

Roland Inan
Didier Law-Tho



“Program testing can be used to show the presence of bugs, but never to show their absence!

"Le test de programmes peut être une façon très efficace de montrer la présence de bugs mais est désespérément inadéquat pour prouver leur absence!"



“Computer Science is no more about computers than astronomy is about telescopes.”

«L'informatique n'est pas plus la science des ordinateurs que l'astronomie n'est celle des télescopes.»

Edsger W. Dijkstra
Computer scientist





A propos de moi...



Didier Law-Tho
IT Expert chez Sanofi
France · [Contact info](#)
500+ connections

[More](#)

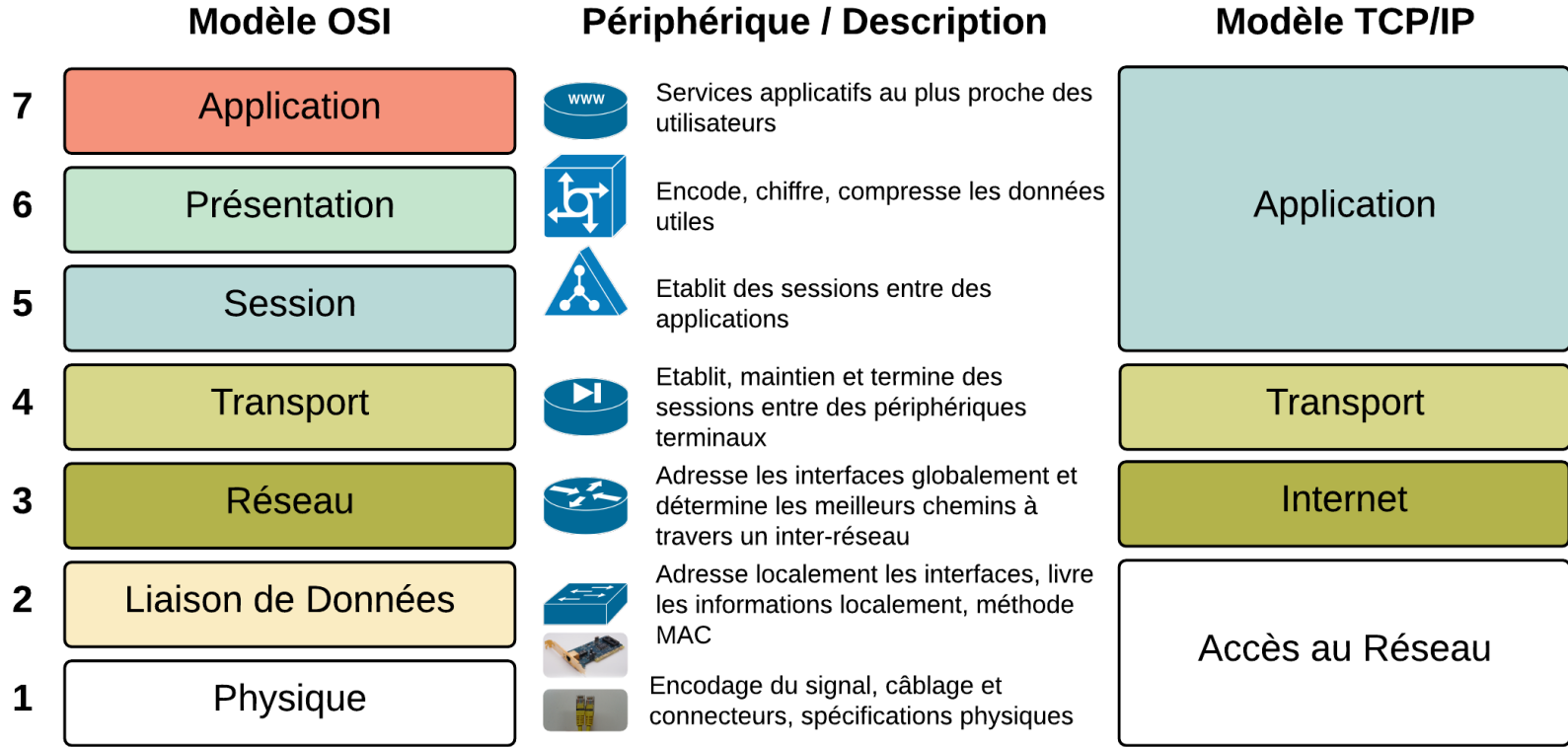
 Sanofi
 Télécom Paris

Plan du cours

- **Rappels des concepts réseau**
- **Bases de la cryptographie**
- **Composants de sécurité réseau**
 - Zones démilitarisées (DMZ)
 - Serveurs mandataires (Proxies)
 - Pare-feux (Firewalls)
 - VPN (Virtual Private Network)
- **Etude de cas:**
 - Projet de mise en place de services de diffusion vidéo live
- **Perspectives**
 - Introduction à la Cybersécurité

