heig-vd

Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

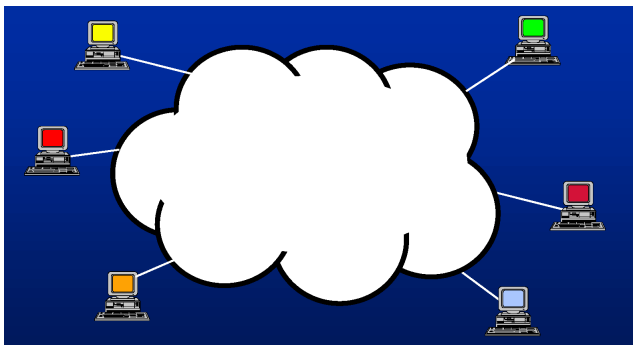
Chapitre VI

La couche réseau

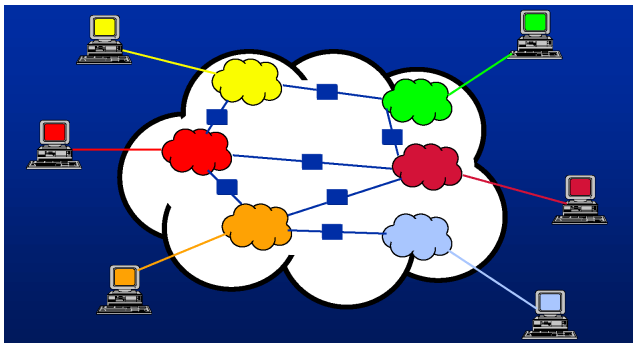
Historique de l'Internet

- Né 1969 comme projet (D)ARPA
  - (Defense) Advanced Research Projects Agency; US
    - Commutation de paquets
    - Interconnexion des universités participant aux projets ARPA
    - Premier réseau: 4 ordinateurs
- 1972: ARPNET (centaine d'ordinateurs)
  - IMP (Interface Message Processor), similaire à X.25
  - NCP (Network Control Program), ancêtre de TCP
- 1974: Début de la spécification de TCP et IP
  - Interconnexion de réseaux hétérogènes: « Internet »
  - Fonctionnement robuste et grande tolérance aux pannes
- 1983: TCP remplace NCP dans ARPANET
- 1984: Division d'ARPANET en ARPANET et MILNET
- 1988: Nouveau réseau Backbone: NSFNET
- 1995: Arrêt du Backbone NSFNET

Architecture de l'Internet



Architecture de l'Internet



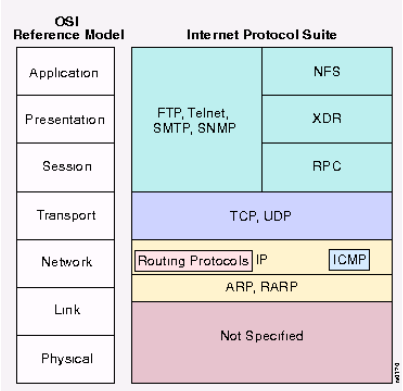
- Réseaux backbones commerciaux
- Les ISP se connectent aux backbones à des points d'interconnexion (IXPs)
- Les entreprises connectent leurs réseaux aux ISP
- Les routeurs gèrent l'acheminement et le routage entre les réseaux

Terminologie

- Internet :
  - LE réseau mondial
- Un internet :
  - Un ensemble de réseau (locaux) interconnectés à l'aide du protocole IP
- Host, système terminal, end-system:
  - Ordinateur connecté à un réseau (client, serveur)
- Routeur, système intermédiaire
  - Équipement capable d'acheminer des datagrammes IP
  - Possède plusieurs (normalement peu d') interfaces réseau
  - Travaille à la couche « réseau » de la hiérarchie TCP/IP
  - Ancien terme : Gateway
- Gateway, passerelle
  - Système intermédiaire effectuant la traduction de protocoles

Modèle TCP/IP en couches

- ARP, RARP:
  - Traduction d'adresses MAC ⇔ IP
- ICMP :
  - Signalisation de problèmes entre routeurs
- Protocoles de routage (OSPF, RIP, BGP)
- **IP**
  - **Acheminement de datagrammes**
  - **Adressage**
  - **Fragmentation et réassemblage**
- Couche transport
  - Orienté connexion, fiable --> TCP
  - Sans connexion --> UDP
- Applications
  - Implémentent généralement plusieurs couches

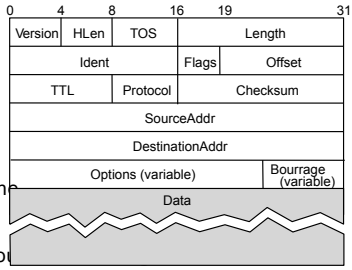


Le protocole IP

- Défini dans la RFC 791
- Objectifs de la conception
  - Doit être utilisable sur toute les technologies sous-jacentes --> Protocole de convergence
- Modèle de service
  - Sans connexion
    - Un datagrammes contient toute l'information pour l'acheminer
  - Service non-fiable: « **best effort** »
    - IP essaie le mieux de délivrer les paquets mais ne peut pas le garantir
      - Des datagrammes peuvent être perdus
      - Des datagrammes peuvent arriver dans le désordre
      - Les datagrammes peuvent être dupliqués
      - Le datagrammes peuvent être retardés

Format des datagrammes IP

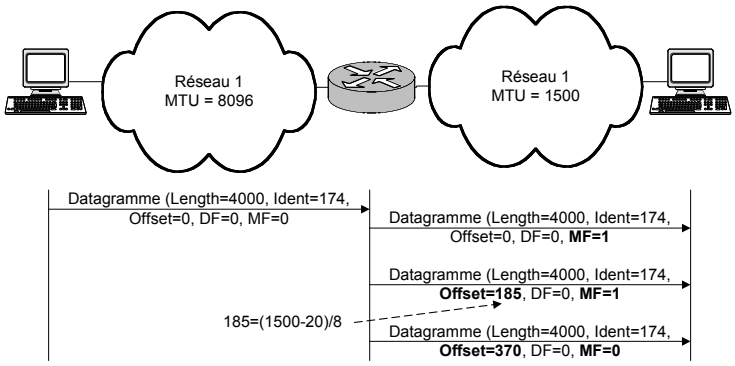
- Longueur: 20 octets – 60 octets
  1. Version : IPv4
  2. HLen: Longueur de l'en-tête
  3. TOS: Type of Service
     - Définition originale jamais utilisée
     - Base des Services Différenciés
  4. Longueur du datagramme (avec l'entête)
     - 16 bit --> longueur max. 65535 octets
     - Nécessite la fragmentation en plusieurs trame
       - Entêtes Ident, Flags, Offset
  5. TTL: Time to live
     - Permet de capturer des paquets dans des bou
  6. Protocole
     - Désigne le protocole de la couche transport (normalement TCP ou UDP)
  7. Somme de contrôle
     - Protège l'en-tête IP, non pas les données
     - Calcul simple (différent de CRC) et protection moins forte
  8. Adresses source et destination : adresses des systèmes terminaux
  9. Options (p.ex. sécurité, options de routage) : Rarement utilisées



Fragmentation et réassemblage

- Problème
  - Les différentes technologies sous-jacentes ont des tailles de trames différentes
    - MTU : Maximum Transfer Unit
  - La source ne connaît pas le chemin emprunté par le datagramme
- Une source/un routeur fragmente un datagrammes si
  MTU de l'interface < taille du datagramme
- Chaque fragment est un datagramme complet
- Le destinataire doit réassembler les fragments
  - Les fragments peuvent arriver dans le désordre
  - Si un fragment est perdu, le datagramme sera supprimé
    - Aucune retransmission de fragments au niveau IP

Exemple de la fragmentation

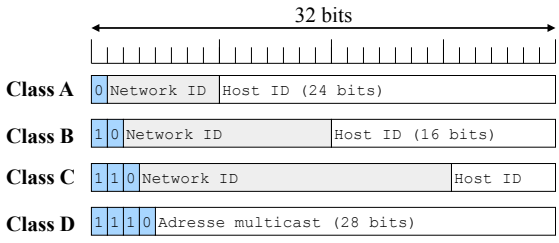


- Ident: identificateur unique de datagramme
- Offset: en multiples de 8 octets
- DF: Don't Fragment bit (utilisé par la source)
- MF: More Fragments (indique le dernier fragment)

Exercices 1 et 2

Adresses IP

- Chaque interface réseau a une adresse IP unique
- Longueur: 4 octets (p.ex. 193.10.4.3)
- Contient deux parties
  1. Identificateur de réseau (Network ID)
     - Assignée par une autorité (p.ex. ISP)
  2. Identificateur de machine (Host ID)



