

La couche réseau de la pile IP

Chaput Emmanuel



2016-2017



Notes :

Plan

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

Notes :

Introduction

- 1 Introduction

Notes :

Introduction

- Le cœur de la pile [11]
- 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"

Notes :

L'adressage IPv4

- 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

Notes :

L'adressage IPv4

Identification des entités de niveau 3

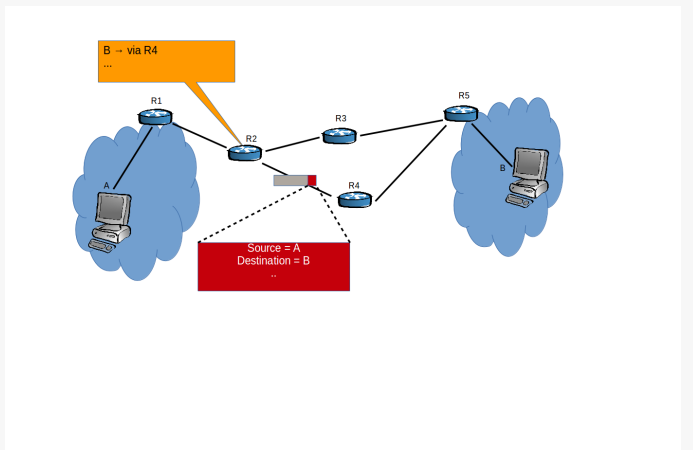
- Individuelle (hôte) et collective (réseau)
- Correspondance éventuelle avec la couche inférieure
- Besoin d'unicité et uniformité dans le réseau
 - Gestion centralisée
- Par exemple, l'adresse du destinataire figure dans un paquet

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, ...

Notes :

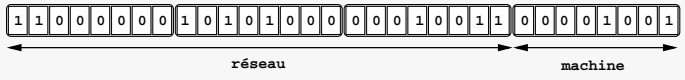
Fonctions de l'adresse



Notes :

L'adressage IPv4

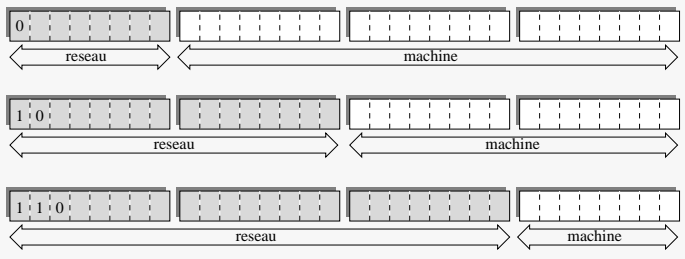
- Format
 - Quatre octets (32 bits)
 - 4 294 967 296 valeurs (théoriquement)
- Notation traditionnelle
 - Décimale pointée
 - aaa.bbb.ccc.ddd
- Exemples
 - 192.168.13.1
 - 147.127.18.98



Notes :

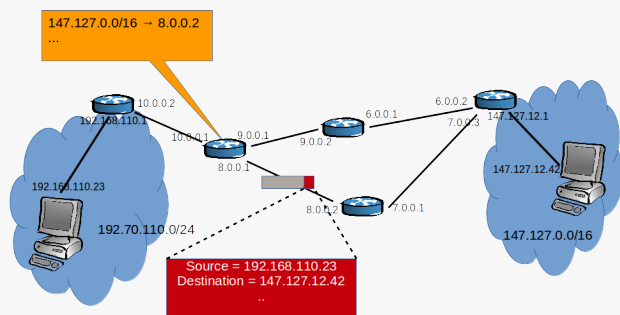
Les classes d'adresses IPv4

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



Notes :

Fonctions de l'adresse IPv4



Notes :

