

Le paquet IP & ICMP

UE LU3IN033 Réseaux
2021-2022

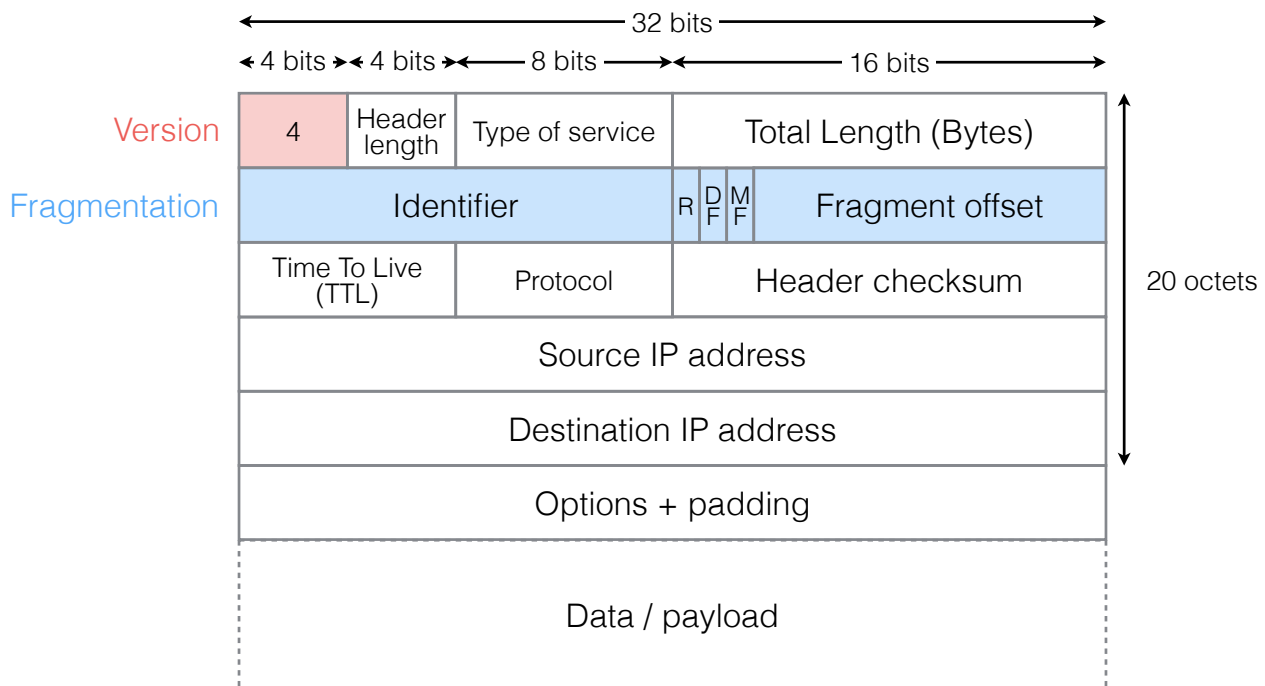
Prométhée Spathis
promethee.spathis@sorbonne-universite.fr



Plan du cours

- Entête du paquet IP
 - Champs de la partie fixe
 - Partie variable : IP options
 - Contrôle d'erreur et boucles de routage
- Longueur d'un paquet IP
 - Taille maximale
 - Fragmentation
- Charge utile du paquet IP
 - Protocoles encapsulés
- Protocole ICMP
 - Tests et diagnostic d'erreurs
 - ping et traceroute

Paquet IPv4



3

Version, Header, ToS

- Version (4 bits)
 - Indique la version du protocole IP
 - Nécessaire pour déterminer la structure de l'entête du paquet
 - Valeurs courantes : "4" (pour IPv4) et "6" (pour IPv6)
- Header length (4 bits)
 - Taille de l'entête exprimée en nombre de mots de 32 bits (4 octets)
 - La valeur "5" (0101) indique une taille de 20 octets (pas d'option IP)
 - La valeur max "15" (1111) indique qu'il y a 40 octets d'options IP
- TOS Type-of-Service (8 bits)
 - Type de chemin sur lequel acheminer le paquet
 - Priorité du paquet par rapport aux autres paquets vus par le routeur
 - Délai faible (transfert audio/video), capacité élevée (téléchargement)

4

IHL, Fragments, TTL

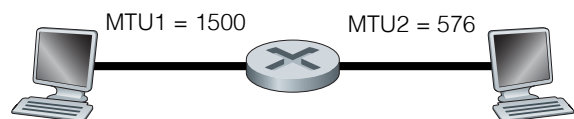
- Total length (16 bits)
 - Taille totale théorique du paquet exprimée en octets
 - Taille max d'un paquet : 65,535 octets ($2^{16} - 1$)
 - La taille d'un paquet est limitée par la MTU
 - Maximum Transmission Unit MTU : taille max du champ données des trames utilisées par la couche liaison de données sous-jacente
- Fragmentation (32 bits) (voir transparent suivant)
 - Identifiant du paquet, drapeaux, et fragment offset
 - Permet de gérer la fragmentation d'un paquet et le réassemblage des fragments
- Time-To-Live (8 bits)
 - Limite la durée de vie des paquets capturés dans une boucle de routage
 - Correspond au nombre maximal de sauts autorisé du chemin emprunté
 - Valeur décrémentée de 1 par chacun des routeurs que traverse le paquet
 - Suppression du paquet dont le TTL = 0 (ICMP Time exceeded)

5

Fragmentation IP

MTU Maximum transmission unit : taille max du champ données des trames utilisées par la couche liaison de données sous-jacente