1-126, 126 réseaux, 16 mio de hôtes

128-191, 16k réseaux, 65k de hôtes

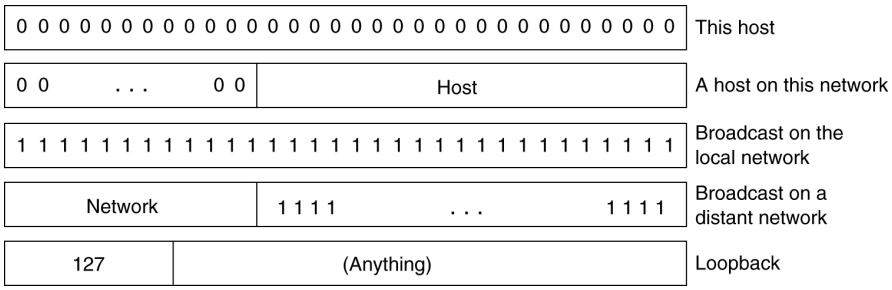
192-223, 2 mio réseaux, 254 hôtes

224-239, sans structure

Adresses particulières

- Class E: 240-254
  - Réservées pour l'avenir

Autres adresses particulières

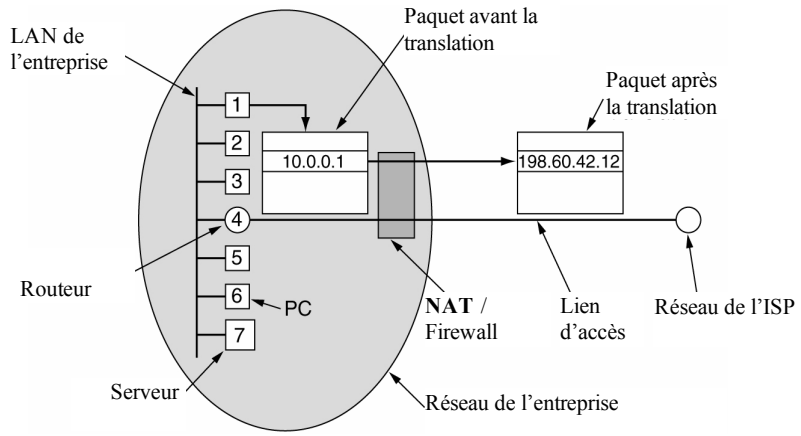


Adressage privé

- Problème: manque d'adresses IP
- Idée
  - Réutilisation des adresses IP
    - Une organisation utilise des adresses privées à l'intérieur du réseau
    - Pour la communication avec l'extérieur, une adresse publique est assignée de manière temporaire
- Adresses privées
  - 10.0.0.0 – 10.255.255.255 (1 réseau classe A)
  - 172.16.0.0 – 172.31.255.255 (16 réseaux classe B)
  - 192.168.0.0 – 192.168.255.255 (256 réseaux classe C)

Exercices 3, 8, 9, 10

NAT
Traduction d'adresses privées

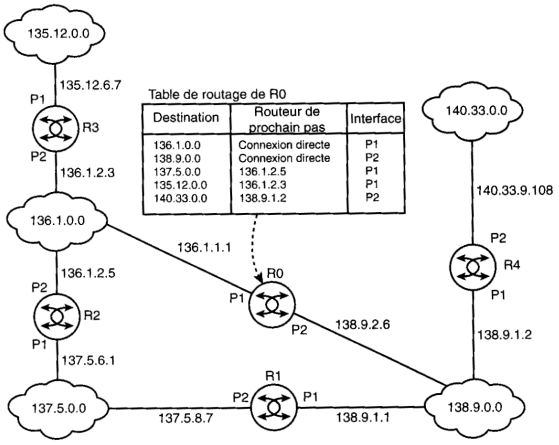


Acheminement des datagrammes

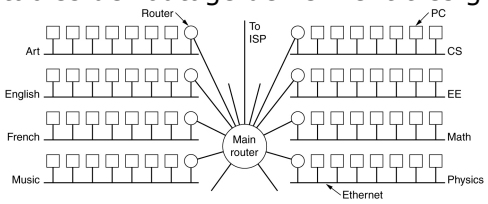
Comment un routeur achemine-t-il un datagramme ?

- Chaque datagramme contient l'adresse de la destination
- Le routeur a une table de routage qui contient des entrées:
  - Destination, Adresse Next Hop, Interface de sortie
- Le routeur cherche dans sa table l'entre pour le Network ID des adresses de destination
- Aucune entrée trouvé
  - Utiliser la route par défaut, s'il y en a
  - Sinon, écarter le datagramme avec une erreur « Non routable »

Table de routage



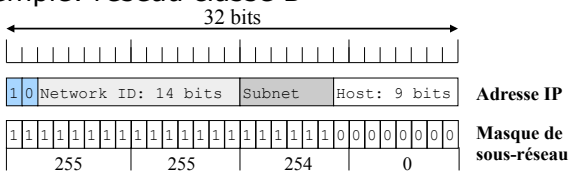
Sous-réseaux

- Dans un réseau important, le nombre de hôtes du réseau pose des problèmes
  - Assignation des adresses IP aux hôtes doit être centralisée
  - Les tables de routage deviennent très grandes
  - 

  - Solution: introduction d'un troisième niveau d'adressage

Sous-réseaux (suite)

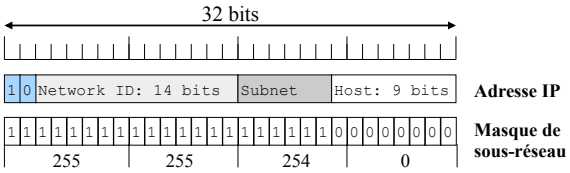
- Principe
  - Création de plusieurs plages d'adressages à l'intérieur d'un réseau
- Adressage à trois niveaux
  - Exemple: réseau classe B



  - Sous-division du réseau classe B en 128 sous-réseaux
    - Chaque sous-réseau comprend jusqu'à 2^9 = 512 stations

Sous-réseaux (suite)

- Adresse de sous-réseau
  - Partie « Host » remplie de 0
- Adresse de diffusion limitée
  - Partie « Host » remplie de 1
- Notation
  - 255.255.255.0 ou /24
- Adresse IP & Masque = Adresse réseau

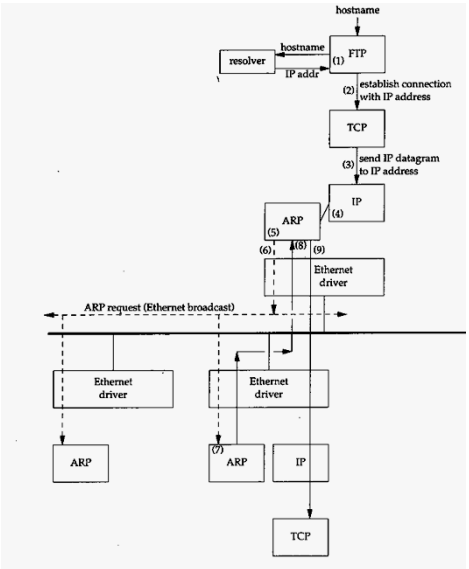


Exercices 11, 14, 15, 17, 18, 19, 20, 22, 24, Siyan p.368-369

ARP:
Résolution d'adresses IP

- **Traduit entre les adresses IP et les adresses physiques**
  - Machine de destination
  - Prochain routeur sur le chemin
- **ARP**
  - A un cache avec les correspondances: adresse IP, adresse physique (ou adresse MAC)
  - Requête en diffusion si l'adresse IP n'est pas dans la table
  - La machine concernée répond avec son adresse physique
  - Les entrées du cache sont éliminées si elles ne sont pas rafraîchies (toutes les 20 min)

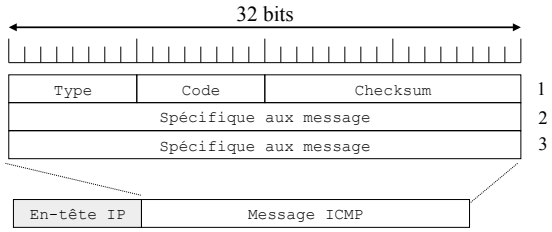
Exemple ARP



Doublons d'adresses IP

ICMP
Internet Control Message Protocol

- Permet de communiquer des problèmes
  - Envoyé par le routeur à la source
- Permet d'effectuer des diagnostiques
  - Envoyer par un utilisateur à un équipement
- Format:



Types de messages ICMP

Type	Message	Description
3	Destination Unreachable	Problème de routage
5	Redirect	Le routeur indique à la source qu'il y a un meilleur chemin
4	Source quench	La routeur signal une congestion au hôte (rarement utilisé)
11	Time exceeded	TTL d'un datagramme est arrivé à 0
0 et 8	Echo request et reply	Ping

- Ping: vérifier la connectivité et le bon fonctionnement d'un système
  - Exemple

