

Avantages liés au regroupement

Amélioration des performances

Gestion efficace de la sécurité

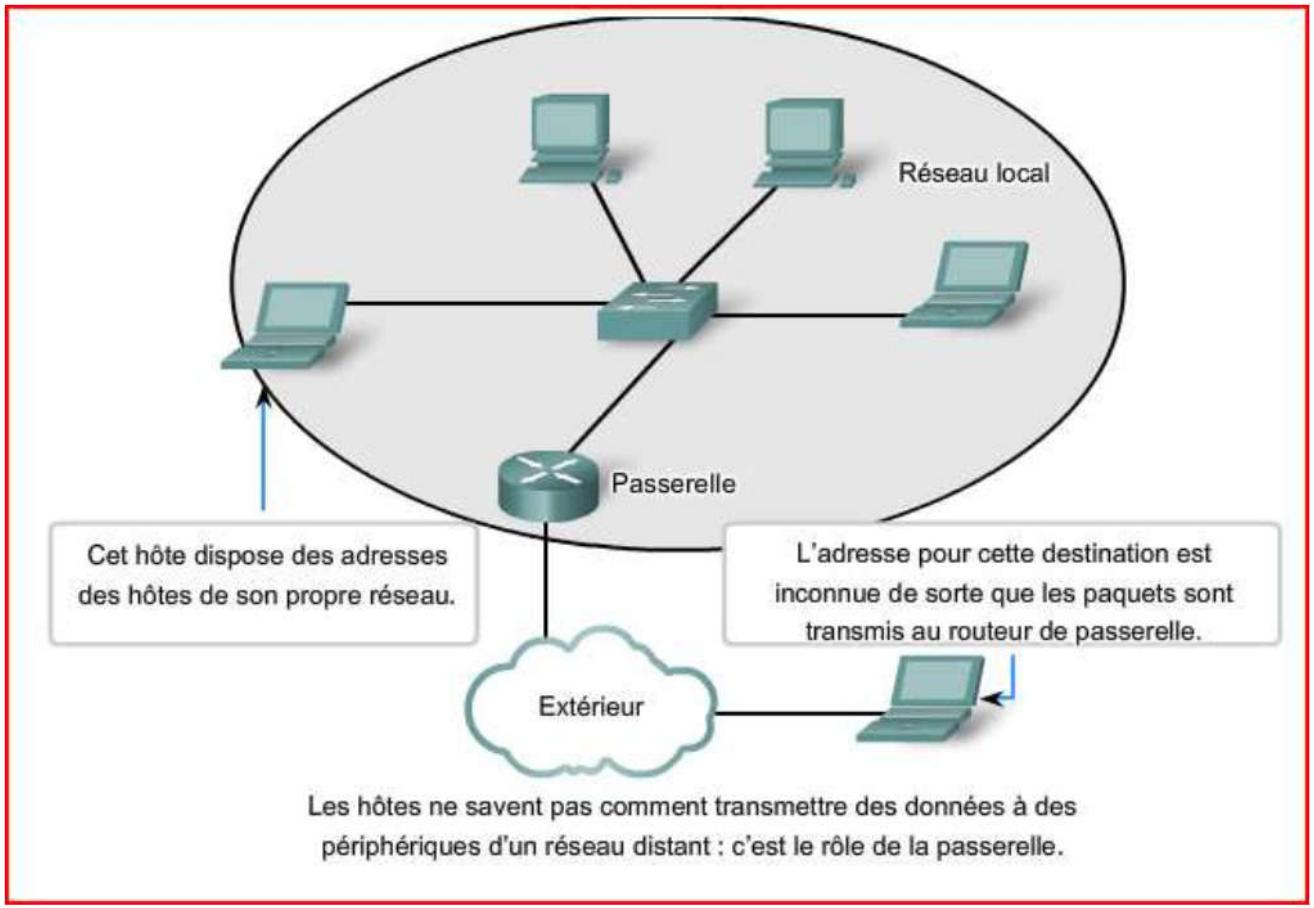
Gestion des adresses

Principe de gestion des adresses

Lorsqu'une station a besoin de communiquer avec un hôte n'appartenant pas à son (sous-) réseau -> il lui suffit de connaitre l'adresse d'un périphérique intermédiaire (**passerelle**).

La **passerelle** est un **routeur** sur un réseau servant de sortie de ce réseau.