- Flags : 3 bits (Réservé : 0, DF, MF)
 - DF : Don't Fragment (les paquets trop grands sont rejetés)
 - MF : More Fragment (positionné si dernier fragment)
- Fragment Offset :
 - taille en octets hors entête des fragments précédant le fragment courant divisée par 8
- Exemple :
 - Données encapsulées : 1300 octets
 - Entêtes des fragments sur le réseau 2 :
 - $576 - 20 = 556$, valeur multiple de 8 la plus proche : $552 = 69 * 8$
 - F1 : offset 0 MF = 1 (taille des données : 552 octets)
 - F2 : offset 69 = $552/8$ MF = 1 (taille des données : 552 octets)
 - F3 : offset $69*2$ MF = 0 (taille des données : 196 octets)



6

Protocol, Checksum

- Protocol (8 bits)
 - Identifie le type de l'entête situé après l'entête IP
 - "1" pour ICMP
 - protocoles Transport : "6" pour TCP, "17" UDP
- Checksum (8 bits)
 - Code de détection d'erreurs portant sur l'entête
 - Vérification bout en bout :
 - la source calcule la valeur du checksum
 - le récepteur calcule le checksum sur l'entête reçu et vérifie si la valeur calculée correspond à celle reçue

7

Exemple : calcul du checksum

The diagram illustrates the structure of a network packet and its bit-level representation. On the left, a packet is shown as a sequence of fields: **entête Ethernet** (blue), **entête IP** (orange), **entête TCP** (green), and **données** (white). Below this, the hexadecimal representation of the packet is shown, with bytes grouped by field: Ethernet (08 00 20 87 b0 44 08 00 11 08 c0 63 08 00 45 00), IP (00 48 49 ba 00 00 1e 06 69 8d c1 37 33 f6 c1 37 33 04 17 70 96 d4 39 7f 84 c2 bf 3a 21 fd 50 18 11 1c 99 bc 00 00 0e 00 31 3f 02 c0 00 11 00 00 3e c1 00 00 00 11 00 00 00 02 28 28 a7 b0 80 29 ea fc 81 58 90 70). On the right, the bit-level representation of the packet is shown, with bits grouped by field and labeled with their hexadecimal values: 0x4500, 0x0048, 0x49BA, 0x0000, 0x1E06, 0x0000, 0xC137, 0x33F6, 0xC137, 0x3304, and 0x698D. A 16-bit window is indicated at the top right.

Exemple : vérification du checksum

																16 bits					
entête Ethernet				entête IP				entête TCP				données									
08	00	20	87	b0	44	08	00	11	08	c0	63	08	00	45	00	0x4500	0100	0101	0000	0000	
00	48	49	ba	00	00	1e	06	69	8d	c1	37	33	f6	c1	37	0x0048	0000	0000	0100	1000	
33	04	17	70	96	d4	39	7f	84	c2	bf	3a	21	fd	50	18	0x49BA	0100	1001	1011	1010	
11	1c	99	bc	00	00	0e	00	31	3f	02	c0	00	11	00	00	0x0000	1000	1111	0000	0010	
3e	c1	00	00	00	11	00	00	00	02	28	28	a7	b0	80	29	0x0000	0000	0000	0000	0000	
ea	fc	81	58	90	70											0x1E06	0001	1110	0000	0110	
																	1010	1101	0000	1000	
																	0x698D	0110	1001	1000	1101
																	1 0001	0110	1001	0101	
																	0xC137	1100	0001	0011	0111
																	1 1101	0111	1100	1100	
																	0x33F6	0011	0011	1111	0110
																	10 0000	1011	1100	0010	
																	0xC137	1100	0001	0011	0111
																	10 1100	1100	1111	1001	
																	0x3304	0011	0011	0000	0100
																	10 1111	1111	1111	1101	
																				10	
																				10	
																				1111 1111 1111 1111	

16 bits à 1 : entête sans erreur

9

Adresses source et destination

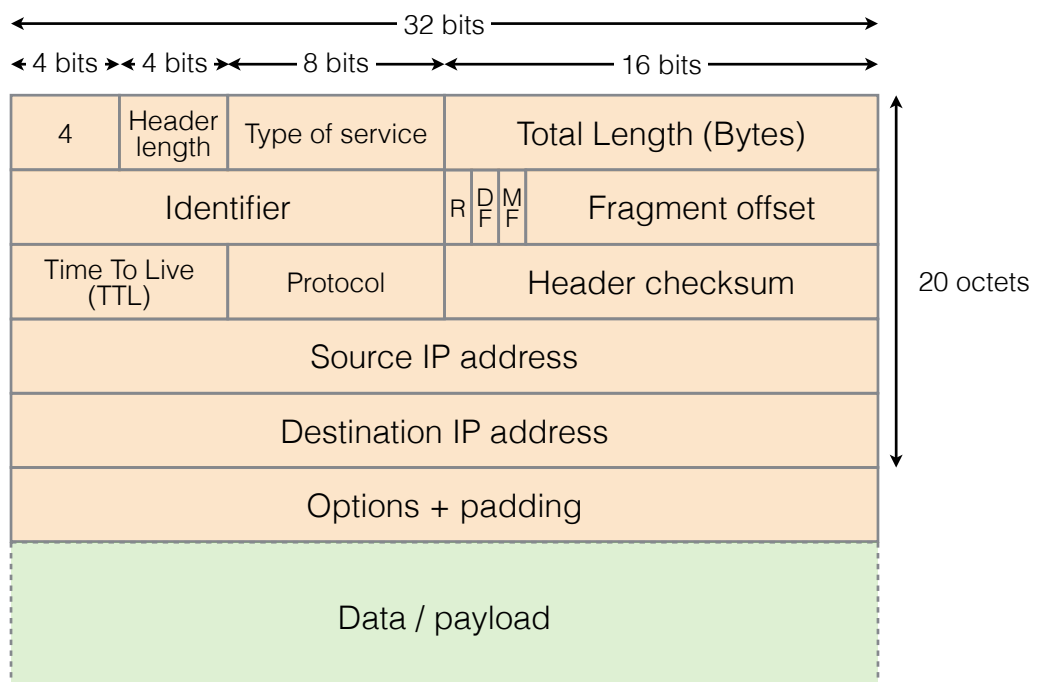
- Deux adresses IP
 - Adresse IP de la source (32 bits)
 - Adresse IP de la destination (32 bits)
- Adresse destination
 - Identifie la machine hôte destination
 - Utilisée par les routeurs pour acheminer le paquet
 - Résulte de la résolution du nom (DNS)
- Adresse source
 - Identifie la machine hôte source
 - Permet à la destination d'accepter ou de rejeter le paquet
 - Utilisée par la destination pour répondre à la source
 - Peut être usurpée
 - Configurée manuellement (administrateur) ou découverte dynamiquement (DHCP)