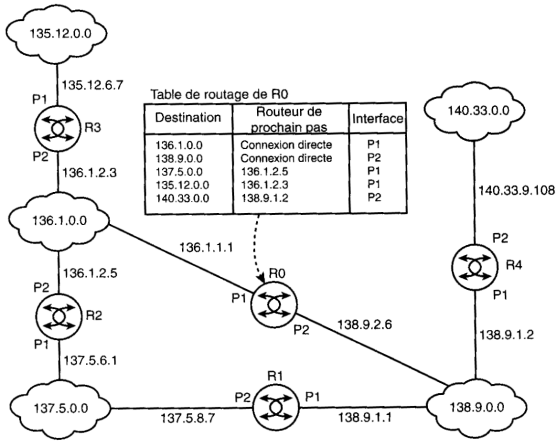
```
ping www.google.ch
PING www.google.ch (192.32.43.12): 56 data bytes
64 bytes from 192.32.43.12: icmp_seq=0 ttl=255 time=12.3 ms
64 bytes from 192.32.43.12: icmp_seq=1 ttl=255 time=20.1 ms
```

  - Variante: ping –r station
    - Affiche le chemin vers la station (jusqu'à 9 sauts)
    - Utilise l'option IP d'enregistrer le chemin parcouru dans l'en-tête IP

Principe du routage

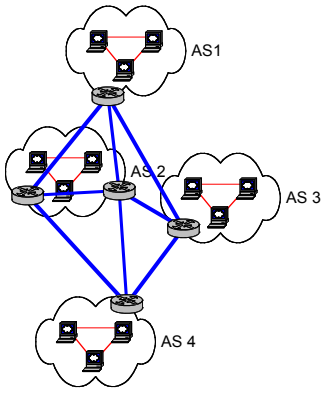
- La fonction principale de la couche réseau est l'acheminement des datagrammes
  - Les routeurs utilisent des tables de routage pour déterminer le prochain saut
  - L'information dans les tables de routage vient
    - De protocoles de routage chargés de trouver des chemins 'optimaux'
    - D'un configuration statique par l'administrateur
- IP
  - *Forwarding* de datagramme sur la base de tables de routage
- Protocoles de routage
  - Déterminer les chemins optimaux et créer les tables de routage

Table de routage



Niveaux de routage

- L'Internet a une structure hiérarchique
  - Interconnexion de réseaux
    - Les réseaux sont administrés par des organisations distinctes
  - Un ou plusieurs réseaux regroupés forment un Système Autonome (AS)
- Deux types de routage
  - Routage à **l'intérieur** d'un AS
    - Interior Gateway Protocol (IGP)
      - Cherche des routes optimales
      - RIP, OSPF
  - Routage **entre** les AS
    - Exterior Gateway Protocol (EGP)
      - Utilisation de règles qui limitent les routes
      - BGP



Algorithmes de routage

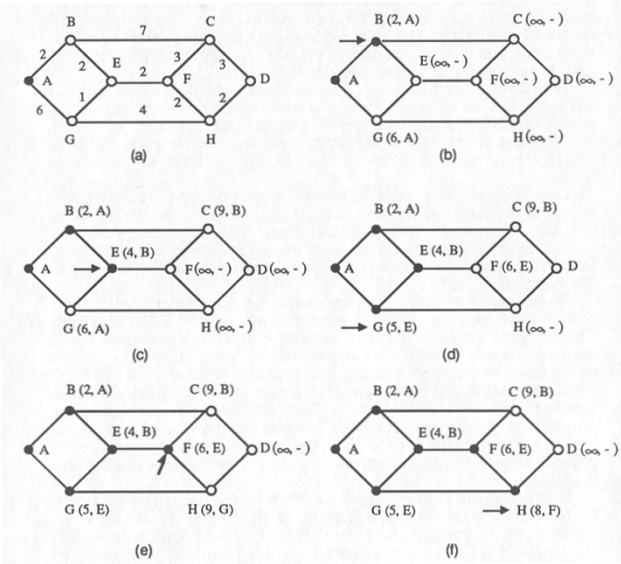
Problème
- Trouver la « *meilleur route* » vers une destination
- Métriques
  - Nombre de sauts, capacités de liens, trafic, délai

- Inondation *(flooding)*
  - Similaire au routage par la source dans Token Ring
- Chemin le plus court
  - Statique : topologie et métriques fixes
  - Dynamique : adaptation aux changements de la topologie
    - Vecteur de distance - connaissance locale des métriques
      - RIP, (IGRP)
    - État de liaison - connaissance globale des métriques
      - OSPF, (PNNI)

Le plus court chemin

- Algorithme de Dijkstra
  - Représenter le réseau par un graphe
  - Pondérer chaque arête k par un coût p_k
  0. Marquer chaque nœud par un doublet (C_i,N_x)
     - C_i : Distance totale de la source
     - N_x : Nœud précédent (pour reconstruir le chemin)
  1. Doublet de chaque nœud initialisé à $(\infty,-)$
     à l 'exception du nœud d 'origine initialisé à (0,-)
  2. Choisir le nœud N_i avec le coût C_i le plus bas et qui n'est pas marqué et le marquer comme 'permanent'
  3. Calculer les coûts des chemins de tous les voisins N_j du nœud N_i : $C_j=C_i+p_k$
  4. Si la nouvelle valeur C_j est plus petite que l'ancienne,
     --> actualiser le doublet de N_j : (C_j,N_i)
  5. Répéter à partir de 2 jusqu'à ce que la destination soit marquée 'permanent'

Exemple



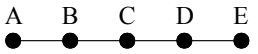
Vecteur de distance

- Chaque routeur maintient une table de routage
  - Pour toutes les destinations : Destination, Nœud suivant, Distance
    - Distance: Nombre de sauts, délai, …
    - Distance peut être infinie si aucune route n'est connue
- Le routeur connaît la distance qui le sépare de ses voisins directs
- Les mises à jour (*updates*) se font directement entre voisins
  - Les voisins échangent les routes connues
  - Périodiquement ou quand la table change (appelé "*triggered update*")
- Algorithme de Bellman-Ford distribué
  - Le routeur X connaît la distance d(X,Y) vers ses voisins Y
  - Initialement, la distance D(X,n) vers la destination *n* est
    - D(X,n) = 0, si X est directement connecté au réseau n
    - D(X,n) = ∞ pour toutes les autres destinations
  - Le routeur X reçoit le vecteur des distances {D(Y,n)} du voisin Y vers tous les *n*
  - Le routeur X calcule la meilleure distance vers la destination n

$$D(X,n) = \min_{\text{voisins Y}} \left(d(X,Y) + D(Y,n) \right)$$

Propagation des bonnes nouvelles

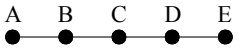
- Une meilleure route se propage rapidement
- Exemple simple :
  - Réseau linéaire
  - Distance: nombre de sauts
  - Nœud A vient de démarrer



∞	∞	∞	∞	État initial
1	∞	∞	∞	Après 1 échange
1	2	∞	∞	Après 2 échanges
1	2	3	∞	Après 3 échanges
1	2	3	4	Après 4 échanges

Propagation de mauvaises nouvelles

- Après une panne, le routage converge très lentement
- Exemple :
  - Lien entre A et B tombe en panne

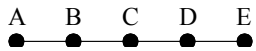


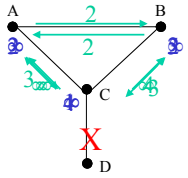
1	2	3	4	État initial
3	2	3	4	Après 1 échange
3	4	3	4	Après 2 échanges
5	4	5	4	Après 3 échanges
6	5	6	5	Après 4 échanges
7	6	7	6	Après 5 échanges
…	…	…	…	
∞	∞	∞	∞	Après n échanges

  - ➢ Problème de la valeur infinie

Solutions pour accélérer la convergence

- Définir une distance maximale *n*
  - Tout au-delà de *n* est infini
  - Limite la taille maximale d'un réseau
- Horizon éclaté (*Split horizon*)
  - La distance vers une destination n'est pas annoncée au nœud suivant dans cette direction
    - Exemple
      - C annonce à D une distance D(C,A) = 2
      - C annonce à B une distance D(C,A) = ∞
  - Ne fonctionne pas toujours
    - Exemple:
      - Distance vers D
      - Lien C – D tombe en panne





Exercices 25, 26, 27, 31, 33, 34, 37

Le protocole RIP

- RIP : *Routing Information Protocol*
  - Protocole de routage par vecteur de distance
  - Métrique: nombre de sauts
    - Valeur 'infinie' : 16 sauts
    - Utilise l'horizon éclaté
- Encore utilisé dans de petits réseaux
  - Facile à configurer
- Version améliorée: RIP2

Routage par état de liaison

- Le routage par vecteur de distance fut utilisé dans l'ARPANET jusqu'en 1979
  - Métrique originale : longueur des files d'attente
    - Idée: chemin avec un délai de transfert minimal
    - Applicable si toutes les lignes ont le même débit
  - Problèmes :
    - Évolution vers des interconnexions hétérogènes
    - Convergence trop lente dans un réseau important
- ➢ Introduction du routage par état de lien (*link state routing*) dans ARPANET