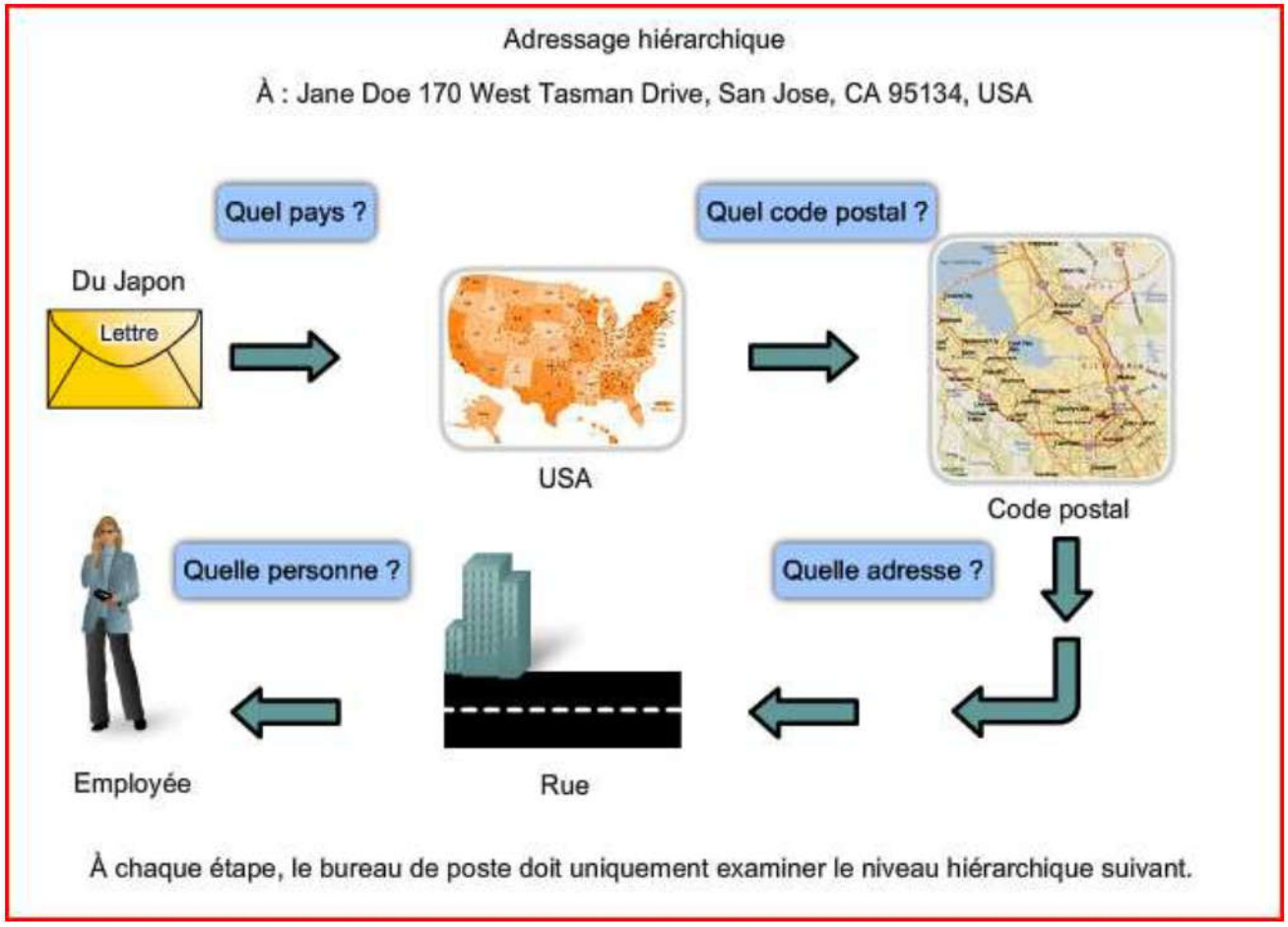
Principe de gestion des adresses



Principe de gestion des adresses

Pour prendre en charge les communications entre les différents réseaux, le système d'adressage de couche réseau est **hiérarchique**.

Exemple d'adressage hiérarchique



Principe de gestion des adresses

Les routeurs acheminent les paquets entre les réseaux en se référant uniquement à la partie de l'adresse de couche réseau requise pour diriger le paquet vers le réseau de destination.

Une fois le paquet arrivé sur le réseau de l'hôte de destination, l'intégralité de son adresse de destination aura été utilisée.

Les adresses IPv4

Présentation des adresses IPv4

Adresses mondiales logiques

Codées sur 32 bits (4 octets)

Constituées de deux parties

- Identification du réseau
- Identification de l'hôte sur ce réseau

Attribution des adresses

Identifiant unique mais en nombre limité (environ 4 milliards)

Numéros IP attribués par l'ICANN (Internet Corporation for Assigned Names and Number)

Gestion pratique déléguée à divers organismes et sociétés privées

- AFNIC
- RENATER
- RIPE

Représentation d'une adresse IP

Les 4 octets constituant l'adresse sont donnés en valeurs décimales séparées par un point.