Exemple de trace (1)

	14 octets	$IHL * 4 = 20$ octets	$Total\ length - (IHL * 4) = 52$ octets
	entête Ethernet	entête IP	données
numéro en hexa de l'octet en début de ligne	segment TCP		
0x00	08 00 20 87 b0 44 08 00 11 08 c0 63 08 00 45 00	octets 0 à 15	
0x10	00 48 49 ba 00 00 1e 06 69 8d c1 37 33 f6 c1 37	octets 16 à 31	
0x20	33 04 17 70 96 d4 39 7f 84 c2 bf 3a 21 fd 50 18	octets 32 à 47	
0x30	11 1c 99 bc 00 00 0e 00 31 3f 02 c0 00 11 00 00	octets 48 à 63	
0x40	3e c1 00 00 00 11 00 00 00 02 28 28 a7 b0 80 29	octets 64 à 79	
0x50	ea fc 81 58 90 70	octets 80 à 85	

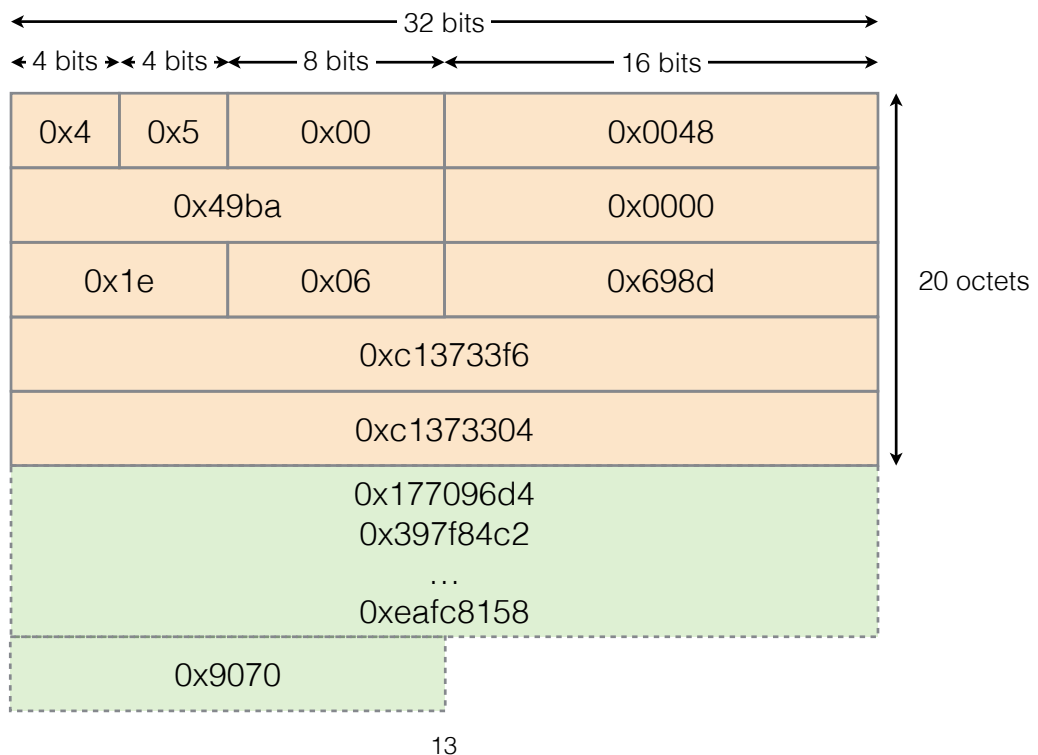
11

Paquet IPv4

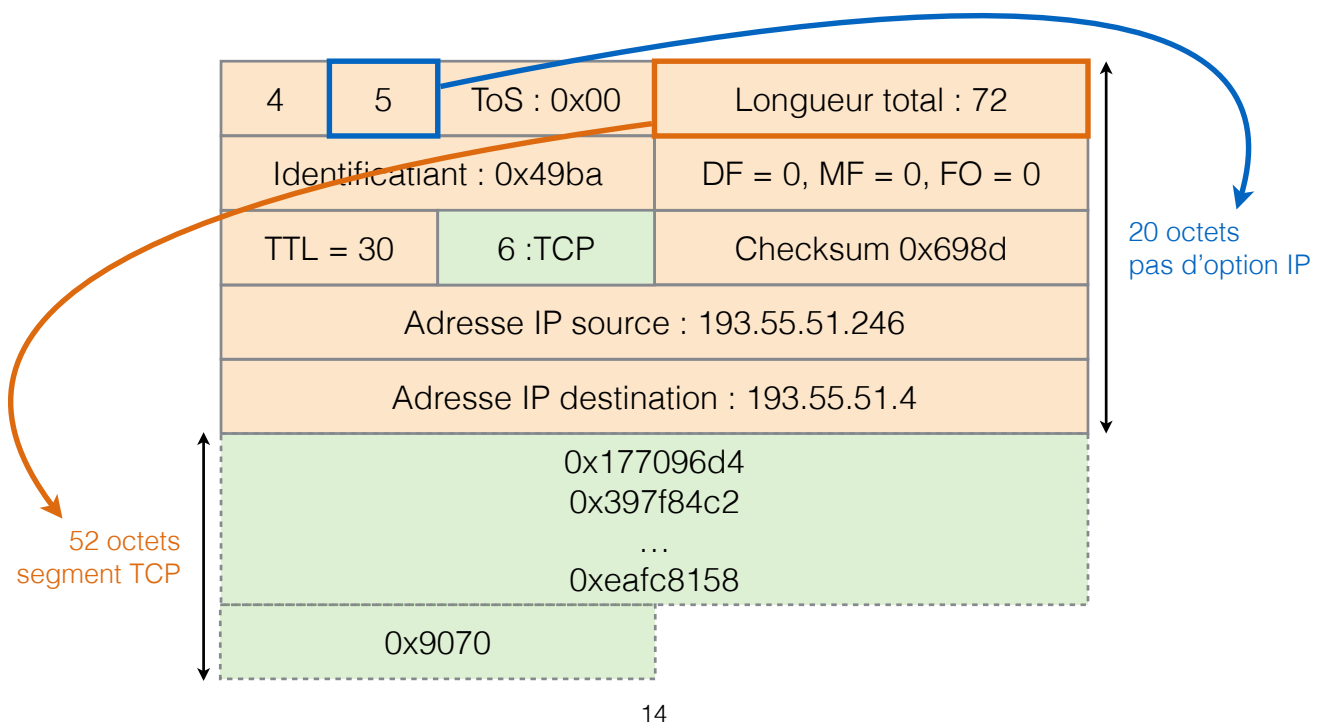


12

Exemple de trace (2)



Exemple de trace (3)



Exemple de trace (4)

- Version : 0x4 paquet IPv4
- Longueur de l'entête IP : 0x5 20 (5*4) octets
- ToS : 0x00
- Longueur totale : 0x0048 72 octets
- Identifiant : 0x49ba
- DF : 0, MF: 0, Fragment offset : 0
- TTL : 0x1e soit 30 sauts
- Protocole : 0x06 TCP (6)
- Somme de contrôle : 0x698d
- Adresse IP source : 0xc13733f6 soit 193.55.51.246