Rappels des concepts réseau

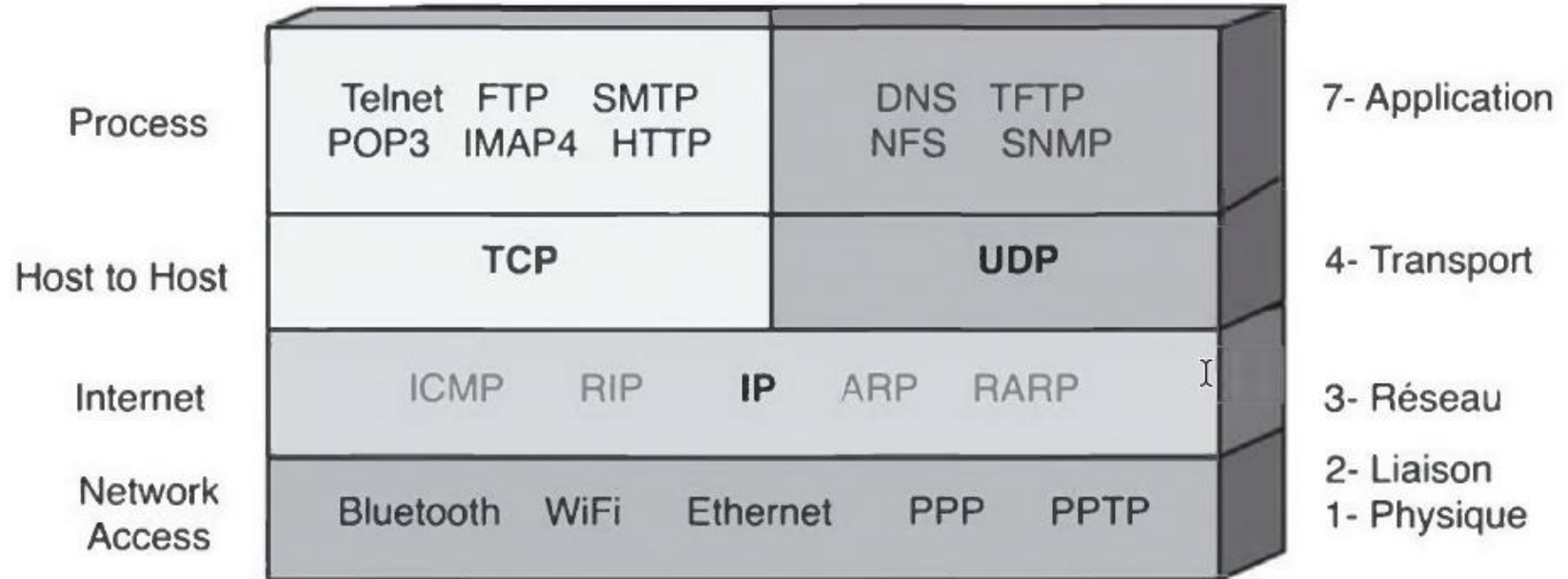
- **Modèle en couches**
- **Classes d'adresses IP**
- **Adresses privées/publiques (RFC 1918)**
- **En-tête des 4 couches de TCP/IP**
- **Étude d'un échange client-serveur**

