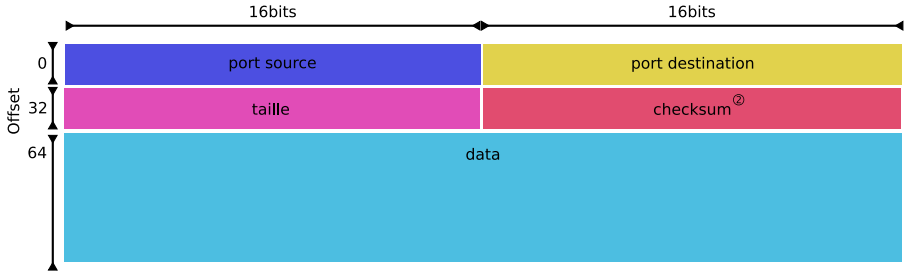
Memento IP/netfilter

Datagramme UDP① (rfc 768)



① un en-tête UDP à une taille fixe : 32 bits (8bytes)
② Le checksum est optionnel (0 si absent)

Facteurs

10^24	yotta
10^21	zetta
10^18	exa
10^15	peta
10^12	tera
10^9	giga
10^6	mega
10^3	kilo
10^2	hecto
10^1	deca
10^-1	deci
10^-2	centi
10^-3	milli
10^-6	micro
10^-9	nano
10^-12	pico
10^-15	femto
10^-18	atto
10^-21	zepto
10^-24	yocto

Protocoles IP

#	description
1	icmp
2	igmp
6	tcp
17	udp
50	esp (ipsec)
51	ah (ipsec)

Principaux ports

#/proto	description
20/tcp	ftp (data)
21/tcp	ftp (control)
22/tcp	ssh
23/tcp	telnet
25/tcp	smtp
53/any	dns
68/udp	dhcp
69/udp	tftp
80/tcp	http
110/tcp	pop
143/tcp	imap
161/udp	snmp
443/tcp	https
500/udp	isakmp
514/udp	syslog
515/tcp	printer

Subnets

CIDR	Hosts	Netmask
/30	4	255.255.255.252
/29	8	255.255.255.248
/28	16	255.255.255.240
/27	32	255.255.255.224
/26	64	255.255.255.192
/24	256	255.255.255.0
/23	512	255.255.254.0
/22	1024	255.255.252.0
/21	2048	255.255.248.0
/20	4096	255.255.240.0
/19	8192	255.255.224.0
/18	16384	255.255.192.0
/17	32768	255.255.128.0
/16	65536	255.255.0.0

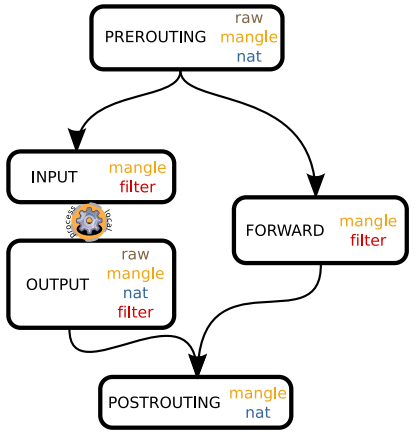
Cibles

(returning/non-returning)

ACCEPT	accepte
DROP	ignore
REJECT	rejet (icmp|udp)
LOG	syslog
SNAT	source nat
DNAT	destination nat
MARK	marque le paquet
MASK	masquerading

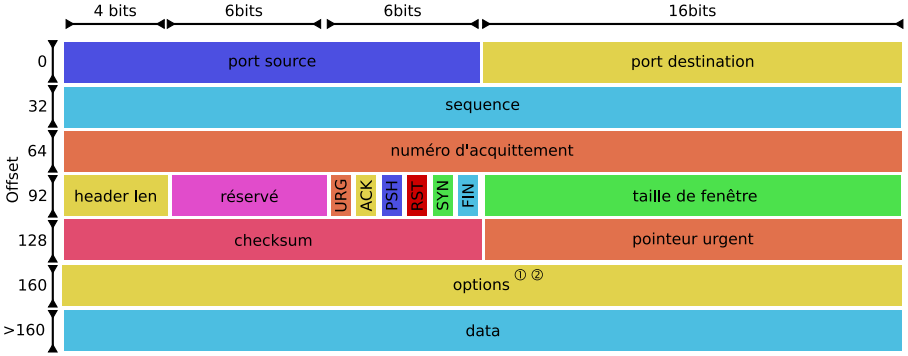
netfilter 2.6.x

tables : raw, mangle, nat, filter
chaînes : PREROUTING INPUT OUTPUT FORWARD POSTROUTING

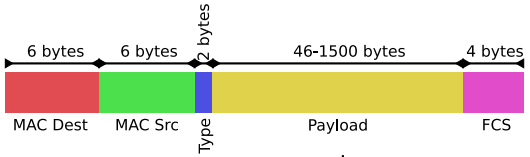


Segment TCP (rfc 793)

① Les options sont... optionnelles
② Padding sur 32 bits



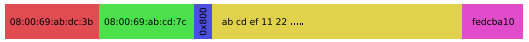
Trame Ethernet II (rfc 894, a.k.a. DIX)



OUI
00:11:22:33:44:55
MAC Address

Ethernet Types

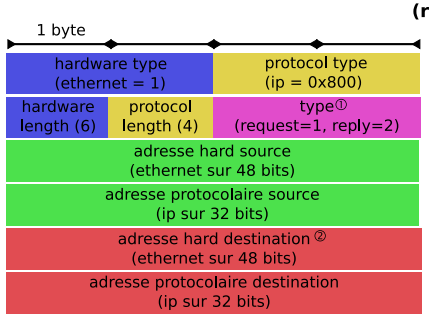
0800	IP
0806	ARP
809B	AppleTalk
8137	IPX/SPX



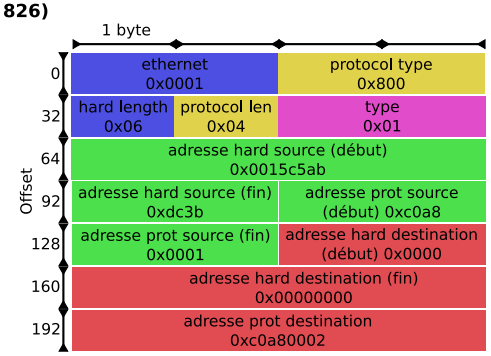
Principaux types et codes ICMP

type	code	description
0	0	echo reply
3	0	network unreachable
3	1	host unreachable
3	2	protocol unreachable
3	3	port unreachable
3	4	frag needed but DF bit set
3	5	source route failed
3	6	destination network unknown
3	7	destination host unknown
3	9	dest. net. administratively prohibited
3	10	dest. net. administratively prohibited
3	11	net. unreachable for TOS
3	12	host unreachable for TOS
4	0	source quench
5	0	redirect for network
5	1	redirect for host
5	2	redirect for TOS and network
5	3	redirect for TOS and network
8	0	echo request
11	0	TTL exceeded in transit
11	1	TTL exceeded during reassembly
12	0	bad IP header

Paquet arp (rfc 826)



exemples pour Ethernet / IP



exemples de requête ARP depuis 192.168.0.1 pour 192.168.0.2

① RARP Request (2), RARP Reply (3)
② Zéros pour une requête (type=1)

Paquet IPv4 (rfc 791)

① Les options sont... optionnelles
② Padding sur 32 bits