- Adresse IP destination : 0xc1373304 soit 193.55.51.4
- Données : 72 - 20 = 52 (Longueur totale - Longueur de l'entête)

15

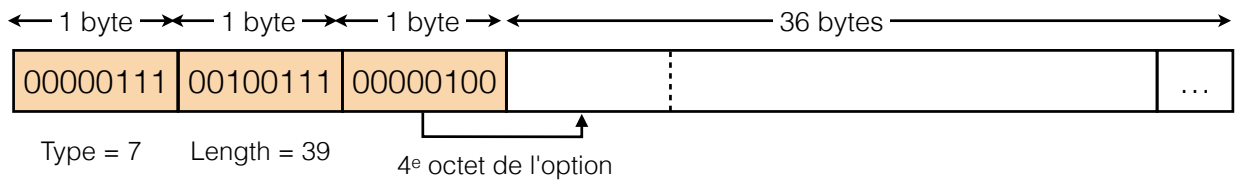
Options IP

Type	Option	Object
0	End of Options List	Used to coincide the end of the options with the end of the header according to the IHL
1	No Operation	Used to align the beginning of the subsequent option on a 32-bit boundary
7	Record Route (RR)	Used to trace the route an IP packet takes
68	Time Stamp (TS)	Used to records the time (in Universal Time) when each network device receives the packet
131	Loose Routing	Used to route the IP packet based on information supplied by the source
137	Strict Routing	Used to forward the IP packet based on information supplied by the source.

- 131 routage lâche : le paquet IP peut transiter par des routeurs intermédiaires avant d'atteindre le routeur suivant dont l'adresse est spécifiée par l'option
- 137 routage strict : le paquet IP traverse la séquence des seuls routeurs telle que spécifiée par l'option