État de lien : principe

- Chaque routeur doit périodiquement effectuer les opérations suivantes:
  1. Découvrir ses voisins et apprendre leur adresse respective
  2. Déterminer la distance vers chacun des voisins
  3. Construire un paquet contentant l'information apprise
  4. Envoyer ce paquet spécial à tous les autres routeurs du sous-réseau
  5. Calculer le plus court chemin vers tous les autres routeurs
- Un routeur apprend alors la topologie complète du réseau
- Calculer le plus court chemin

Découvrir ses voisins

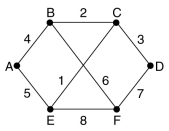
- Un routeur envoie périodiquement des messages Hello sur toutes les lignes de sortie
  - Un routeur voisiné répond avec
    - son nom,
    - son adresse IP, …
  - Ainsi, un routeur détecte rapidement l'état des liens de sortie (up, down)

Déterminer la métrique des liens

- Un protocole d'état de liens peut se baser sur plusieurs métrique pour le calcul du plus court chemin
  - Exemples :
    - délai,
    - throughput,
    - fiabilité de transmission
- Les métriques peuvent être mesurées à l'aide de paquets de test

Diffusion de l'information

- Chaque routeur construit des paquets contentant l'information sur l'état des liens locaux (LSP: *link state packet*)



Link State Packets						
A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

- Les LSP d'un routeur sont diffusés dans le réseau entier
  - Inondation fiable
    - Un routeur transmet un LSP reçu sur tous les ports sauf le port de réception
    - Un numéro de séquence unique permet d'éliminer des LSP dupliqués
      - Un routeur incrémente le no. de séquence pour chaque LSP émis
    - Les autres routeurs enregistrent le LSP le plus récent de chaque nœud
    - Éliminer les LSP quand sa durée de vie est terminée
    - La réception d'un LSP est confirmé par un accusé de réception

Calcul du plus court chemin

- Un routeur apprend l'état des liens du réseau entier
- Le calcul du plus court chemin peut être effectué en local
  - Aucune dépendance du calcul d'autres routeurs
  - Convergence rapide et garantie
- Méthodes de calcul : p.ex. algorithme de Dijkstra

Comparaison
Vecteur de distance – État de lien

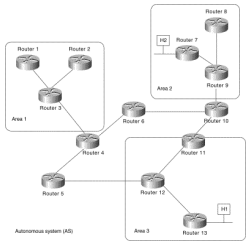
- Vecteur de distance
  - Transmission des vecteurs de distance entre voisins
    - Information globale: distances vers toutes les destinations
    - Peuvent devenir très longs dans des réseaux importants
  - Calcul distribué
    - Convergence peut être lente
    - Problème du comptage à infini
      - La distance maximale doit être limitée, p.ex. à 15
- État de lien
  - Diffusion de l'information topologique par inondation
    - Information sur la topologie locale vue d'un routeur
    - Nécessite la limitation de la taille d'un réseau
  - Calcul local --> convergence rapide et fiable

Exercices 35, 36, 49

OSPF
Open Shortest Path First

- Caractéristiques du protocole
  - Protocole 'ouvert' : standard Internet non-propriétaire
  - Protocole d'état de lien
  - Permet l'utilisation de plusieurs métriques
    - Routage peut dépendre du type de trafic
  - Permet l'équilibrage de la charge sur plusieurs chemins à coût égal (*load balancing*)
  - Protocole IGP (à l'intérieur d'un Système Autonome)
    - Introduit une hiérarchie supplémentaire dans l'AS : les zones
- Protocole de routage le plus utilisé actuellement

Hiérarchie du routage



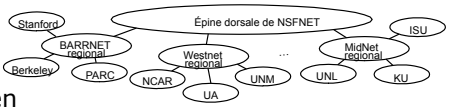
- Un AS est divisé en zones (*areas*)
  - Zone 0 : réseau backbone
    - Interconnecte les autres zones
- OSPF connaître 4 types de routeurs
  - Routeur intra-zone
    - Entièrement à l'intérieur d'une zone
  - Routeur inter-zones (*Area Border Router* ABR)
    - Connecté à plus d'une zone
  - Routeur fédérateur (*Backbone Router*)
    - Connecté à l'épine dorsale (zone 0)
  - Routeur inter-systèmes autonomes (*Boundary Routers*)
    - Connecté aux routeurs d'autres Systèmes Autonomes

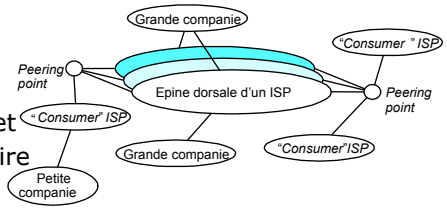
Échange d'information de topologie

- Principe
  - La topologie d'une zone est invisible aux routeurs d'autres zones
  - Les routeurs intra-zone ne connaissent pas la topologie du réseau backbone
- Fonctionnement
  - Un routeur intra-zone diffuse des LSP à tous les routeurs de sa zone
    - Construction des plus courts chemins à l'intérieur de chaque zone,
      y compris la zone 0
  - Les routeurs inter-zones injectent des résumés d'état de liens inter-zones dans les zones locales
    - Permet aux routeurs intra-zones de trouver la meilleure sortie vers une autre zone

Protocoles de routage inter-domaine (*Exterior Gateway Protocols*)

- Protocoles de routage entre Systèmes Autonomes
  - Premier protocole : EGP
    - Nécessitait une topologie en arborescence simple
    - N'est plus utilisé
  - Protocole actuelle : BGP (*Border Gateway Protocol*)
    - A remplacé EGP dans Internet
    - Permet une topologie arbitraire





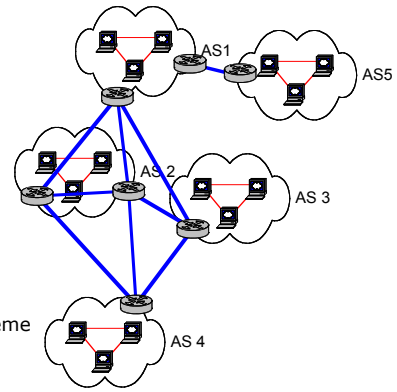
Exercice 50

BGP

- Principes de conception
  - Doit pouvoir gérer les routes dans l'Internet global
    - Actuellement, un routeur BGP connaît environ 90'000 routes
  - Ne peut pas se baser sur les métriques utilisées dans les AS
    - Chaque AS est libre de choisir sa stratégie de routage
    - La notion du plus court chemin n'est pas applicable
  - Utilise des stratégies de routage pour filtrer les routes acceptables
    - Exemple Sun : ne pas utiliser une route qui travers l'AS de Microsoft
- BGP ne cherche pas le meilleur chemin mais un chemin quelconque
  - Échange des informations d'accessibilité
  - Évite des boucles de routage
  - Configuration locale d'une stratégie de routage

Systèmes Autonomes (AS)

- Sous le contrôle d'une seule administration
- Peut comprendre plusieurs réseaux (NetIds)
  - Exemples:
    - Réseau d'un ISP et de ses clients
    - Réseau d'une grande entreprise
- Types d'AS
  - Le bout de AS : (*stub AS*)
    - A une seule connexion avec un autre système autonome
    - Transporte du trafic local seulement
  - AS multi-ports: (*multi-homed AS*)
    - A des connexions avec plus d'un système autonome
    - Refuse de transporter le trafic de transit
  - AS de transit : (*transit AS*)
    - A des connexions avec plusieurs autres AS
    - Transporte le trafic local et le trafic de transit

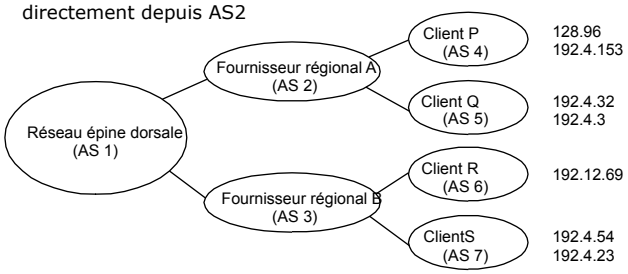


Fonctionnement de BGP

- Chaque système autonome a un ou plusieurs routeurs BGP
- Un routeur BGP annonce vers l'extérieur :
  - les réseaux à l'intérieur de l'AS
  - les réseaux externes atteignables à travers l'AS
  - Communique le chemin entier pour atteindre chaque réseau
    - Exemple : AS A annonce une route vers un réseau n:
      - n : A-B-C-F (chemin des AS traversés)
    - Permet de filtrer les routes
    - Permet de détecter facilement des boucles de routage
  - ➢ External BGP
- Un routeur BGP communique avec les routeurs internes
  - Diffuse quelques routes apprises vers l'intérieur du AS
  - S'assure de la connectivité à d'autres AS
  - ➢ Internal BGP