11000000 10101000 00011001 10000100

192 . 168 . 25 . 132

Partie réseau / partie hôte

Remarque préliminaire : tous les hôtes d'un même réseau ont la même partie réseau.

La séparation de l'adresse en deux sous-adresse (réseau et hôte) se fait selon un **masque**.

Le masque est constitué de 4 octets (32 bits) dont les bits à 1 identifient la partie réseau de l'adresse et les bits à 0 la partie hôte.

Utilisation du masque

Adresse IP : 192.168.25.132

11000000.10101000.00011001.10000100

Masque : 255.255.255.0

11111111.11111111.11111111.00000000

192.168.25.132 : réseau.hôte

Utilisation du masque

On aurait pu choisir comme masque :

11111111.00000000.11111111.11111111

ou encore

11100111.11001111.11110011.11111100

Mais très peu pratique !

Utilisation du masque

Le choix de conserver la contiguïté des bits entraîne qu'un nombre limité d'octets peut apparaître en tant que constituant de masque.

11111111, 11111110,11111100,…00000000

Soit en décimal :

255,254,252,248,240,224,192,128,0

Cela permet de déterminer facilement et rapidement la validité d'un masque

255.255.224.0 : Ok

255.255.232.0 : Nok (car 232 -> 11101000)

Longueur de préfixe

Il s'agit d'une autre écriture du masque.

Détermine simplement le nombre de bits utilisés pour définir la partie réseau.

10.0.0.0/255.0.0.0 équivaut à 10.0.0.0/8

192.168.25.32/255.255.255.248 équivaut à

192.168.25.32/29

Dernière remarque….

Le choix du masque détermine le nombre d'hôtes qui pourront prendre place dans ce réseau.

Il faut donc bien le choisir !

Classes d'adresses

Historiquement, ces classes permettaient de définir des catégories de sous-réseaux en fonction de leur taille et en leur associant des plages d'adresses.

Trois classes principales : A B C

Plus 2 : D et E

Classes d'adresses

Classe A

Premier bit de l'adresse à 0

Masque de sous-réseau en 255.0.0.0.

Soit plus de 16 000 000 d'hôtes possibles.

Réservée aux très grands réseaux (administrations et grandes entreprises)

126 réseaux de ce type

Classes d'adresses

Classe B

Deux premiers bits de l'adresse à 10

Masque de sous-réseau en 255.255.0.0.

Soit plus de 65 000 d'hôtes possibles.

Environ 16000 réseaux de ce type

Classes d'adresses

Classe C

Trois premiers bits de l'adresse à 110

Masque de sous-réseau en 255.255.255.0

Soit **254** hôtes possibles par réseau

Réseaux de petites tailles

Environ 2 000 000 réseaux de ce type

Classes d'adresses

Classe C

Au fait ? Pourquoi seulement 254 hôtes possibles puisque sur 1 octet complet on peut coder 255 valeurs (en plus de 0)?

L'adresse 255.255.255.255 est destinée au broadcast.

Classes d'adresses

Classe D

Quatre premiers bits de l'adresse à 1110

Masque de sous-réseau en 255.255.255.240

Expérimental

Réservé au multicast

Classes d'adresses

Classe E

Quatre premiers bits de l'adresse à 1111

Masque de sous-réseau en 255.255.255.240

Expérimental

Classes d'adresses

Ce système gâchait beaucoup d'adresses.

Exemple : une entreprise demandant 80 000 adresses -> classe A (16 697 214 inutilisées)

Système abandonné fin des années 90 et remplacé par l'adressage CIDR.

L'homme du jour

Vint Cerf, né le 23 juin 1943 dans le Connecticut. Ingénieur, chercheur et inventeur américain. Il est co-inventeur avec Bob Kahn du protocole TCP/IP et considéré comme l'un des pères fondateurs d'internet.

Il reçut le Prix Turing en 2004.

Matériel concerné par la couche

Passerelle (gateway) : équipement d'un réseau reliant deux réseaux de types différents. Plus couramment, ce terme désigne le routeur particulier entre un réseau local et le réseau internet.

Routeur : équipement réseau permettant l'interconnexion de réseaux et assurant le routage des paquets (couche 3) en déterminant le chemin qu'ils vont devoir suivre.

Matériel concerné par la couche

Passerelle (gateway) :

Routeur :

Conclusion

La couche réseau permet de définir le mode d'adressage de tous les hôtes sur un réseau global.

Elle définit également les protocoles de routage permettant de transmettre de proche en proche les paquets.

Le protocole le plus important et le plus utilisé est le protocole IP (Internet Protocol).

Encore quelques mots….

Qu’est-ce qu’une IP publique ? (IP Wan)

Qu’est-ce qu’une IP locale ou privée ? (IP Lan)

192.168.0.x

Une IP Statique/ IP Dynamique