16

Option Record Route

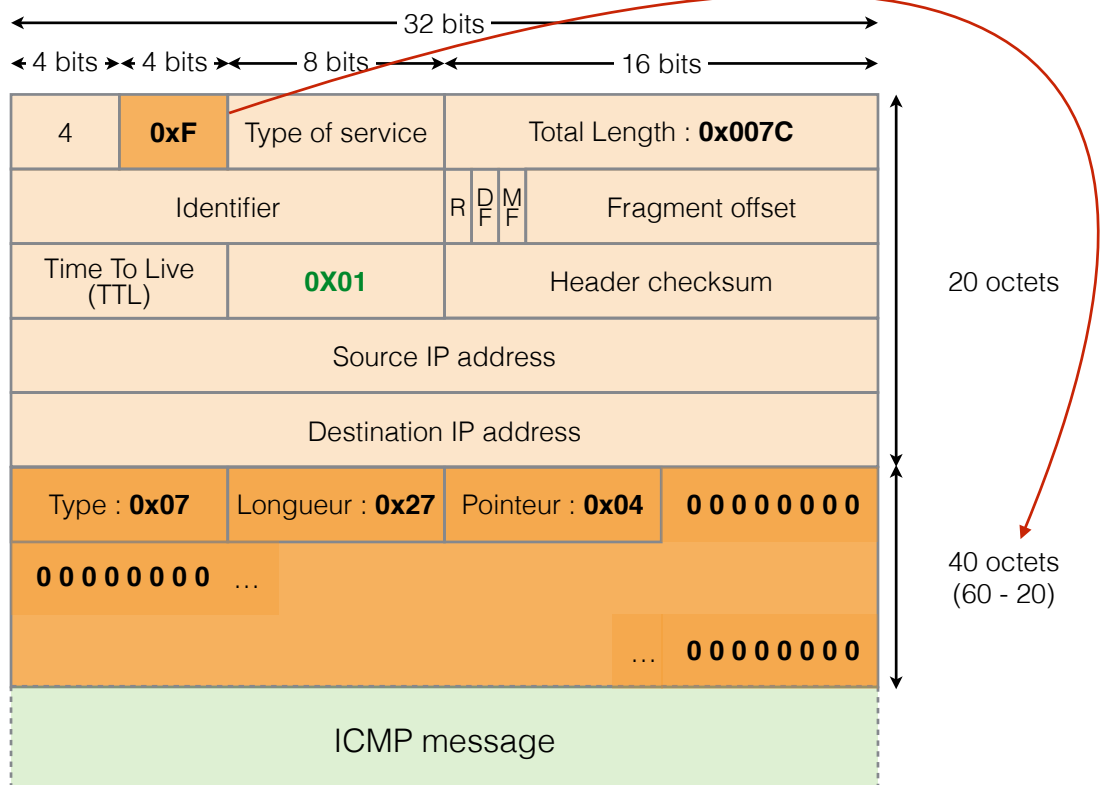


```

08 00 20 0a ac 96 08 00 20 0a 70 66 08 00 4f 00
00 7c cb c9 00 00 ff 01 b9 7f 84 e3 3d 05 c0 21
9f 06 07 27 04 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 08 00 a2 56 2f 00
00 00 29 36 8c 41 00 03 86 2b 08 09 0a 0b 0c 0d
0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d
2e 2f 30 31 32 33 34 35 36 37
    
```

