

La couche réseau de la pile IP

Chaput Emmanuel

INP TOULOUSE ENSEEIHT

2024-2025



Chaput Emmanuel La couche réseau de la pile IP 2024-2025 1 / 75

Plan

- 1 Introduction
- 2 L'adressage IPv4
- 3 L'adressage IPv6
- 4 Anycast et multicast
- 5 Le protocole IP
- 6 Le protocole ICMP
- 7 Les protocoles ARP et RARP
- 8 Références bibliographiques

Chaput Emmanuel La couche réseau de la pile IP 2024-2025 2 / 75

Introduction

- 1 Introduction
- 2 L'adressage IPv4
- 3 L'adressage IPv6
- 4 Anycast et multicast
- 5 Le protocole IP
- 6 Le protocole ICMP
- 7 Les protocoles ARP et RARP
- 8 Références bibliographiques

Chaput Emmanuel La couche réseau de la pile IP 2024-2025 3 / 75

Introduction

- Le cœur de la pile [?]
- Commutation de paquets
 - En mode non connecté
 - Aucune garantie
 - "Best Effort"
 - Pas de négociation de qualité de service
- Aucune contrainte sur la couche liaison
 - "IP sur tout"

Chaput Emmanuel La couche réseau de la pile IP 2024-2025 4 / 75

L'adressage IPv4

- 1 Introduction
- 2 L'adressage IPv4
 - Les classes d'adresses
 - Les sous-réseaux
 - Les adresses spéciales
 - L'attribution des adresses IPv4
 - L'adressage CIDR
 - La résolution des noms
 - Manipulation
 - Quiz
- 3 L'adressage IPv6
- 4 Anycast et multicast
- 5 Le protocole IP
- 6 Le protocole ICMP
- 7 Les protocoles ARP et RARP

Chaput Emmanuel La couche réseau de la pile IP 2024-2025 5 / 75

L'adressage IPv4

Identification des entités de niveau 3

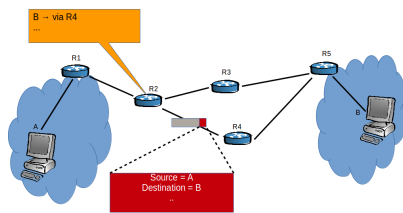
- Individuelle (hôte) et collective (réseau)
- Correspondance éventuelle avec la couche inférieure
- Besoin d'unicité et uniformité dans le réseau
 - Gestion centralisée
- Par exemple, l'adresse du destinataire figure dans un paquet

Localisation de ces entités

- Il faut trouver le destinataire d'un paquet dans le réseau
- Hiérarchie minimaliste
 - Machine, réseau
 - Une partie de l'adresse désigne le réseau
 - Une autre partie désigne l'entité dans ce réseau
 - Évolutions au grès des besoins
 - Masque, CIDR, IPv6, ASN, ...

Chaput Emmanuel La couche réseau de la pile IP 2024-2025 6 / 75

Fonctions de l'adresse

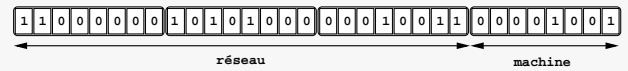


L'adresse de B permet

- à A d'identifier B comme destinataire de ses paquets
- aux routeurs de déterminer où est B pour les acheminer.

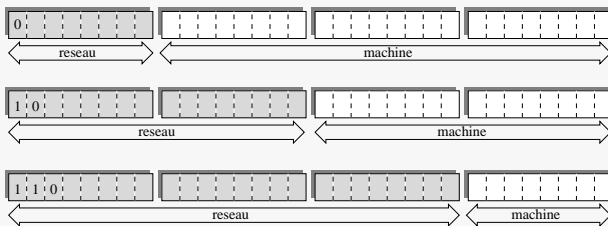
L'adressage IPv4

- Format
 - Quatre octets (32 bits)
 - 4 294 967 296 valeurs (théoriquement)
- Notation traditionnelle
 - Décimale pointée
 - aaa.bbb.ccc.ddd
- Exemples
 - 192.168.13.1
 - 147.127.18.98



Les classes d'adresses IPv4

- Trois tailles possibles de réseau (classes A, B, C)
- Granularité forte
- Historique