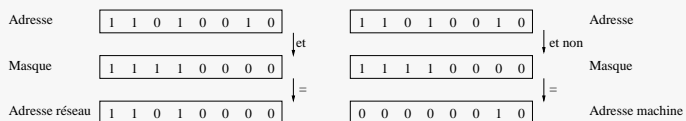
Sous-réseaux IP

- 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 [19][21]
 - Délimitation plus libre entre la partie réseau et la partie machine d'une adresse

Notes :

Le netmask

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



Notes :

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 [27]

Notes :

L'attribution des adresses IPv4

- Affectation hiérarchique
 - Plus haut niveau : IANA et ses RIRs
 - Fournisseurs d'accès
 - Administrateur du réseau
- Possibilité d'utiliser des adresses "non routables"
- Outils
 - Configuration statique
 - Commande `ifconfig` ou équivalent
 - Fichier de configuration
 - Configuration dynamique
 - Protocole DHCP ou équivalent
 - Possibilité de ré-affectation

Notes :

Classless Inter Domain Routing

Pourquoi CIDR [12] [13] ?

- 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

Notes :

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



Notes :

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

Notes :

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
```

Notes :

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
```

Notes :

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
```

Notes :

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,LOWER_UP> 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  
valid_lft 2591712sec preferred_lft 604512sec  
inet6 fe80::5e26:aff:fe19:fb5f/64 scope link  
valid_lft forever preferred_lft forever
```

Notes :

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 siyuca.leei.enseeiht.fr.

;; ADDITIONAL SECTION:
ns1.enseeiht.fr. 86400 IN A 147.127.176.22
siyuca.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::1:2

;; 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
```

Notes :

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

Notes :

L'adressage IPv6

- 3 L'adressage IPv6
 - L'attribution des adresses IPv6

Notes :

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

Notes :

Utilisation des adresses IPv6

D'après [14]

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 [15]

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

Notes :

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

Notes :

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

Notes :

Le protocole IP

- 4 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
 - Le protocole IPv6
 - Quizz

Notes :

Le protocole IP

- IPv4 [11] défini en 1981
 - À l'œuvre depuis 1983 !
 - Pas de gestion de congestion
 - Extrêmement simple
- Milieu des années 1990, propositions d'évolutions
 - IPng, ...
- IPv6 [9][14][5]
 - Espace d'adressage plus vaste
 - Entête plus simple
 - Configuration automatique
 - Mobilité
 - Sécurité, qualité de service mieux intégrées

Notes :

Le paquet IPv4

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

Notes :

Format de l'en-tête

Version	4 ...
IHL	IP Header Length (en mots de 32 bits)
TOS	<i>Voir plus loin</i>
Length	Taille totale en octets
Identification	<i>Voir plus loin</i>
Flags	<i>Voir plus loin</i>
Offset	<i>Voir plus loin</i>
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	<i>Voir plus loin</i>
Data	Charge utile

Notes :

Le champ *Type Of Service* TOS

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

precedence Plus utilisé

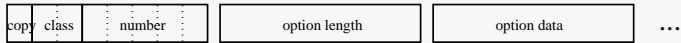
- D** Pour minimiser le délai
- T** Pour maximiser le débit
- R** Pour maximiser la fiabilité
- M** Pour minimiser le coût [1]

Remplacé par le DSCP DiffServ [23] et ECN [26]

Notes :

Les options IPv4

Format général



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 [18]

Notes :

Le routage par la source

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

Notes :

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

Notes :

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

Notes :

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
```

Notes :

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
```

Notes :

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
```

Notes :

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

Notes :

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 \neq 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

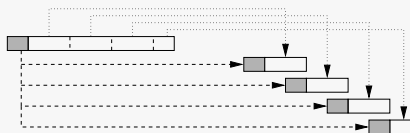
Notes :

Fragmentation et réassemblage : où ?

- Fragmentation
 - Uniquement sur les routeurs (voir ci-dessus)
 - Éventuellement fragmentation de fragments
- Réassemblage
 - Uniquement sur le récepteur
 - Relativement coûteux
 - [4]

Notes :

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`

Notes :

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

Notes :

Quel avenir pour la fragmentation ?