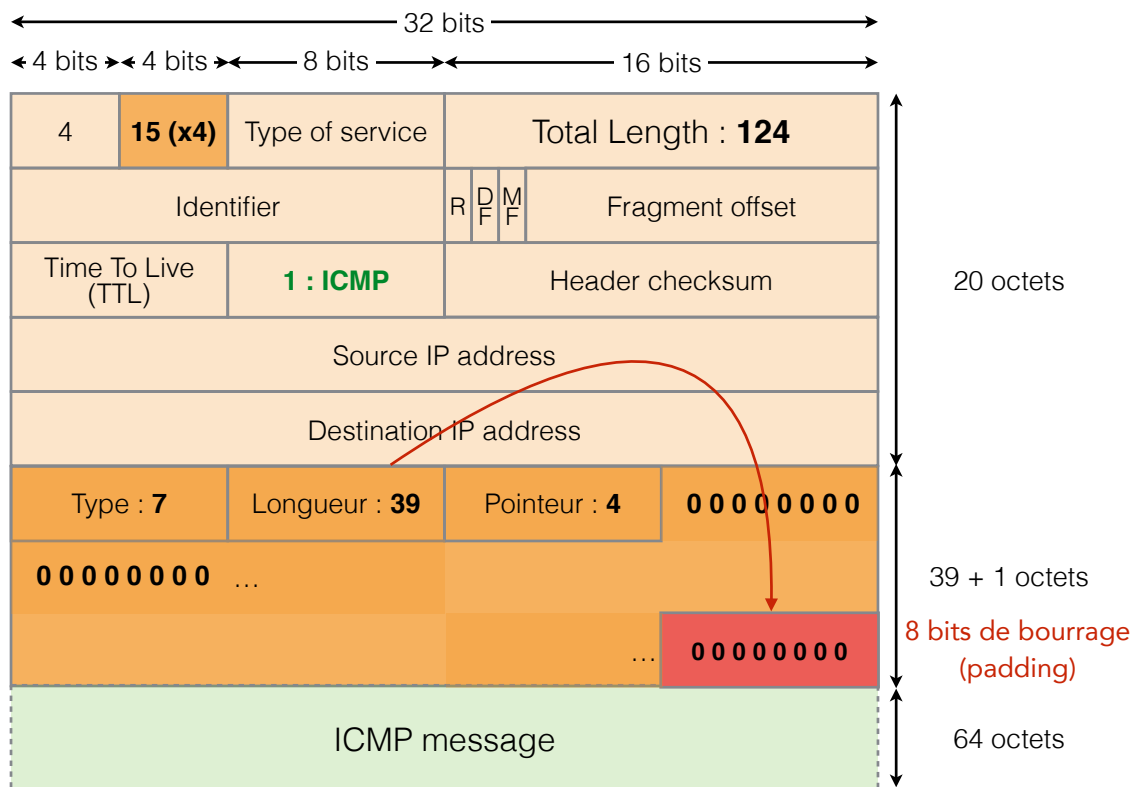
17

Paquet IPv4 avec option Record Route



18

Paquet IPv4 avec option Record Route



19

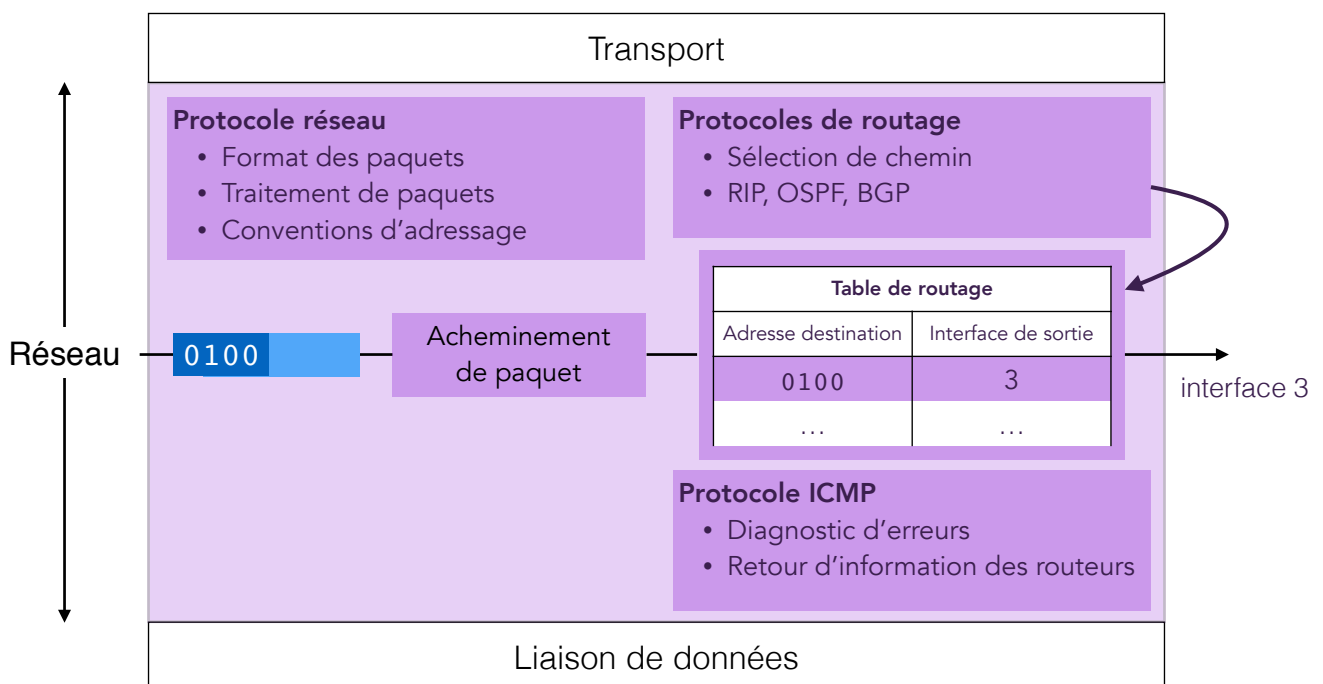
Conclusion

- Champs d'entête du paquet IP
 - les erreurs sur l'entête sont détectées par le checksum
 - les paquets en erreur sont jetés par le récepteur
 - la durée de vie d'un paquet est limitée par son TTL
 - suppression des paquets dont le TTL est nul
- Longueur d'un paquet IP
 - les paquets trop longs peuvent être :
 - fragmentés avant d'être acheminés sur une liaison avec une MTU restrictive
 - supprimés par ces même routeurs
- Charge utile du paquet IP
 - le type de l'entête encapsulé par un paquet est identifié par le champ Protocole
 - 6 : TCP, 17 : UDP, 1 : ICMP