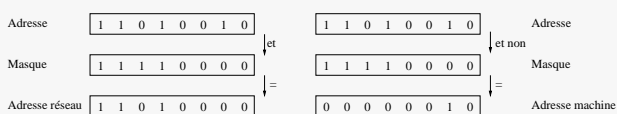


Sous-réseaux IP

- Fin 1984 : un millier de machines sur Internet
 - Avec des réseaux de plus en plus complexes
- Utilisation de plus en plus courante d'un second niveau de hiérarchie
 - Notion de "sous-réseau" IP
 - Plusieurs niveaux de précision du routage
- Mise en place via un masque [?][?]
 - Délimitation plus libre entre la partie réseau et la partie machine d'une adresse

Le netmask

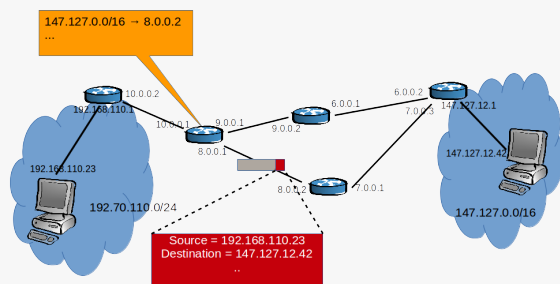
- Le masque identifie dans l'adresse
 - le réseau (partie "fixe")
 - le sous-réseau (partie "variable")
- Principe de base sur un octet :



Quelques adresses particulières

- Tous les bits machine à 1
 - Adresse de diffusion
- Tous les bits machine à 0
 - Adresse du réseau
- Premier et dernier sous-réseaux
 - 0.0.0.0 et 255.255.255.255
- 127.0.0.0
 - Réseau de rebouclage
- 10.0.0.0, 172.16.0.0-172.31.0.0, 192.168.x.0
 - Usage privé [?]

Fonctions de l'adresse IPv4



L'attribution des adresses IPv4

Choix des adresses : affectation hiérarchique

- Plus haut niveau : IANA et ses RIRs
- Fournisseurs d'accès
- Administrateur du réseau
- Garantie d'unicité
- Limite de la notion de classes
 - Trop peu de réseaux
 - Réseaux trop vastes
- Possibilité d'utiliser des adresses à usage privé [?]
 - Dites également "non routables"
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16

L'attribution des adresses IPv4

Outils de configuration des machines

- Configuration statique
 - Chaque machine (interface) se voit attribuer son adresse de façon "définitive"
 - Gestion "manuelle"
 - Elle pourra être associée simplement à un nom symbolique
 - Commande `ifconfig` ou équivalent
 - Fichier de configuration
- Configuration dynamique
 - Un ensemble d'adresses peut être réparti sur un ensemble (plus limité) de machines
 - Gestion automatique
 - L'unicité doit être assurée
 - Protocole DHCP ou équivalent
 - Possibilité de ré-affectation

Classless Inter Domain Routing

Pourquoi CIDR [?] [?] ?

- Septembre 1993
 - 2 000 000 de machines
 - 30 000 domaines
- Raréfaction des adresses
- Prévisions à court terme (moins de trois ans)
 - Plus de réseaux de classe B disponible
 - Explosion des tables de routages
 - 173 en juillet 1988
 - 8561 en décembre 1992

Principes de CIDR

- *Supernetting* (premier nom)
 - Technique similaire au subnetting
- Préfixe de longueur quelconque
 - Fin des classes
- Possibilité d'agrégation de routes
 - Limitation de l'explosion des tables
- Redéfinition des techniques d'allocation
 - Permettre la hiérarchie



La résolution des noms

- Problème uniquement humain
 - Retenir des noms plutôt que des numéros
- Notion d'annuaire
 - Correspondance nom/adresse
 - Échelle mondiale
 - Service réparti
- Service applicatif
 - Voir le chapitre correspondant pour la description du protocole

Manipulation (Linux net tools)

Configuration d'une interface

ifconfig eth0 192.168.19.31 255.255.255.0

Consultation d'une interface

ifconfig eth0

Déconfiguration d'une interface

ifconfig eth0 0.0.0.0

Activation/désactivation d'une interface

ifconfig eth0 up
ifconfig eth0 down

Création d'un alias

ifconfig eth0:1 10.0.0.31 255.255.0.0

Chaput EmmanuelLa couche réseau de la pile IP2024-202519 / 75

Manipulation (Linux iproute2)