- La fragmentation est un mal nécessaire [17]
 - Coûteux
 - Inefficace
- Apparition du PMTUD [20]
- Pas de fragmentation dans IPv6

Notes :

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

Notes :

Le paquet IPv6

Version	Traffic class	Flow label	
	Payload length	Next header	Hop limit
Source IPv6 address			
Destination IPv6 address			

- 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

Notes :

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

Notes :

Le protocole ICMP

5 Le protocole ICMP

- Format d'un message ICMPv4
- Echo request/reply
- Timestamp request/reply
- Destination unreachable
- Mask request/reply
- Route discovery
- Redirect
- Time exceeded
- Parameter problem
- Source quench
- ICMPv6
- Quizz

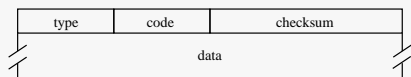
Notes :

Le protocole ICMP

- *Internet Message Control Protocol* [25]
- Plan de contrôle de IP
- Messages véhiculés par IP
- Communication entre entités IP

Notes :

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

Notes :

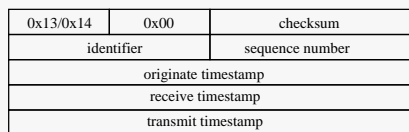
Echo Request/Reply



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

Notes :

Timestamp request/reply



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

Notes :

Destination unreachable

0x03	code	checksum
0		
IP header + 8 bytes		

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

Notes :

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 [3])

Notes :

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 [3])
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"

Notes :

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
- [21]

Notes :

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
- [7]

Notes :

Redirect

0x05	code	checksum
gateway address		
IP header + 8 bytes		

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

Notes :

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

Notes :

Parameter problem

0x0c	code	checksum
pointer	unused	
IP header + 8 bytes		

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

Notes :

Source quench

0x04	code	checksum
unused		
IP header + 8 bytes		

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

Notes :

- Très similaire à ICMPv4
- Défini dans [6]
- Attribution d'adresse sans état
 - Sollicitation diffusée par l'hôte
 - Préfixe fourni par un serveur
- Intègre l'équivalent d'ARP
 - Neighbor Discovery [22]
 - Version sécurisée [2]
- Gestion du multipoint
 - Multicast Listener Discovery [8] [28]
- Gestion de la mobilité [16]

Notes :

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

Notes :

Les protocoles ARP et RARP

- 6 Les protocoles ARP et RARP
 - Exemples

Notes :

Les protocoles ARP et RARP

Address Resolution Protocol

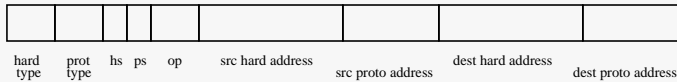
- Correspondance adresse IP vers adresse MAC
- Réponse de l'intéressé
- Mise en place d'un cache
- [24]

Reverse Address Resolution Protocol

- Correspondance adresse MAC vers adresse IP
- Réponse d'un serveur
- [10]

Notes :

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 ...

Notes :