Exemple EBGP

- Router BGP pour AS2 annonce l'accessibilité de P et Q
  - Les réseaux 128.96, 192.4.153, 192.4.32, et 192.4.3, peuvent être atteints directement depuis AS2



- Le routeur BGP de l'épine dorsale annonce
  - Les réseaux 128.96, 192.4.153, 192.4.32, et 192.4.3 peuvent être atteints le long du chemin (AS1, AS2).
- Le routeur BGP peut supprimer des chemins annoncés précédemment

Exercices 44, 46

Routages sans classes

- Problème actuelle de BGP
  - Les adresses classe B sont épuisées
  - Une grande entreprise ayant plus de 255 hôtes doit utiliser plusieurs adresses classe C
  - Un routeurs BGP doit connaître et annoncer des routes pour chaque réseau classe C
    - En théorie jusqu'à 2 mio de routes vers des réseaux classe C
- Solution
  - Allocation de blocs de taille variable d'adresses classe C
    - Site à 2000 hôtes : allocation de 8 adresses classe C contiguës
      - Meilleure efficacité que l'allocation d'une adresse classe B
  - Un bloc d'adresses est alloué de telle manière qu'il forme un super-réseau avec un préfix d'identificateur de réseau commun

Exemple

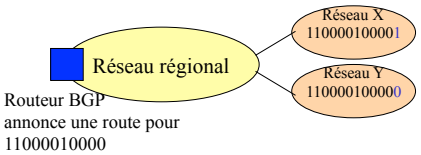
- Site ayant besoin de 4000 adresses
  - Allocation de 16 adresses classe C:
    - 192.4.16 – 192.4.31
    - Structure normale des adresses

  - Ces adresses on le même préfixe binaire
    - Premiers 20 bits = 11000000 00000100 0001
    - Elles peuvent être agrégées dans un seul 'super-réseau' ayant un identificateur de réseau sur 20 bits

- Contrainte
  - Les blocs d'adresses doivent avoir une taille de 2^x d'adresses classe C

Classless Inter-Domain Routing

- CIDR
  - Implémenté dans la nouvelle version BGP-4
    - Définit des identificateurs de réseau de longueur variable
    - Compromis entre efficacité et complexité du routage
  - Agrégation de routes avec CIDR
    - Si un routeur utilise la même route pour plusieurs blocs d'adresses contigus, il peut annoncer une seule route



    - Exemple
      - Adresses classe C 194.0.0.0 – 195.255.255.255 --> Europe
      - Un routeur BGP américain considère les premiers 8 bit pour le routage
      - Un routeur BGP européen doit considérer des préfixes plus longs

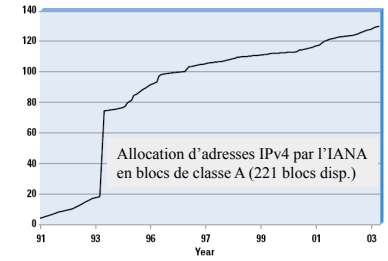
Exercices 40, 41, 42, 43

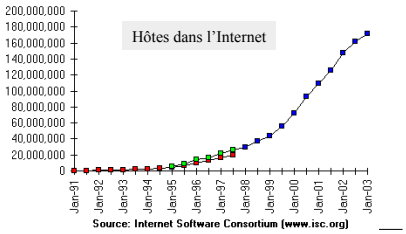
IPv6

- La nouvelle version du protocole IP
  - RFC 2460
- Pourquoi un nouveau protocole
  - Problèmes d'IPv4
    - Pénurie d'adresses
    - Croissance des tables de routage
    - Panoplie de protocoles autour d'IP
      - ARP pour chaque technologie sous-jacente
      - ICMP, IGMP
      - Mobilité (IP Mobile)
      - Sécurité (IPSec)

Pénurie d'adresses IPv4

- Mesures prises pour éviter l'épuisement des adresses
  - Adressage privé et NAT
    - Problèmes de compatibilité
      - Protocoles de sécurité
      - Applications multimédia
  - Allocation d'adresses classe C et routage CIDR
    - Permet une meilleure efficacité d'allocation d'adresse
- ➢ Pas d'épuisement avant 2010 ou 2015, mais
  - Problèmes avec NAT
  - Problèmes d'efficacité d'IPv4 pour les réseaux à haut débit





Objectifs principaux d'IPv6

- Supporter des milliards d'ordinateurs, terminaux mobiles, …
- Réduire la taille des tables de routage
- Simplifier le protocole
  - Acheminement à haute vitesse
- Fournir une meilleure sécurité
- Permettre la mobilité d'ordinateurs
- Permettre au protocole une évolution future
- Permettre une coexistance entre IPv4 et IPv6
- Rester compatible avec les protocoles TCP, UDP, OSPF, RIP, BGP, DNS, ainsi qu'avec les applications

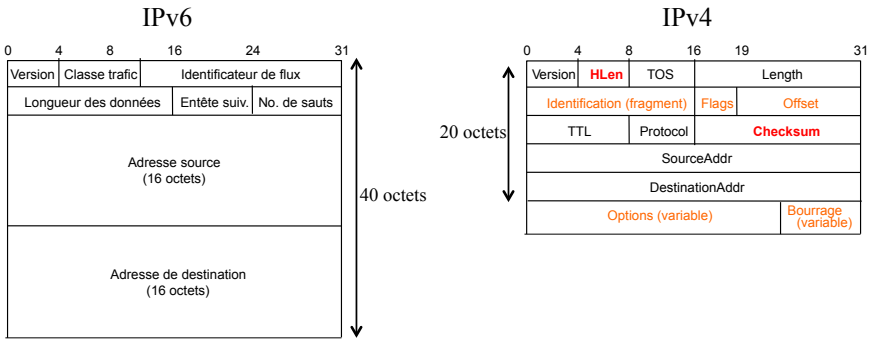
Historique

- RFC 1550: Appel de propositions pour IPng
- Déc. 1992: 21 propositions, 7 sélectionnées
- 3 propositions publiées et discutées
  - Deering (1993) : SIP: Simple Internet Protocol
  - Francis (1993) : Pip
  - Katz, Ford (1993) : TUBA: TCP et UDP sur CLNP (OSI)
- Combinaison et modification de SIP et Pip
  --> SIPP (SIP Plus) --> IPv6 (1995)

Survol des caractéristiques principales

- Adresses sur 128 bits au lieu de 32 bits dans IPv4
  - Adressage hiérarchique
- En-têtes simplifiés
  - Nombre de champs réduit de moitié
- Extensibilité de l'en-tête par des options
  - Traitement efficace des datagrammes par les routeurs
  - Introduction de nouvelles fonctionnalités
- Intégration d'éléments de sécurité
  - Authentification, intégrité, confidentialité
- Intégration de mécanismes de gestion de mobilité
- Nouvelles fonctionnalités
  - Configuration automatique d'adresses
  - Routage par la source
  - Découverte de la MTU le long d'une route
- La fragmentation n'est plus supportée par les routeurs
- ICMP, IGMP, ARP remplacés par ICMPv6

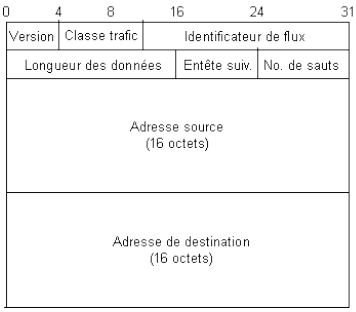
Format de l'en-tête de base



- Longueur fixe de l'en-tête
  - *Header Length* n'est plus nécessaire
  - Les en-têtes d'extensions sont utilisés pour des fonctionnalités optionnelles
- Le champs *Checksum* est éliminé pour des raisons d'efficacité
  - Le contrôle d'erreur à la couche Transport (TCP, UDP !) devient obligatoire

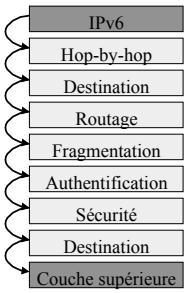
Les champs de l'en-tête

- Classe de trafic (8 bit)
  - Correspond au champs Type Of Service d'IPv4
  - Sera utilisé avec la sémantique des Services Différenciés
- Identificateur de flux (20 bit)
  - Normalisation pas encore terminée
  - Pourrait faciliter la classification des paquets d'une connexion
- Longueur des données (16 bit)
  - Indique la longueur des données qui suivent l'en-tête (contrairement au champs Longueur dans IPv4
  - Longueur maximale en mode normal: 65'535 octets
  - Option 'Jumbogrammes' pour des datagrammes plus longs
- En-tête suivant (8 bits)
  - Indique le type de l'en-tête qui suit
    - En-tête d'extension ou protocole de la couche supérieure
- Nombre de sauts
  - Similaire au champs Time-To-Live en IPv4
  - Décrémenté à chaque pas jusqu'à zéro