Configuration d'une interface

ip addr add 192.168.19.31/24 dev eth0

Consultation d'une interface

ip addr show dev eth0

Déconfiguration d'une interface

ip addr del 192.168.19.31/24 dev eth0

Activation/désactivation d'une interface

ip link set eth0 up
ip link set eth0 down

Ajout d'un alias

ip addr add 10.0.0.31/16 dev eth0 label eth0:1

Chaput EmmanuelLa couche réseau de la pile IP2024-202520 / 75

Manipulation (Cisco IOS)

Configuration d'une interface

Router (config) # interface fa0/0
Router (config-if) # ip address 192.168.19.31 255.255.255.0

Consultation d'une interface

Router # show interface fa0/0

Déconfiguration d'une interface

Router (config-if) # no ip address 192.168.19.31 255.255.255.0

Activation/désactivation d'une interface

Router (config-if) # no shutdown
Router (config-if) # shutdown

Configuration d'une adresse secondaire

Router (config-if) # ip address 10.0.0.31 255.255.0.0 secondary

Chaput EmmanuelLa couche réseau de la pile IP2024-202521 / 75

Exemple

ifconfig eth0
eth0 Link encap:Ethernet HWaddr 5c:26:0a:19:fb:5f
inet adr:147.127.240.76 Bcast:147.127.240.255 Masque:255.255.255.0
adr inet6: 2001:660:6603:14:5e26:aff:fe19:fb5f/64 Scope:Global
adr inet6: fe80::5e26:aff:fe19:fb5f/64 Scope:Lien
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:28795742 errors:0 dropped:0 overruns:0 frame:0
TX packets:32975939 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 lg file transmission:1000
RX bytes:23706988108 (22.0 GiB) TX bytes:34809932178 (32.4 GiB)
Interrupt:20 Mémoire:e9600000-e9620000
ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWERUP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
link/ether 5c:26:0a:19:fb:5f brd ff:ff:ff:ff:ff:ff
inet 147.127.240.76/24 brd 147.127.240.255 scope global eth0
inet6 2001:660:6603:14:5e26:aff:fe19:fb5f/64 scope global dynamic
validlft 2591712sec preferredlft 604512sec
inet6 fe80::5e26:aff:fe19:fb5f/64 scope link
validlft forever preferredlft forever

Chaput EmmanuelLa couche réseau de la pile IP2024-202522 / 75

Consultation de l'annuaire DNS

dig www.enseeiht.fr

;; <>> Dig 9.9.5-9ubuntu0.3-Ubuntu <>> www.enseeiht.fr
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 41580
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.enseeiht.fr. IN A

;; ANSWER SECTION:
www.enseeiht.fr. 86400 IN A 193.48.203.34

;; AUTHORITY SECTION:
enseeiht.fr. 86400 IN NS ns1.enseeiht.fr.
enseeiht.fr. 86400 IN NS ns2.nic.fr.
enseeiht.fr. 86400 IN NS sivuca.leei.enseeiht.fr.

;; ADDITIONAL SECTION:
ns1.enseeiht.fr. 86400 IN A 147.127.176.22
sivuca.leei.enseeiht.fr. 86400 IN A 147.127.16.11
ns2.nic.fr. 27359 IN A 192.93.0.4
ns2.nic.fr. 27359 IN AAAA 2001:660:3005:1:1:1:2

;; Query time: 3 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Wed Sep 23 12:09:22 CEST 2015
;; MSG SIZE rcvd: 202

Chaput EmmanuelLa couche réseau de la pile IP2024-202523 / 75

Quiz

L'adresse IPV4 de B

1

est unique sur Internet

2

est écrite dans sa carte ethernet

3

permet à A de savoir où est situé B

La table de routage d'un routeur de cœur

1

contient les adresses de toutes les machines

2

est remplie par l'administrateur

3

permet à IP de choisir vers où envoyer un paquet

Dans un paquet IP il y a

1

l'adresse de l'émetteur et du destinataire si c'est le premier paquet

2

toujours l'adresse de l'émetteur celle et du destinataire

3

uniquement l'adresse du destinataire

Chaput EmmanuelLa couche réseau de la pile IP2024-202524 / 75

L'adressage IPv6

- 1 Introduction
- 2 L'adressage IPv4
- 3 **L'adressage IPv6**
 - L'attribution des adresses IPv6
- 4 Anycast et multicast
- 5 Le protocole IP
- 6 Le protocole ICMP
- 7 Les protocoles ARP et RARP

L'adressage IPv6

- 128 bits (16 octets)
 - 667×10^{15} adresses au millimètre carré
- Notation hexadécimale
 - 2001 :660 :6603 :8 :216 :36ff :fe70 :e9d3
 - Notations simplifiées possibles
- Utilisation plus riche
 - Forte hiérarchie
 - Notion de portée (scope) : local, site, global
 - Attribution statique ou dynamique
 - Interactions avec adresses IEEE
 - Intégration de l'anycast et du multicast

Utilisation des adresses IPv6

D'après [?]