Le protocole ICMP



Protocole ICMP

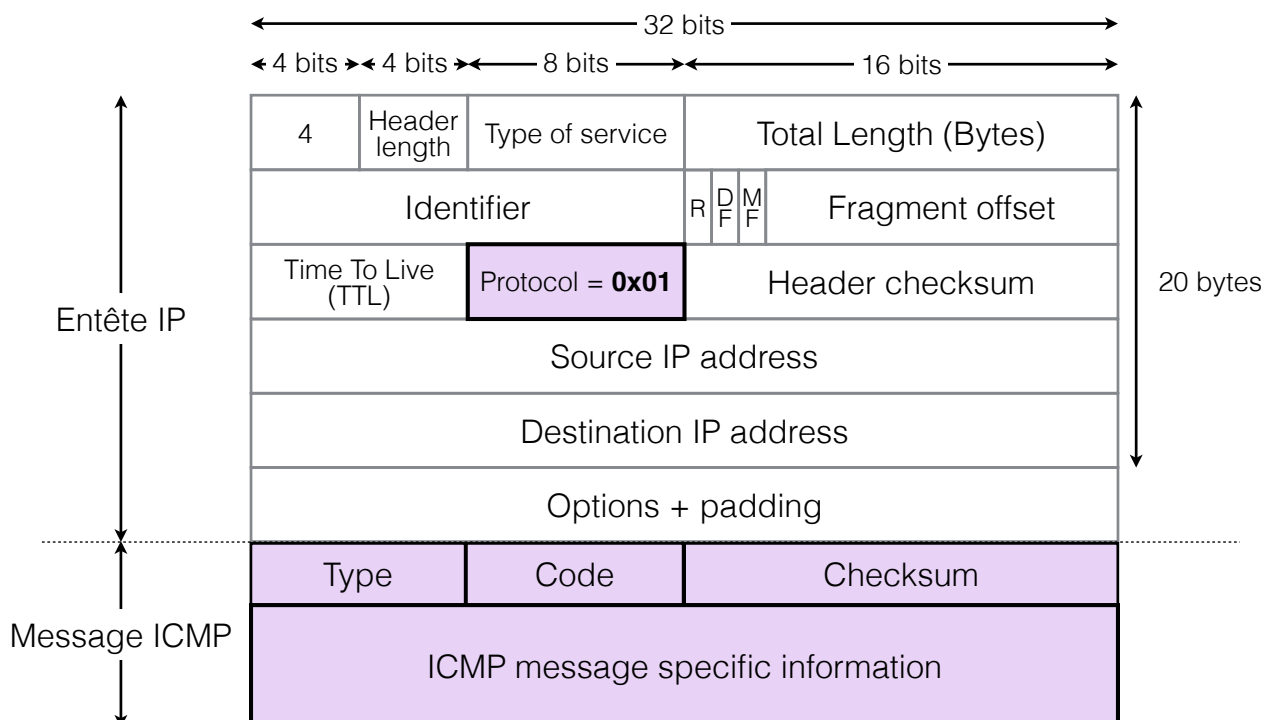


Protocole ICMP

- **Fonctionnalités de ICMP :**
 - messages d'erreur en cas d'erreurs d'acheminement ou de livraison
 - messages d'information permettant des tests de connectivité
- **Implémenté au dessus d'IP**
 - au même niveau que TCP (6) ou UDP (17)
 - champ Protocol IP : 1
- **Diagnostics d'erreur**
 - messages ICMP retournés à la source en cas de problème
 - temps dépassé, paquet trop grand, destination inaccessible, ...
- **Les messages ICMP contiennent :**
 - des informations relatives à l'erreur
 - type : nature de l'erreur, code : raison de l'erreur
 - copie partielle du paquet ayant provoqué l'erreur (dans la limite de 1480 octets)

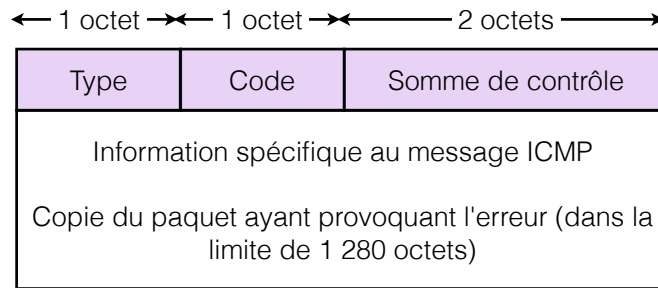
23

Encapsulation IP de ICMP



24

ICMP Messages



- **Type: nature du message ICMP**
 - messages d'erreur
 - messages d'information
- **Code: cause de l'erreur**
- **Somme de contrôle (checksum) :**
 - Vérification de l'intégrité :
 - du message ICMP
 - du pseudo-entête IP (similaire à TCP et UDP)

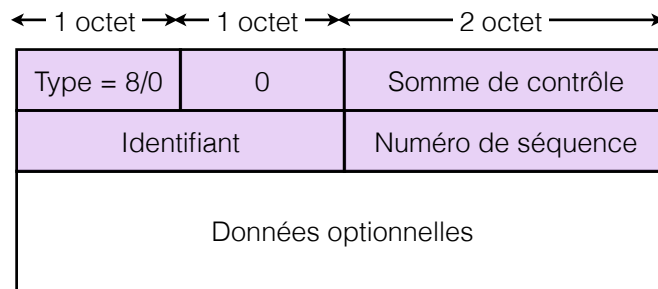
25

Types et codes ICMP

Type	Code	Message
0	0	Echo Reply
3	0	Destination Network Unreachable
3	1	Destination Host Unreachable
3	2	Destination Protocol Unreachable
3	3	Destination Port Unreachable
3	6	Destination Network Unknown
3	7	Destination Host Unknown
4	0	Source Quench
5	0	Redirect
8	0	Echo Request
11	0	Time Exceeded
11	1	Reassembly Time Exceeded
12		Parameter Problem
13		Timestamp
14		Timestamp Reply
15		Information Request
16		Information Reply
17		Address Mask Request
18		Address Mask Reply

26

Echo Request (Type=8) / Echo Reply (Type=0)