Les en-têtes d'extension

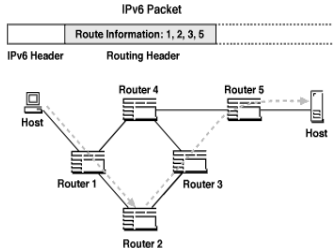
- Permettent d'implémenter des fonctionnalités supplémentaires
- Sont examinés par les systèmes terminaux (sauf en-tête *hop-by-hop*)
- Chaque en-tête indique l'en-tête suivant dans le premier champs
- L'ordre de l'examen des en-têtes est important



Examiné par chaque routeur intermédiaire. Utilisé pour les jumbogrammes.	
Examiné par les router indiqué dans l'extension de routage	
Liste de routeurs à traverser (Routage par la source)	
Fragmentation et réassemblage par les systèmes terminaux	
Authentification	
Contient les données chiffrées du datagrammes	
Examiné par le destinataire final du datagramme	
P.ex. TCP, UDP	

En-tête de routage

- Indique une séquence de routeurs qui doivent être traversés par le datagramme
- Permet de réaliser le routage par la source
  - Fonctionnalité existante déjà dans IPv4 mais peu efficace
- Algorithme
  - L'adresse destinataire du datagramme envoyé par la source est celle du premier routeur
  - Le premier 'destinataire' trouve l'adresse du prochain routeur dans l'en-tête de routage et la met comme prochain 'destinataire'
  - Chaque routeur décrémente la valeur du champ 'Segments restants'
- Plusieurs types de routage peuvent être définis



Format de l'en-tête de routage

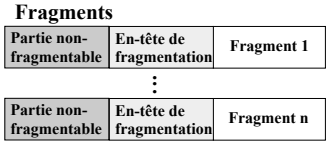
0	8	16	31
En-tête suivant	Long. en-tête	Type de routage	Segm. restants
Réservé			
Adresse 1			
…			
Adresse N			

Fragmentation

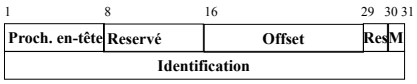
- Contrairement à IPv4, la fragmentation est uniquement utilisée par la source du datagramme
- Un routeur qui devrait transmettre un datagramme trop long renvoie un message ICMP à la source qui indique la MTU permise (Message ICMPv6 « Paquet trop grand »)
- Chaque interface doit avoir une MTU d'au minimum 1280 octets
- Algorithme
  - Le datagramme originale est composé de deux parties
    - Partie non-fragmentable
      - En-tête IPv6 de base
      - Toutes les extensions à examiner par les nœuds intermédiaires
    - Partie fragmentable
  - Chaque fragment transmis comprend
    - La partie non-fragmentable
    - L'en-tête de fragmentation
    - Une partie du datagramme

Datagramme IP

Fragments



Format de l'en-tête de routage



Adressage IPv6

- Adresses sur 128 bits (16 octets)
  - Permet (théoriquement) d'adresser $3{,}4 \cdot 10^{38}$ interfaces
  - Selon des calculs très pessimistes, plus de 1000 adresses par m^2 de la surface de la terre
- Une interface a plusieurs adresses
  - Adresses locales (lien, site)
  - Adresse globale
- Notation
  - 8 groupes de 4 chiffres hexadécimaux, séparés par ':'
    - FADC:AB75:4345:4A45:AF3F:3255:F431:A44B
  - Les premiers 0 d'un groupe peuvent être omis
    - 123 au lieu de 0123
  - **Compression des zéros**: plusieurs groupes 0 peuvent être remplacés par '::'
    - 1080:0:0:0:0:800:200C:2342 --> 1080::800:200C:2342
    - 0:0:0:0:0:0:0:1 --> ::1
  - **Suffixe en décimal pointé**: les adresses IPv4 peuvent être écrit avec les 4 derniers octets en notation décimale
    - ::192.31.32.46

Espaces d'adresses actuellement alloués

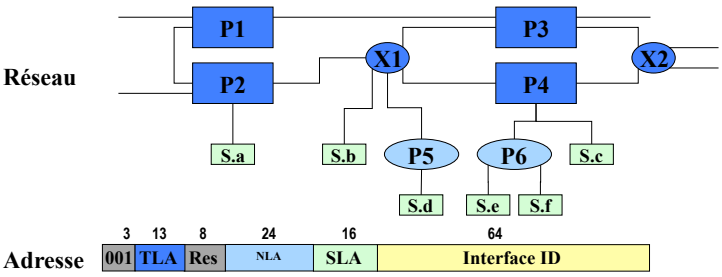
- Types d'adresses
  - Adresses unicast
  - Adresses multicast
  - Adresses anycast
- Sans adresse broadcast
  - Diffusion peut être simulée par des adresses multicast

Préfixe	Type d'adresse	Fraction de l'espace d'adresses
0000 0000	**Réservé (compatible IPv4)**	**1/256**
0000 0001	Non affecté	1/256
0000 001	Adresses NSAP (OSI)	1/128
0000 010	Adresses Network IPX Novell	1/128
0000 011	Non affecté	1/128
0000 1	Non affecté	1/32
0001	Non affecté	1/16
001	**Adresses unicast globales agrégeables (RFC 2374)**	**1/8**
010	Non affecté	1/8
011	Non affecté	1/8
100	Non affecté (avant : adresses géographiques)	1/8
110	Non affecté	1/8
1110	Non affecté	1/16
1111 0	Non affecté	1/32
1111 10	Non affecté	1/64
1111 110	Non affecté	1/128
1111 1110	Non affecté	1/256
1111 1110 0	Non affecté	1/512
1111 1110 10	**Adresse locale unicast de lien**	**1/1024**
1111 1110 11	**Adresse locale unicast de site**	**1/1024**
1111 1111	**Adresses multicast**	**1/256**

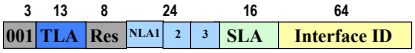
Adresses globales unicast avec agrégation

- Idée similaire à CIDR
  - L'Internet à une structure hiérarchique
    - Réseaux backbone, ISPs, clients
  - Le schéma doit permettre l'agrégation d'adresses à plusieurs niveaux afin de réduire la taille des tables de routage
- Structuration des adresses IPv6 en 3 niveaux
  - Niveau de la topologie publique
    - Réseaux backbone et ISP qui permettent le transit
  - Niveau d'un site
    - Réseau 'stub' d'une organisation
  - Identificateur d'interface

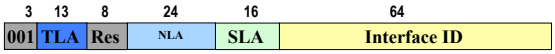
Niveaux de l'adressage



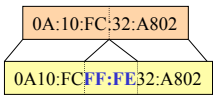
- TLA Id : Top Level Aggregator Id
  - TLA désigne un réseau backbone
  - Actuellement jusqu'à 8'192 TLA
  - Routeurs du plus haut niveau devront connaître les routes pour tous les TLA
- NLA Id : Next level Aggregator Id
  - Assignés par un TLA
  - Possibilité de créer une hiérarchie de NLA



Niveaux de l'adressage cont.



- SLA : Site Level Aggregator Id
  - Utilisé par une organisation ou une entreprise
  - Permet de crée une hiérarchie d'adresses à l'intérieur d'une organisation
    - Similaire aux sous-réseaux dans IPv4
- Interface Id
  - Format défini par la norme IEEE EUI-64
  - Doit être unique au niveau globale
  - Construction à partir d'une adresse MAC
    - Ajouter les octets FFFE entre les 3 premiers octets (fournisseur) et les 3 derniers octets (numéro de série de la carte)
    - Exemple :
      - Adresse MAC :
      - Interface Id :



Adresses particulières

- Adresses locales unicast de lien
  - Utilisation limitée aux interfaces directement connectées sur le même 'lien' (sans routeur intermédiaire)
  - Utilisées par les protocoles de configuration d'adresses globales, de découverte de voisins, …
- Adresses locales unicast de site
  - Utilisables dans un réseau sans connexion à l'extérieur
  - Similaires aux adresses privées d'IPv4
  - Le routeurs de sortie filtrent les paquets avec des adresses locales
- Adresse indéterminée
  - Composée uniquement de zéros, notation abrégée '::'
  - Utilisée pendant l'initialisation d'un nœud
- Adresse de bouclage
  - 0:0:0:0:0:0:0:1 ou ::1 en notation abrégée
  - Utilisée pour la communication inter-processus sur un nœud

Nouvelle fonctionnalité : Découverte de voisins

- *Neighbor discovery* (RFC 2461)
- Remplace le protocole ARP
- Implémentée à l'aide de nouveaux messages ICMPv6
  - Message 'Sollicitation de voisins'
    - Envoyé à l'adresse multicast '*All nodes*' du 'lien'
    - Contient l'adresse IPv6 du nœud cherché
  - Message 'Annonce d'un voisin'
    - Envoyé en réponse à une sollicitation ou spontanément
    - Contient l'adresse IPv6 et physique (MAC) du nœud