Attribuées 2000::/3

- Statiquement ou dynamiquement

Lien local FE80::/10

- Adresse IEEE sur les derniers octets

Site local FC00::/7

- Préfixe, subnet, adresse IEEE sur les derniers octets [?]

Multicast FF00::/8

- Permanentes ou non, portée variable

Compatibles IPv4 2002::/16

- Tunnel IPv6 sur IPv4 (6to4)

Mappés IPv4 ::FFFF:0:0/96

- Routage de paquets IPv4 sur IPv6

L'attribution des adresses IPv6

- Affectation hiérarchique
 - Comme IPv4 (en gros)
 - Plus simple (?)
- Possibilité d'utiliser des adresses locales
- Outils
 - Configuration statique
 - Commande `ifconfig` ou équivalent
 - Fichier de configuration
 - Essentiellement sur les routeurs
 - Configuration dynamique
 - Intégrée à ICMPv6 (mécanisme *stateless*)
 - Protocole DHCPv6 ou équivalent

Les outils d'attribution d'adresses IPv6

- Les outils *statefull*
 - Les mêmes que pour IPv4
 - DHCP, NCP dans PPP, ...
 - Voir le cours sur le plan de gestion
- Les outils *stateless*
 - Router Advertisement (RADV)
 - Voir le cours sur le plan de gestion

Anycast et multicast

- 1 Introduction
- 2 L'adressage IPv4
- 3 L'adressage IPv6
- 4 **Anycast et multicast**
- 5 Le protocole IP
- 6 Le protocole ICMP
- 7 Les protocoles ARP et RARP
- 8 Références bibliographiques

Anycast

- L'adresse IP permet de désigner un destinataire
 - Un équipement individuel
 - Pas un service
 - Comment prendre en compte de la redondance ?
- Les adresses *anycast* permettent de désigner un service
 - Qui peut être déployé sur plusieurs équipements
 - Sans *a priori* sur celui qui va recevoir les paquets
- Usage typique
 - Le DNS [?]
 - Les CDN
- Défini dans [?], et [?, ?] pour IPv6

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

31 / 75

Les adresses *anycast*

- Pas de plage particulière
 - Une adresse *anycast* n'est pas identifiable
 - En IPv4 comme en IPv6
- Tout repose sur le routage
 - Probablement vers une adresse unique
- IPv6 définit des adresse de "*Subnet Router*"
 - Uniquement le format (bits de poids faibles nuls)
 - Utilité apparemment limitée !

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

32 / 75

Anycast : un cas d'usage

- Le serveur racine DNS M est répliqué dans différents *clusters*
 - Voir <https://m.root.servers.org>
 - Adresse IPv4 202.12.27.33
 - Adresse IPv6 2001:dc3::35
- Depuis un premier réseau

```
# traceroute 202.12.27.33
traceroute to 202.12.27.33 (202.12.27.33), 30 hops max, 60 byte packets
 1 cl-nl.virtwire.netroute.com.au (46.166.137.9)  0.081 ms  0.031 ms  0.033 ms
 2 185.107.116.22 (185.107.116.22)  4.561 ms 185.107.116.21 (185.107.116.21)  9.022 ms 185.107.116.22 (185.107.116.22)
 3 wide-project.telehouse-pa2.nl-ix.net (193.239.116.217)  11.154 ms 11.159 ms 11.110 ms
 4 M.ROOT-SERVERS.NET (202.12.27.33)  11.108 ms 11.145 ms 11.126 ms
```