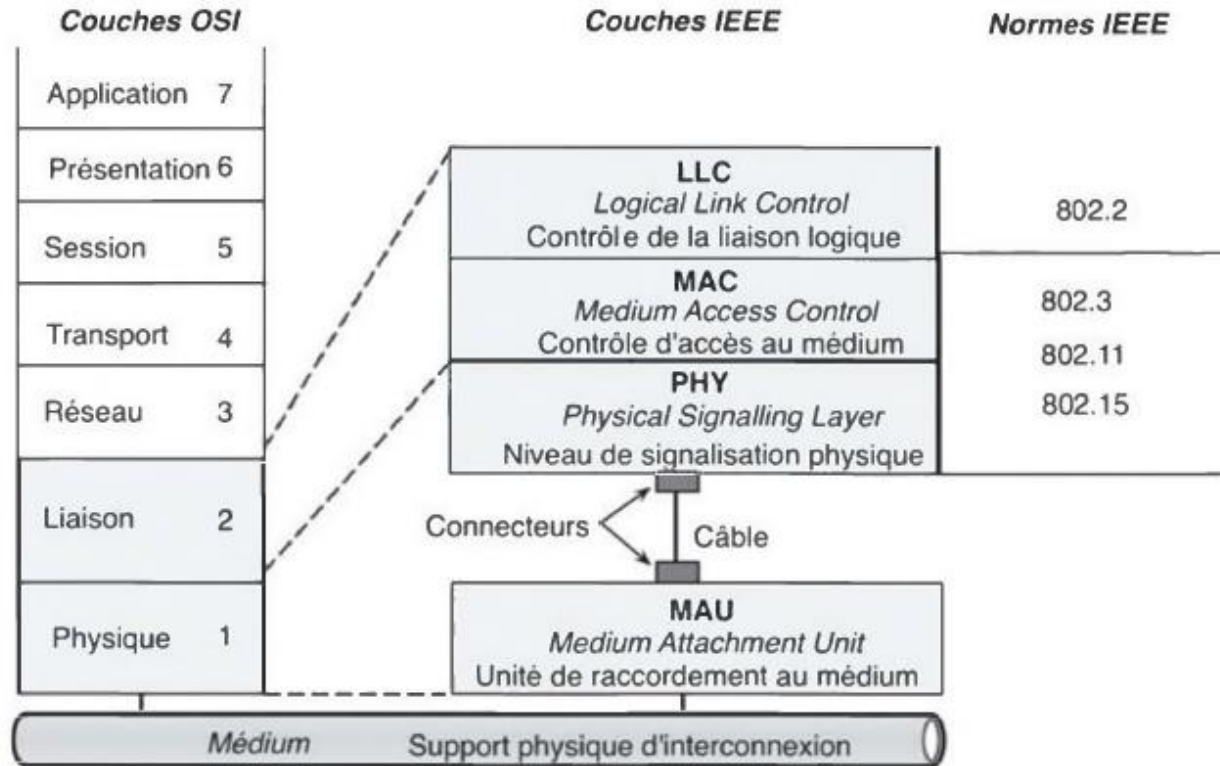


Modèle en couches

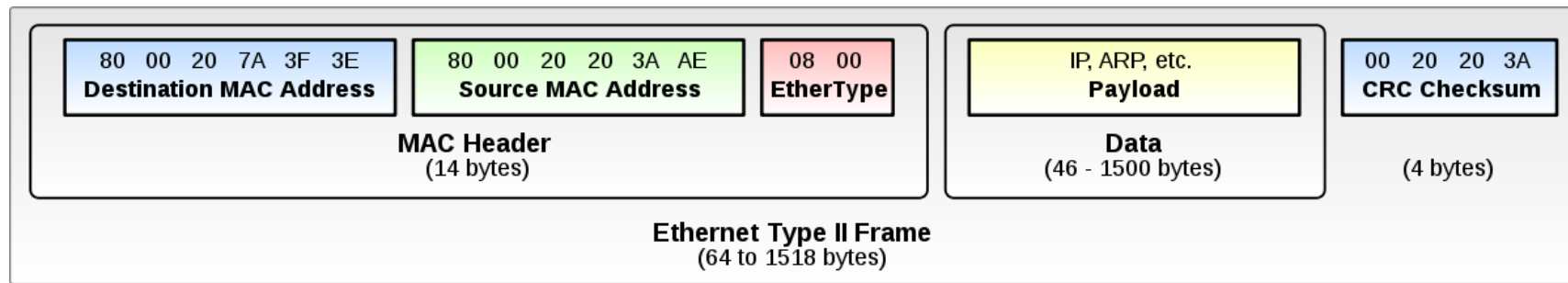
Modèle TCP/IP