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,nonans=rp(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 00:125:64: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
```

Notes :

- [1] [P. Almquist](#).
RFC 1349 : Type of service in the internet protocol suite.
Standard track, IETF, July 1992.
- [2] [Ed. Arkko, J. Kempf, B. Zill, and P. Nikander](#).
Secure neighbor discovery (SEND).
RFC 3971, Internet Engineering Task Force, March 2005.
- [3] [F. Baker](#).
Requirements for IP Version 4 Routers.
RFC 1812 (Proposed Standard), June 1995.
Updated by RFCs 2644, 6633.
- [4] [D. Clark](#).
IP datagram reassembly algorithms.
RFC 815, Internet Engineering Task Force, July 1982.
- [5] [A. Conta and S. Deering](#).
Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6).
RFC 1885, Internet Engineering Task Force, December 1995.

Notes :

- [6] [A. Conta and S. Deering](#).
Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification.
RFC 2463, Internet Engineering Task Force, December 1998.
- [7] [S. Deering](#).
RFC 1256 : Icmp router discovery messages.
Technical report, IETF, September 1991.
- [8] [S. Deering, W. Fenner, and B. Haberman](#).
Multicast listener discovery (MLD) for ipv6.
RFC 2710, Internet Engineering Task Force, October 1999.
- [9] [S. Deering and R. Hinden](#).
Internet protocol, version 6 (ipv6) specification.
RFC 1883, Internet Engineering Task Force, December 1995.
- [10] [R. Finlayson, T. Mann, J. Mogul, and M. Theimer](#).
Reverse address resolution protocol.
RFC 903, Internet Engineering Task Force, June 1984.

Notes :

- [11] [The Ingeniering Task Force](#).
RFC 791 : Internet protocol.
Technical report, IETF, 1981.
- [12] [V. Fuller, T. Li, J. Yu, and K. Varadhan](#).
RFC 1338 : Supernetting : an address assignment and aggregation strategy.
Informational, IETF, June 1992.
- [13] [V. Fuller, T. Li, J. Yu, and K. Varadhan](#).
RFC 1519 : Classless inter-domain routing (CIDR) : an address assignment and aggregation strategy.
Proposed standard, IETF, September 1993.
- [14] [R. Hinden, S. Deering, and Edson Ursini](#).
IP version 6 addressing architecture.
RFC 1884, Internet Engineering Task Force, December 1995.
- [15] [R. Hinden and B. Haberman](#).
Unique Local IPv6 Unicast Addresses.

Notes :

Technical Report 4193, "Internet Engineering Task Force", October 2005.

- [16] D. Johnson, C. Perkins, and J. Arkko.
Mobility support in ipv6.
RFC 3775, Internet Engineering Task Force, June 2004.
- [17] Christopher A. Kent and Jeffrey C. Mogul.
Fragmentation considered harmful.
SIGCOMM Comput. Commun. Rev., 25(1) :75–87, January 1995.
- [18] G. Malkin.
Traceroute using an IP option.
RFC 1393, Internet Engineering Task Force, January 1993.
- [19] J. Mogul.
Internet subnets.
RFC 917, Internet Engineering Task Force, October 1984.
- [20] J. Mogul and S. Deering.
RFC 1191 :path mtu discovery.
Technical report, IETF, November 1990.

Notes :

- [21] J. Mogul and J. Postel.
Internet standard subnetting procedure.
RFC 950, Internet Engineering Task Force, August 1985.
- [22] T. Narten, E. Nordmark, and W. Simpson.
Neighbor discovery for IP version 6 (ipv6).
RFC 2461, Internet Engineering Task Force, December 1998.
- [23] K. Nichols, S. Blake, F. Baker, and D. Black.
Definition of the differentiated services field (DS field) in the ipv4 and ipv6 headers.
RFC 2474, Internet Engineering Task Force, December 1998.
- [24] D. Plummer.
Ethernet address resolution protocol : Or converting network protocol addresses to 48.bit ethernet address for transmission on ethernet hardware.
RFC 826, Internet Engineering Task Force, November 1982.
- [25] J. Postel.

Notes :

RFC 792 : Internet control message protocol.
Technical report, IETF, 1981.

- [26] K. Ramakrishnan, S. Floyd, and D. Black.
The addition of explicit congestion notification (ECN) to IP.
RFC 3168, Internet Engineering Task Force, September 2001.
- [27] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear.
RFC 1918 : Address allocation for private internets.
Best current practice, Internet Engineering Task Force, February 1996.
- [28] Ed. Vida and Ed. Costa.
Multicast listener discovery version 2 (mldv2) for ipv6.
RFC 3810, Internet Engineering Task Force, June 2004.

Notes :