- Depuis un autre réseau

```
traceroute to 202.12.27.33 (202.12.27.33), 30 hops max, 60 byte packets
 1 irit-iptiv192.enseelht.fr (147.127.92.2)  5.228 ms 5.431 ms 5.416 ms
 2 172.22.130.17 (172.22.130.17)  6.419 ms 6.394 ms 6.609 ms
 3 193.55.105.98 (193.55.105.98)  7.102 ms 7.102 ms 7.048 ms
 4 tel-3-toulouse-rtr-021.noc.renater.fr (193.51.181.178)  7.539 ms 7.532 ms 7.746 ms
 5 te4-1-bordeaux-rtr-021.noc.renater.fr (193.51.177.37)  24.553 ms 24.546 ms 24.523 ms
 6 te0-0-0-3-lyon1-rtr-001.noc.renater.fr (193.51.177.41)  23.890 ms 28.116 ms 28.126 ms
 7 tel-2-rennes-rtr-021.noc.renater.fr (193.51.177.34)  28.100 ms 28.100 ms 28.094 ms
 8 xe0-0-4-paris1-rtr-131.noc.renater.fr (193.51.177.234)  27.235 ms 27.511 ms 27.497 ms
 9 193.51.180.45 (193.51.180.45)  27.775 ms 193.51.180.43 (193.51.180.43)  28.050 ms xe1-0-2-paris2-rtr-131.noc.renater.fr (193.51.180.45)
 10 wide-m-root-server-2.sfinx.tm.fr (194.68.129.148)  28.308 ms 24.911 ms 25.167 ms
 11 m.root-servers.net (202.12.27.33)  21.915 ms 21.916 ms 21.904 ms
```

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

33 / 75

Multicast

- IP permet de transmettre un paquet à un destinataire unique
 - Une adresse est attribuée à une interface (et donc une machine)
 - L'*anycast* permet de délivrer à un service (mais sur une seule machine)
- Comment transmettre un paquet à un grand nombre de destinataires ?
 - Diffusion d'un flux multimédia
 - Mise à jour de cache
 - ...
- Utilisation du *multicast*
 - Définition d'une plage d'adresses
 - IPv4 224.0.0.0/4
 - IPv6 ff00::/8
 - Politique de routage spécifique
 - Les paquets doivent être dupliqués

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

34 / 75

Le protocole IP

1 Introduction

2 L'adressage IPv4

3 L'adressage IPv6

4 Anycast et multicast

5 Le protocole IP

- Le paquet IPv4
- Le champ *Type Of Service* TOS
- Les options IPv4
- La commutation et le routage IP
- Manipulation
- MTU, fragmentation/réassemblage

6 Quizz

6 Le protocole ICMP

7 Les protocoles ARP et RARP

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

35 / 75

Le protocole IP

- IPv4 [?] défini en 1981
 - À l'œuvre depuis 1983 !
 - Pas de gestion de congestion
 - Extrêmement simple
- Milieu des années 1990, propositions d'évolutions
 - IPng, ...
- IPv6 [?][?][?]
 - Espace d'adressage plus vaste
 - Entête plus simple
 - Configuration automatique
 - Mobilité
 - Sécurité, qualité de service mieux intégrées

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

36 / 75

Le paquet IPv4

Version	IHL	TOS	Length	
Identification			Flags	Offset
TTL	Protocol	Checksum		
Source address				
Destination address				
Options				Padding
Data				

Format de l'en-tête

Version 4 ...
IHL IP Header Length (en mots de 32 bits)
TOS Voir plus loin
Length Taille totale en octets
Identification Voir plus loin
Flags Voir plus loin
Offset Voir plus loin
TTL Time To Live
Protocol Identification de la charge utile
Checksum Contrôle de l'en-tête
Source address Adresse de l'émetteur
Destination address Adresse du destinataire
Options Voir plus loin
Data Charge utile

Le champ *Type Of Service* TOS

precedence	D	T	R	M	0
------------	---	---	---	---	---

precedence Plus utilisé

D Pour minimiser le délai

T Pour maximiser le débit

R Pour maximiser la fiabilité

M Pour minimiser le coût [?]

Remplacé par le DSCP DiffServ [?] et ECN [?]

Les options IPv4

Format général

copy	class	number	option length	option data	...
------	-------	--------	---------------	-------------	-----

copy Copiée ou non en cas de fragmentation

class Contrôle, débogage, métrologie, ...

number Identifie l'option dans sa classe

Exemples

- Record route
- Loose source routing
- Strict source routing
- Timestamp
- Security
- Stream Id
- Traceroute [?]