Modèle OSI

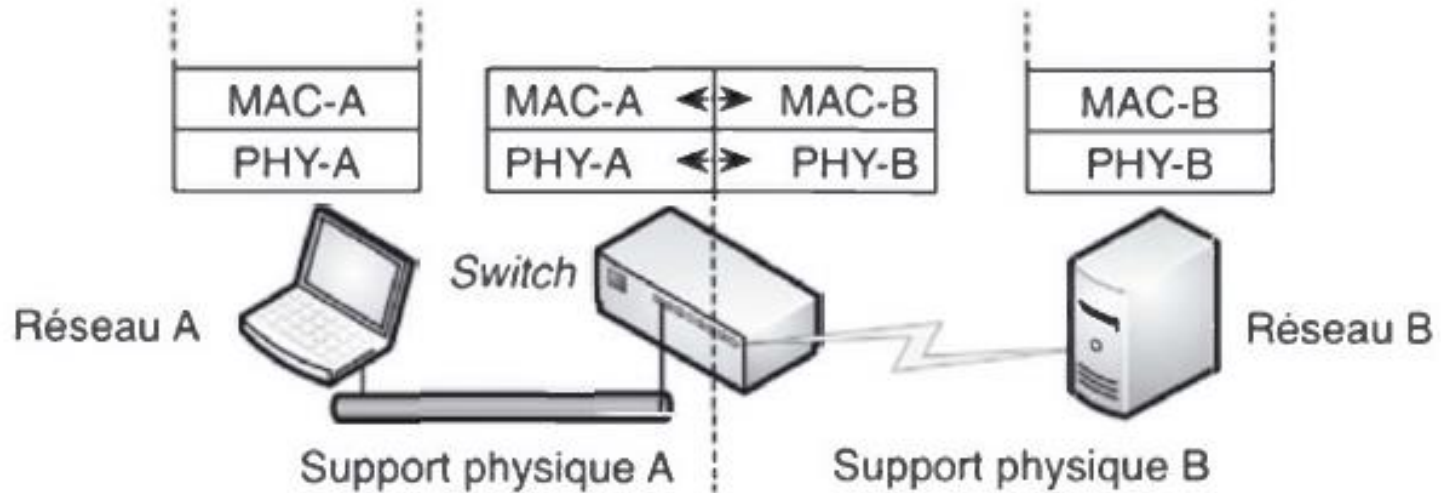




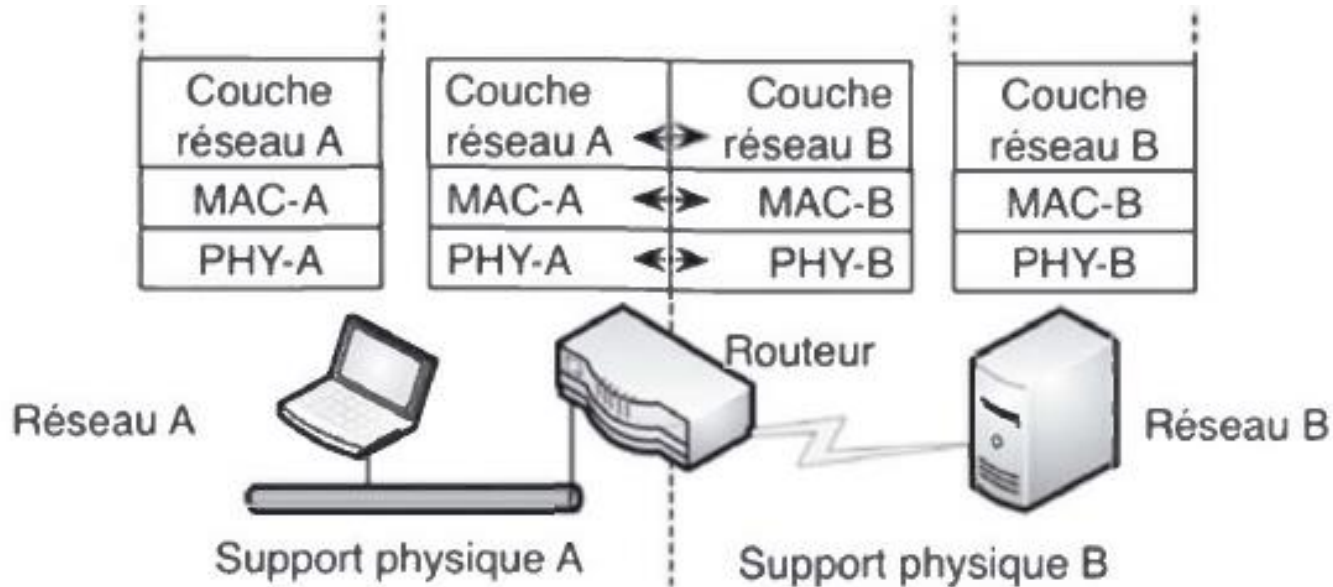
Correspondance OSI - IEEE.