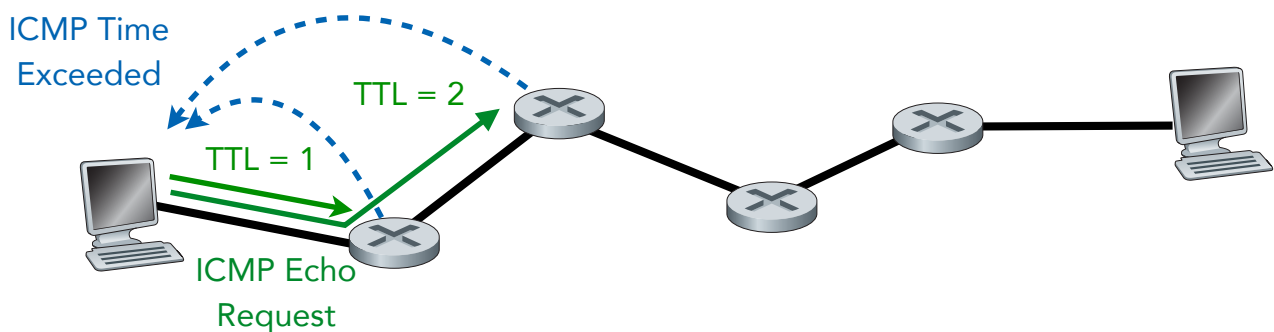


- Pour vérifier si une machine est joignable ou les problèmes de routage
 - mesure du délai aller-retour (valeurs min max moyenne)
 - comptage des messages Echo request ou Echo reply perdus
- Champ Identifier :
 - permet de faire correspondre les messages Echo Reply reçus aux messages Echo Request si envoyés à différentes machines
- Champ Sequence Number :
 - permet de faire correspondre un Echo Reply à l'Echo request correspondant si plusieurs Echo Request envoyés à la même machine

27

Traceroute

- La commande Traceroute envoie des messages ICMP 'Echo Request' en incrémentant leur TTL



28

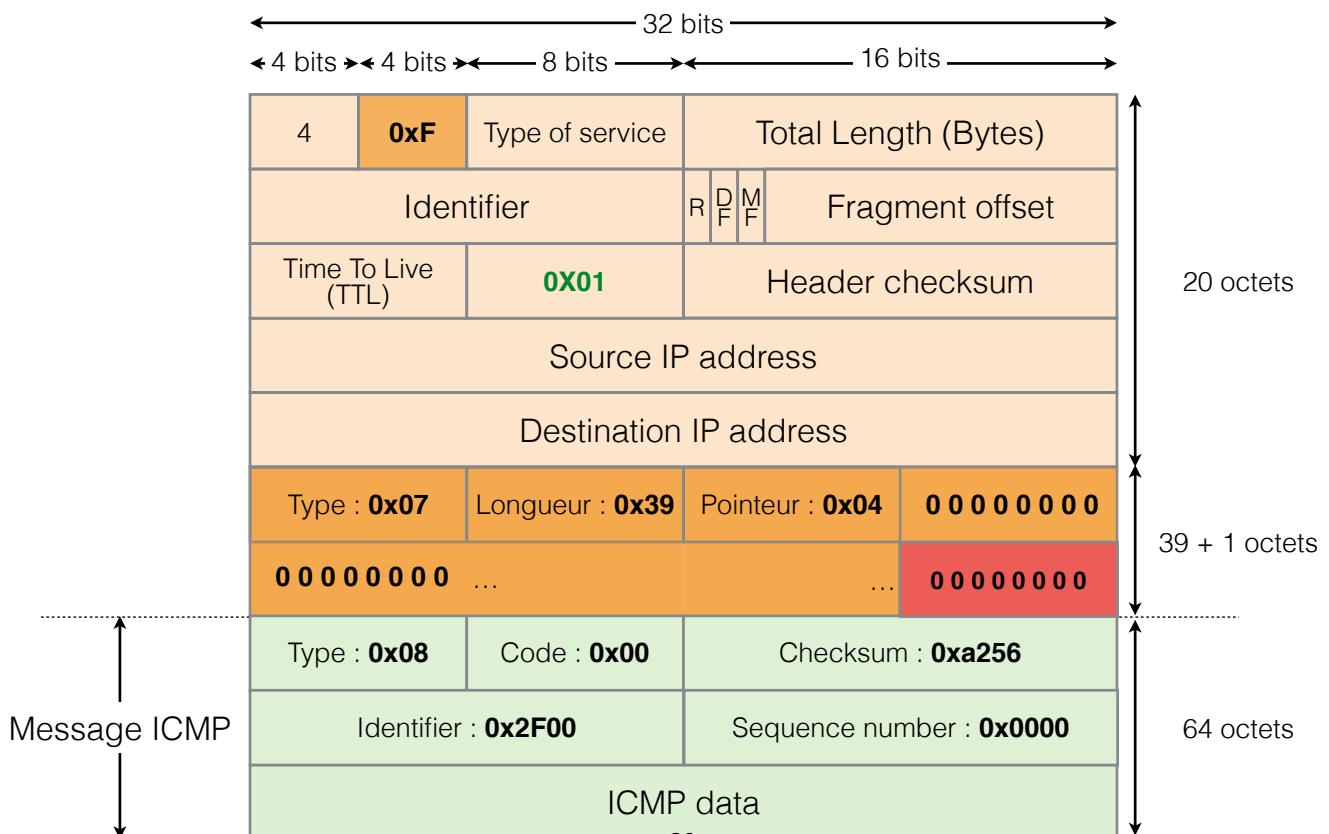
Option Record Route

Type = 8/0	0	Checksum
Identifier		Sequence number
Optional Data		

08	00	20	0a	ac	96	08	00	20	0a	70	66	08	00	4f	00
00	7c	cb	c9	00	00	ff	01	b9	7f	84	e3	3d	05	c0	21
9f	06	07	27	04	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	08	00	a2	56	2f
00	00	29	36	8c	41	00	03	86	2b	08	09	0a	0b	0c	0d
0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d
1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d
2e	2f	30	31	32	33	34	35	36	37						

29

Paquet IPv4 avec option Record Route



Conclusion

- Paquet IP
 - Taille max de l'entête : 60 octets
 - entête fixe : 20 octets
 - options IP : entre 0 et 40 octets
 - Fragmentation
 - ajuster la taille des paquets au champ données des trames
- Protocole ICMP
 - Tester la connectivité
 - Diagnostiquer les erreurs de routage ou de livraison
 - ping et traceroute