Le routage par la source

- Routage strict ou lâche (0x87 ou 0x83)
- Faible capacité
- Rarement utilisé
- Faille de sécurité

La commutation et le routage IP

- Paquet entrant
 - Commutation vers quelle voie de sortie ?
- Mode paquet
 - C'est du routage
- Fondé sur une table de routage
 - IP n'a pas la charge de la construction
 - Reporté dans le plan de contrôle

Bilan : mécanisme IP très simple, virtuellement aussi efficace que X.25

Notion de table de routage

Une table de routage c'est

- Un ensemble de routes

Une route, c'est

- Une destination (adresse IP et masque)
- Une interface de sortie
- Éventuellement un prochain routeur

Exemple de table de routage

Observation de la table sur un système Unix

Routing tables					
Destination	Gateway	Genmask	Flags	...	Interface
127.0.0.1	127.0.0.1	255.0.0.0	UH	...	lo0
193.54.120.0	192.70.110.93	255.255.255.0	UG	...	le0
default	192.70.110.97	0.0.0.0	UG	...	le0
192.70.110.128	192.70.110.94	255.255.255.192	UG	...	le0
192.70.110.64	0.0.0.0	255.255.255.192	U	...	le0
192.93.254.0	192.70.110.94	255.255.255.0	UG	...	le0
192.70.110.129	0.0.0.0	255.255.255.255	UH	...	ppp0

Manipulation (Linux net tools)

Consultation de la table

```
# route
```

```
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 192.168.246.2 0.0.0.0 UG 0 0 0 eth0
192.168.246.0 * 255.255.255.0 U 1 0 0 eth0
```

Ajout d'une route

```
# route add -net 192.168.125.0/24 gw 192.168.246.2
```

Suppression d'une route

```
# route del -net 192.168.125.0/24 gw 192.168.246.2
```

Manipulation (iproute2)

Consultation

```
# ip route
```

```
default via 192.168.246.2 dev eth0 proto static
192.168.246.0/24 dev eth0 proto kernel scope link src 192.168.246.136 metric 1
```

Ajout d'une route

```
# ip route add 192.168.125.0/24 via 147.127.240.23
```

Suppression d'une route

```
# ip route del 192.168.125.0/24 via 147.127.240.23
```

Algorithme

Principe de la recherche

- Recherche d'une route vers l'adresse *exacte* de destination du paquet
 - Si trouvée, émission *via* cette route
- Recherche d'une route vers le plus petit réseau contenant l'adresse
 - Si trouvée, émission *via* cette route
- Recherche d'une route par défaut
 - Si trouvée, émission *via* cette route
- Destruction du paquet
 - Et émission d'un message ICMP

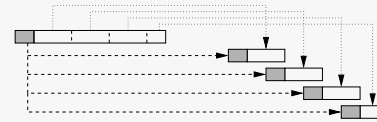
MTU, fragmentation/réassemblage

- Chaque couche liaison est caractérisée par une MTU
 - *Maximum Transmission Unit*, taille maximale d'un paquet
- En émission, cette taille est connue
 - Paramètre de l'interface
- Sur un routeur
 - Problème si MTU de sortie > MTU d'arrivée
 - Fragmentation du paquet en paquets plus petits (*fragments*)
 - Interdite par le bit *DF* (*Don't Fragment*)
- Sur le récepteur
 - Réception des fragments
 - Réassemblage du paquet d'origine

Fragmentation et réassemblage : qui s'en charge ?

- Fragmentation
 - Uniquement sur les routeurs (voir ci-dessus)
 - Eventuellement fragmentation de fragments
- Réassemblage
 - Uniquement sur le récepteur
 - Relativement coûteux
 - [?]

Construction des fragments



- Un fragment est un paquet
- Ordre fourni par Offset
- Paquet incomplet
 - Utilisation du bit MF (*More Fragment*)
- Nécessité d'un identifiant
 - Utilisation du Fragment Id

Réassemblage

- Attente de l'ensemble des fragments
 - Utilisation de timers
- Arrivée potentiellement dans le désordre
 - Besoin de réordonner
- Taille inconnue
 - Gestion *dynamique* de la mémoire

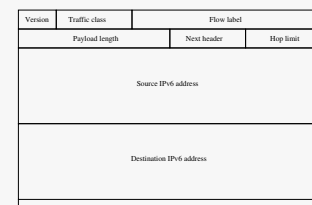
Quel avenir pour la fragmentation ?