Nouvelle fonctionnalité : Configuration automatique sans état

- Facilité la gestion du réseau des stations terminales, non pas des routeurs
- Basée sur 2 nouveaux messages ICMPv6
  - Message ICMPv6 'Sollicitation des routeurs'
  - Message ICMPv6 'Annonce d'un routeur'
    - Envoyé périodiquement ou après une sollicitation
      - Inclut des options pour signaler la MTU du lien, …
      - Indique si l'auto-configuration sans état est permise et le préfix du sous-réseau à utiliser
      - Peut limiter la durée de vie du préfixe indiqué
- Algorithme
  1. La station construit une adresse locale de lien
     - Préfix 'FE80::' plus l'ID de l'interface (--> MAC)
     - Le nœud teste s'il y a un conflit en envoyant un message 'Sollicitation de voisins'
  2. La station envoie une sollicitation de routeurs à l'adresse multicast 'All routers' du lien
  3. Le routeur renvoie une annonce de routeur avec un préfixe du sous-réseau
  4. La station obtient une adresse globale en concaténant le préfixe avec l'ID de l'interface

Configuration automatique avec état

- Basée sur l'utilisation d'un serveur DHCPv6
- Permet une meilleure contrôle de l'utilisation d'adresses
- Normalisation en cours

Transition vers IPv6

- Moteurs de la transition
  - Pénurie d'adresses dans les pays avec une forte croissance de l'Internet
  - Demande d'adresses pour les nouveaux types de réseaux (réseaux mobiles, réseaux domotiques)
- Obstacles
  - Pas de '*killer application*' d'IPv6
    - IPv6 offre les mêmes fonctionnalités que IPv4
  - Coût de la migration
    - Mise à jour de l'équipement et des applications
    - Formation des administrateurs de réseau
  - Manque d'expérience, peur de pannes, …

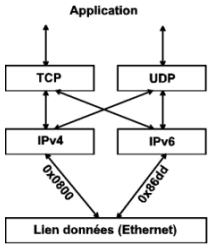
➢ Processus progressive avec une longue phase de coexistence d'IPv4 et IPv6

Techniques de transition

- Double pile IPv4 et IPv6
- 'Tunneling' d'IPv6 dans IPv4
- Traduction IPv6 ⇔ IPv4
  - NAT-PT
  - Relais applicatifs

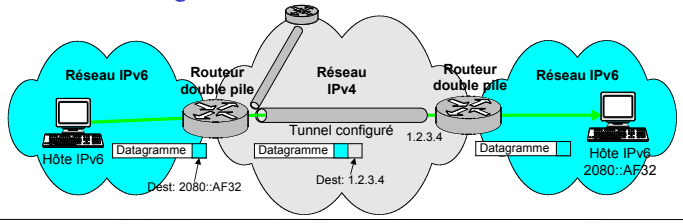
Double pile IPv4 et IPv6

- Permet la compatibilité entre IPv4 et IPv6
- Une machine a des adresses IPv4 et IPv6
  - Un hôte double pile peut communiquer avec des hôtes IPv4, IPv6 et double pile
- Comment choisir la version d'IP d'une transmission ?
  - DNS répond à une requête avec une adresse IPv4, IPv6 ou les deux



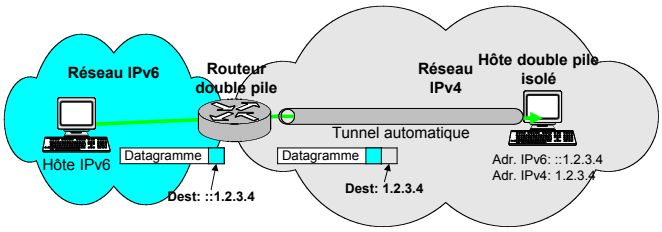
Tunnels IPv6 sur IPv4

- Les réseaux de transit seront migrés progressivement vers IPv6
- L'infrastructure IPv4 restera en place
  - Routeurs double pile
- Pendant la transition il sera nécessaire de transmettre des datagrammes IPv6 des clients sur l'infrastructure IPv4
- Scénario I
  - Des îlots IPv6 sont interconnectés à travers un réseau IPv4
  - Un tunnel configuré IPv6 sur IPv4 est établi entre routeurs



Scénario II: Tunnel automatique

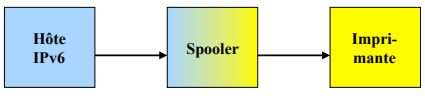
- Utilisable si la terminaison du tunnel est un hôte
  - Tunnel hôte – hôte
  - Tunnel routeur – hôte
- Permet d'établir un tunnel sans configuration
- Utilise une adresse IPv6 'compatible IPv4'
  - Format 0:0:0:0:0:0:d.d.d.d
  - Conversion possible entre IPv4 et IPv6



Traduction IPv4 ⇔IPv6

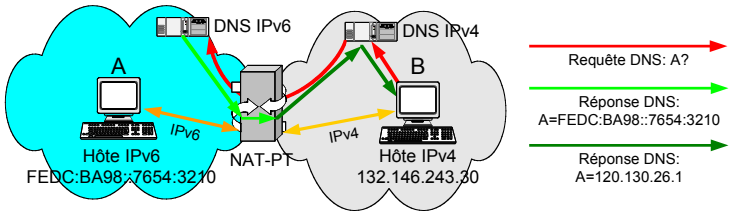
- Permet l'interopérabilité entre des équipements IPv4 pur et IPv6 pur
  - Applicable dans une phase ultérieure de la transition
- Différentes solutions sont possibles

1. Relais applicatifs (*Application Layer Gateway*, ALG)
   - Passerelle spécifique pour chaque application (Mail, Web, …)
   - Exemple: Vielle imprimante sans pile IPv6



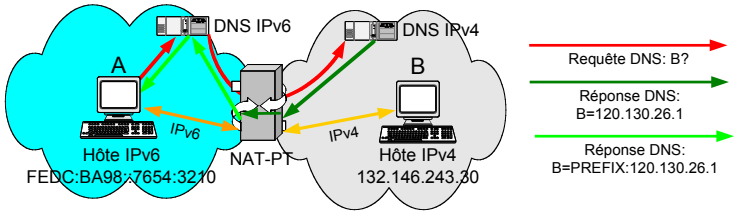
Traduction IPv4 ⇔IPv6 cont.

2. NAT-PT (*Network Address Translation – Protocol Translation*, RFC 2766)
   - Une passerelle NAT-PT convertit les en-têtes entre IPv6 et IPv4
   - Connexion IPv4 --> IPv6
     - B envoie requête DNS pour A
     - DNS répond avec une adresse IPv6
     - La passerelle NAT-PT intercepte la réponse DNS et assigne une adresse IPv4 temporaire à A: FEDC:BA98::7654:3210 --> 120.130.26.1
     - Ensuite communication entre B et A à travers la passerelle NAT-PT



NAT-PT cont.

- Connexion IPv6 --> IPv4
  - A envoie une requête DNS pour B
  - DNS répond avec une adresse IPv4
  - La passerelle NAT-PT intercepte la réponse DNS ajoute un préfix: 132.146.243.30 --> PREFIX::132.146.243.30
  - Lorsque A envoie un datagramme, la passerelle NAT-PT assigne une adresse IPv4 temporaire à A



Résumé IPv6

- Pénurie d'adresses --> Adresses sur 128 bit
- Croissance des tables de routage --> Adressage hiérarchique et agrégation de routes
- Acheminement à haut débit --> traitement efficace de l'en-tête IP
  (en-têtes d'extensions, fragmentation, …)
- Meilleure intégration des protocoles secondaires
  (ARP, IGMP, IP Mobile, IPSec, …)
- Fonctionnalités supplémentaires
  - Découverte de voisins (fonctionnalité d'ARP en IPv4)
  - Autoconfiguration
- Techniques de migration
  - Double pile et tunnels
  - Traduction de protocoles IPv4 ⇔ IPv6

Exercices 51, 52, 53, 54

Mobilité dans IP

- Objectif
  - Rendre possible le déplacement d'un ordinateur mobile (PC portable, agenda électronique, …) d'un réseau à un autre de manière transparente pour les applications
- Types
  - Nomadicité (*portability*)
    - Déplacement 'off-line', mais sans re-paramétrage manuelle
    - Nécessite l'interruption de toutes les connexions en cours
    - --> DHCP
  - Mobilité d'un ordinateur
    - Un ordinateur mobile peut changer sont point d'attachement sans interrompre les communications en cours
  - Réseau mobile
    - Réseau ad-hoc sans infrastructure