- La fragmentation est un mal nécessaire [1]
 - Coûteux
 - Inefficace
- Apparition du PMTUD [?]
- Pas de fragmentation dans IPv6

Le *Path MTU Discovery*

- Notion de *Path MTU*
 - MTU du chemin
 - Minimum des MTU
- Découverte de proche en proche
 - Utilisation du bit DF (*Don't Fragment*)
 - Messages ICMP
- Symptôme de la schizophrénie de la pile IP

Le paquet IPv6



- Version : 6!
- Traffic class : pour la qualité de service
- Flow label : pas utilisé ...
- Payload length : volume de la charge utile
- Next header : type du contenu (N-SAPI)
- Hop limit : équivalent au TTL

Quizz

Un paquet IP envoyé par A à B contient

- 1 l'adresse de A et celle de B
- 2 l'adresse de B
- 3 un numéro de connexion

Un paquet IPv4 trop gros

- 1 ça n'existe pas
- 2 doit être "coupé"
- 3 n'arrivera jamais à destination

Un paquet fragmenté est rassemblé

- 1 par le prochain routeur
- 2 par son destinataire
- 3 jamais

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

55 / 75

Le protocole ICMP

1 Introduction

2 L'adressage IPv4

3 L'adressage IPv6

4 Anycast et multicast

5 Le protocole IP

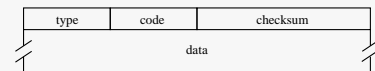
6 Le protocole ICMP

- Format d'un message ICMPv4
- Echo request/reply
- Timestamp request/reply
- Destination unreachable

- Route discovery
- Redirect
- Time exceeded
- Parameter problem
- Source quench
- ICMPv6
- Quizz

7 Les protocoles ARP et RARP

Format d'un message ICMPv4



- Différents types
 - Echo request
 - Destination unreachable
 - ...
- Parfois plusieurs codes
 - Host unreachable
 - Network unreachable
 - ...
- Somme de contrôle sur le message
- Données optionnelles

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

57 / 75

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

56 / 75

Echo Request/Reply

0x08/0x00	0x00	checksum
identifiant	sequence number	
Data		

- Test minimaliste de la pile IP
- Mesure du RTT
 - Etampille dans les données
- Utilisé par ping et traceroute

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

59 / 75

Timestamp request/reply

0x13/0x14	0x00	checksum
identifiant	sequence number	
originate timestamp		
receive timestamp		
transmit timestamp		

- Dates "absolues"
 - En millisecondes depuis minuit GMT
- Calcul de délai, de RTT

Chaput Emmanuel

La couche réseau de la pile IP

2024-2025

60 / 75

Destination unreachable

0x03	code	checksum
0		
IP header + 8 bytes		

- Rarement utile pour IP
- ICMP de IP à IP
 - Nécessité de l'en-tête

Les variantes de Destination Unreachable

- net unreachable** Réseau inaccessible, code 0x00
- host unreachable** Hôte inaccessible, code 0x01
- protocol unreachable** Protocole inaccessible, code 0x02
- port unreachable** Port inaccessible, code 0x03
- fragmentation needed and DF set** Fragmentation nécessaire pour un paquet dont le bit DF est positionné, code 0x04
- source route failed** Échec du routage par la source, code 0x05
- destination network unknown** Réseau de destination inconnu, code 0x06 (obsolète [?])

Les variantes de Destination Unreachable (suite)

- destination host unknown** Hôte destination inconnu, code 0x07
- source host isolated** Hôte source isolé, code 8 (ne semble jamais avoir été clairement défini(ssable) ? Obsolète [?])
- network administratively prohibited** Accès au réseau interdit par l'administrateur, code 9
- host administratively prohibited** Accès à la machine cible impossible ("pare-feu")
- network unreachable for TOS** Réseau inaccessible avec ce champ TOS
- host unreachable for TOS** Hôte inaccessible avec ce champ TOS
- communication administratively prohibited** Communication impossible du fait d'un "pare-feu"

Mask request/reply

0x17/0x18	0x00	checksum
identifiant		sequence number
netmask		

- Permet de découvrir le masque associé au réseau
- Utile au démarrage de la machine
- Rendu obsolète par DHCP
- [?]

Route discovery

0x0a	0x00	checksum
0x00		0x00
0x09	0x00	checksum
number	size	lifetime
router		
preference		

- Configuration automatique des tables de routage des machines
- Requête au démarrage
- Rendu obsolète par DHCP
- [?]

Redirect

0x05	code	checksum
gateway address		
IP header + 8 bytes		

- En cas d'erreur de configuration
- Rediriger les paquets pour
 - Le réseau
 - L'hôte
 - ...

Time exceeded

0x0b	code	checksum
unused		
IP header + 8 bytes		

- TTL passe à 0
 - Code 0
 - Émis par un routeur
- Réassemblage impossible
 - Code 1
 - Émis par le destinataire

Parameter problem

0x0c	code	checksum
pointer	unused	
IP header + 8 bytes		

- Problème de compréhension d'un paramètre
- Option inconnue
- Utilité ?

Source quench

0x04	code	checksum
unused		
IP header + 8 bytes		

- Émis par un routeur saturé
- Forme de *Backward ECN*
- Permet le contrôle de congestion

ICMPv6

- Très similaire à ICMPv4
- Défini dans [?]
- Attribution d'adresse sans état
 - Sollicitation diffusée par l'hôte
 - Préfixe fourni par un serveur
- Intègre l'équivalent d'ARP
 - Neighbor Discovery [?]
 - Version sécurisée [?]
- Gestion du multipoint
 - Multicast Listener Discovery [?] [?]
- Gestion de la mobilité [?]

Quizz

Sans le protocole ICMP, le protocole IP

- 1 fonctionnerait mieux
- 2 pourrait fonctionner presque aussi bien
- 3 ne fonctionnerait pas

On peut envoyer un paquet IP

- 1 dès qu'on a ouvert une connexion grâce à ICMP
- 2 uniquement tant qu'on n'a pas reçu de message ICMP l'interdisant
- 3 quand on veut

Un message ICMP est transmis

- 1 dans un segment TCP
- 2 dans un paquet IP
- 3 dans une trame ethernet

Les protocoles ARP et RARP

- 1 Introduction
- 2 L'adressage IPv4
- 3 L'adressage IPv6
- 4 Anycast et multicast
- 5 Le protocole IP
- 6 Le protocole ICMP
- 7 Les protocoles ARP et RARP
 - Exemples

Les protocoles ARP et RARP

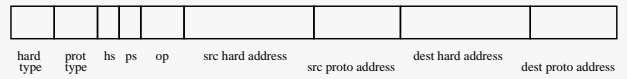
Address Resolution Protocol

- Correspondance adresse IP vers adresse MAC
- Réponse de l'intéressé
- Mise en place d'un cache
- [?]

Reverse Address Resolution Protocol

- Correspondance adresse MAC vers adresse IP
- Réponse d'un serveur
- [?]

Les messages ARP et RARP



- Opération
 - Requête/réponse
 - ARP/RARP
- Adresses source et destination
 - Vis à vis du message
 - Permutation entre requête et réponse
- Théoriquement indépendant ...

Emission d'une requête ARP

• Envoi avec Scapy

```
>>> req = Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst="147.127.240.161")
>>> req.summary()
'Ether / ARP who has 147.127.240.161 says 147.127.240.145'
>>> rep,non=arp(req,timeout=2)
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
>>> ans.summary()
Ether / ARP who has 147.127.240.161 says 147.127.240.145 --> Ether / ARP is at 00:25:64:a2:06:b3
says 147.127.240.161 / Padding
>>>
```

• Observation de la table

```
$ arp -a
bladerunner.enseeiht.fr (147.127.240.231) at 84:2b:2b:b7:f2:e9 [ether] on eth0
futunafw.enseeiht.fr (147.127.240.201) at 00:50:56:24:02:01 [ether] on eth0
routeurfw-240.enseeiht.fr (147.127.240.200) at 00:50:56:24:02:01 [ether] on eth0
```

• Suppression d'une entrée de la table

```
# arp -d 147.127.240.201
```

• Observation par Wireshark

```
15:13:49.800504 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 147.127.240.200
tell 147.127.240.145, length 28
15:13:49.801336 ARP, Ethernet (len 6), IPv4 (len 4), Reply 147.127.240.145
is-at 28:18:78:fc:53:5a, length 28
```

[1] Christopher A. Kent and Jeffrey C. Mogul.
Fragmentation considered harmful.
SIGCOMM Comput. Commun. Rev., 25(1) :75–87, January 1995.