Problème de l'adressage IP

- Une adresse IP
  - identifie un système terminal
    - Correspondance statique entre le nom de domaine et l'adresse IP par DNS
  - détermine la route vers un système terminal
    - L'adresse IP comprend un NetId et un HostId
    - Le routage utilise le NetId pour trouver le chemin vers le système terminal
- Contradiction
  - Un ordinateur mobile nécessite une adresse fixe pour être joignable
  - Une adresse fixe implique un routage fixe
- Idée : Utiliser deux adresses
  - Une adresse qui identifie un ordinateur
  - Une adresse qui permet de joindre l'ordinateur

Mobile IP

- Défini dans la RFC 2002 (3344)
  - Permet une mobilité globale dans Internet
  - Solution au niveau de la couche Réseau
- Principes de conception
  1. Transparence pour les applications existantes
     - Un ordinateur mobile doit être capable de communiquer avec un autre ordinateur qui n'implémente pas IP Mobile
     - Un ordinateur mobile doit être joignable en utilisant uniquement son adresse IP (normale)
  2. Transparence pour les routeurs existants
     - Aucune modification de la méthode de routage
     - Sans modification permanente des tables de routage
  3. Sécurité
     - Un ordinateur mobile ne doit pas être plus exposé qu'une autre machine

Terminologie

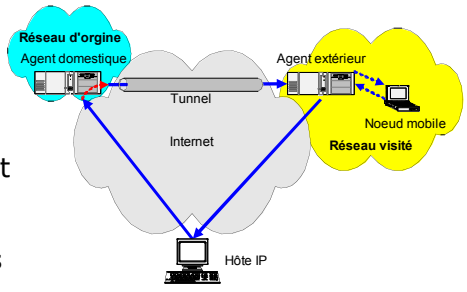
- Nœud mobile
  - Nœud qui peut changer de points d'attachement sur l'Internet tout en maintenant les communications en cours
- Réseau d'origine (*Home Network*)
  - Réseau auquel appartient l'adresse IP du nœud mobile
- Réseau extérieur (*Foreign Network*)
  - Réseau visité par le nœud mobile
- Agent domestique (*Home Agent*)
  - Routeur avec une interface sur le réseau d'origine du nœud mobile
- Agent extérieur (*Foreign Agent*)
  - Routeur situé dans le réseau visité par le mobile

Adresses

1. Adresse de domiciliation (*Home Address*)
   - Adresse principale de l'ordinateur mobile dans son réseau d'origine
   - Adresse sur laquelle le mobile est contacté par d'autres machines
2. Adresse de réexpédition (*Care-of Address, c/o address*)
   - Adresse faisant partie du réseau visité
   - Utilisée par l'agent domestique et l'agent extérieur pour acheminer des messages
   - Deux types
     - « Adresse de réexpédition par agent extérieur »
       - Adresse de l'agent extérieur
     - « Adresse de réexpédition par colocataire »
       - Adresse assignée de manière temporaire à l'ordinateur mobile

Principe du protocole

1. Un nœud mobile obtient une adresse de réexpédition du réseau visité
2. Le nœud mobile enregistre son adresse c/o auprès de son agent domestique
3. L'agent domestique intercepte tous les paquets destinés au nœud mobile et les transmet à travers un tunnel vers l'adresse c/o
4. Le nœud mobile envoie ses paquets directement aux correspondants



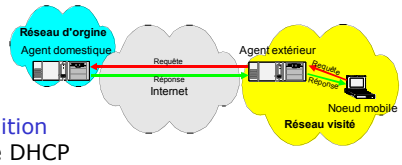
Découverte des agents

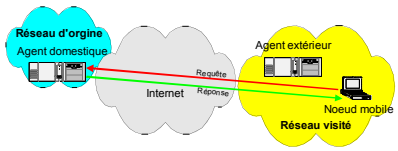
- Permet à un nœud mobile de savoir s'il se trouve dans son réseau d'origine ou dans un autre réseau
- Principe
  - Les agents diffusent périodiquement des messages « *Agent advertisement* » sur le LAN auquel ils sont attachés
  - Un nœud mobile peut aussi solliciter une réponse d'un agent présent en envoyant un message de découverte d'agent
- Format des messages
  - Extension des messages ICMP standard
  - Le message « *Agent advertisement* » contient
    - Une adresse de réexpédition que le nœud mobile peut utiliser
    - Une durée de vie pendant laquelle l'agent prend en compte l'enregistrement du mobile

0	8	16	24	31
TYPE (16)	LENGTH	SEQUENCE NUM		
LIFETIME		CODE	RESERVED	
CARE-OF ADDRESSES				

Enregistrement

- Lorsqu'un mobile est hors de son réseau d'origine il enregistre son adresse temporaire auprès de son agent domestique
- Deux cas
  1. Le mobile utilise l'adresse de réexpédition de l'agent extérieur
     - Le mobile envoie une requête d'enregistrement à l'agent extérieur qui la fait suivre à l'agent domestique
     - L'agent domestique revoie la réponse d'enregistrement à l'agent extérieur qui la passe au mobile
  2. Le mobile utilise une adresse de réexpédition par colocataire, obtenue p.ex. à l'aide de DHCP
     - La requête et la réponse sont envoyées directement entre le mobile et l'agent domestique





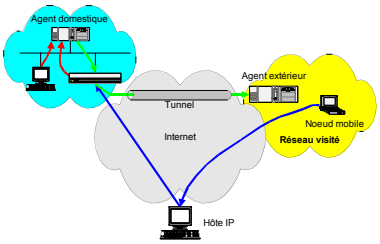
Contenu des messages d'enregistrement

0	8	16	31
TYPE (1 or 3)	FLAGS	LIFETIME	
HOME ADDRESS			
HOME AGENT			
CARE-OF ADDRESS			
IDENTIFICATION			
EXTENSIONS . . .			

- **Type**: requête ou réponse
- **Durée de vie**: les agents peuvent limiter la durée de validité de l'enregistrement
- Adresse de domiciliation et adresse de réexpédition
- Agent domestique
- **Identification**: valeur générée par le mobile pour identifier les requêtes et réponse et pour des raisons de sécurité
- **Drapeaux/Code**: indique le succès de la requête ou des options supplémentaires
- **Extensions**: p.ex. authentification

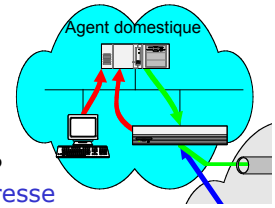
Transmission des datagrammes

- Mobile --> Correspondant
  - Le mobile envoie des datagramme avec son adresse de domiciliation comme source
  - Le datagramme utilise le routage habituel pour arriver au destinataire
- Correspondant --> Mobile
  - Les datagrammes envoyés par une machine quelconque au mobile sont routés vers le réseau d'origine du mobile
  - L'agent domestique doit
    - Intercepter les datagrammes destinés au mobile
    - Les réexpédier vers le mobile en contournant le routage normal



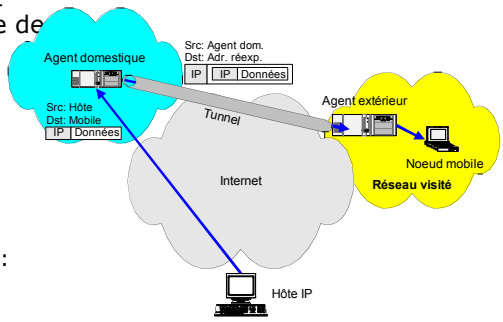
Interception des messages

- L'agent domestique doit intercepter les messages provenant
  - De l'extérieur (d'un ordinateur se trouvant dans un autre réseau)
  - De l'intérieur (d'un ordinateur local connecté au même réseau)
- L'agent domestique ne se trouve pas nécessairement dans le chemin des datagrammes
- Technique : proxy ARP
  - L'agent mobile répond aux requêtes ARP concernant le nœud mobile avec son adresse MAC
    - ➢ Toutes les trames destinées au nœud mobile arrivent à l'agent domestique



Tunnel

- Technique souvent utilisée pour contourner le routage habituel
- Principe
  - L'agent domestique encapsule le datagramme intercepté dans un autre datagramme, ayant comme destinataire l'adresse de réexpédition
  - La terminaison du tunnel décapsule le datagramme original
    - Réexpédition par agent extérieur :
      - L'agent extérieur sert de terminaison de tunnel
    - Réexpédition par colocation :
      - Le nœud mobile termine le tunnel



Aspects problématiques de Mobile IP

- Sécurité
  - Le mécanisme d'enregistration permet à un intrus de dévier/interrompre des communications
    - Mécanisme d'authentification
  - Configuration des firewalls des réseaux visités/d'origine
- Inefficacité de routage (*triangle routing*)
  - Une solution est de communiquer l'adresse de réexpédition au correspondant pour établir un tunnel direct vers le nœud mobile
    - Le correspondant doit implémenter IP Mobile
- Fast handoff
  - Pendant la transition d'un réseau à un autre, des paquets peuvent arriver à la mauvaise adresse de réexpédition
  - « A better than nothing fast handover », Doswald, Robert