Pont et Commutateur (Switch)

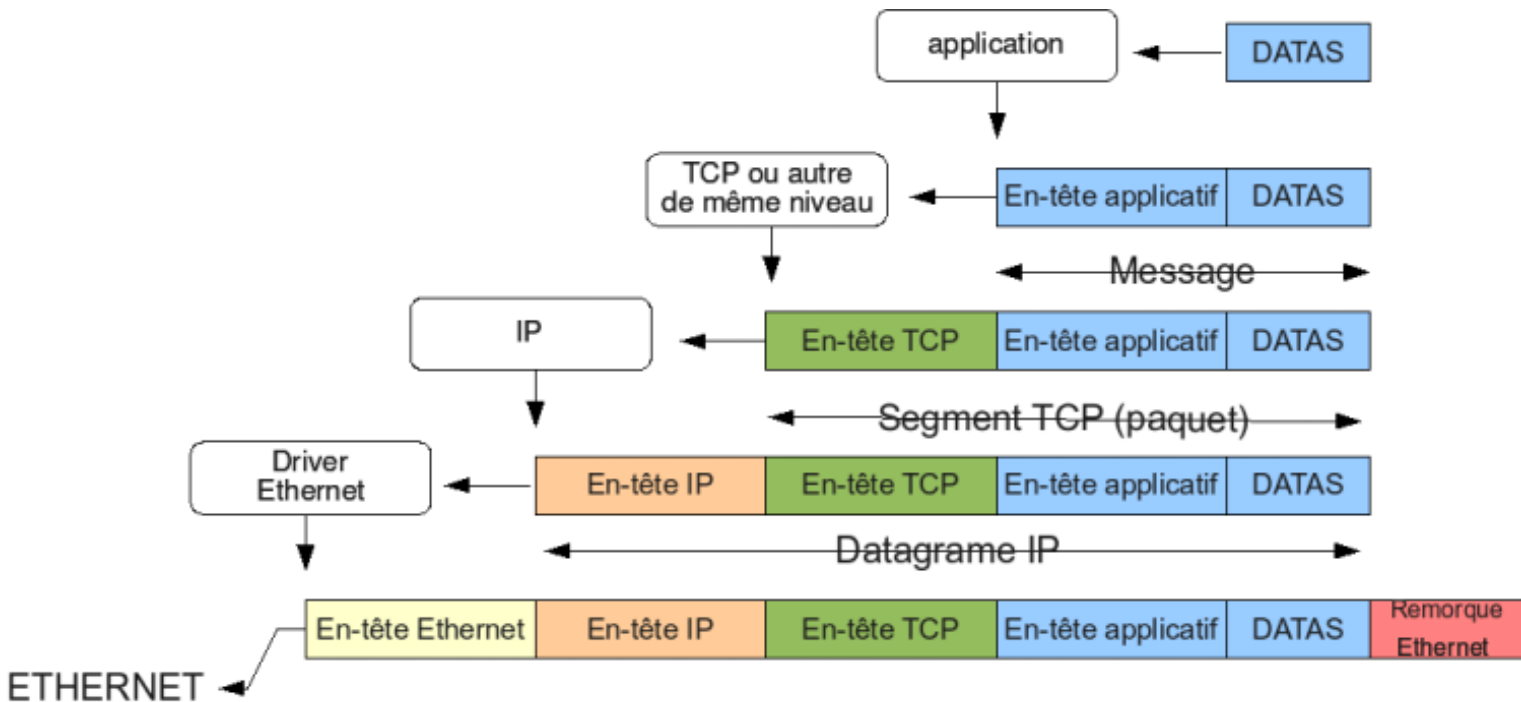


Architecture d'un pont ou d'un commutateur.

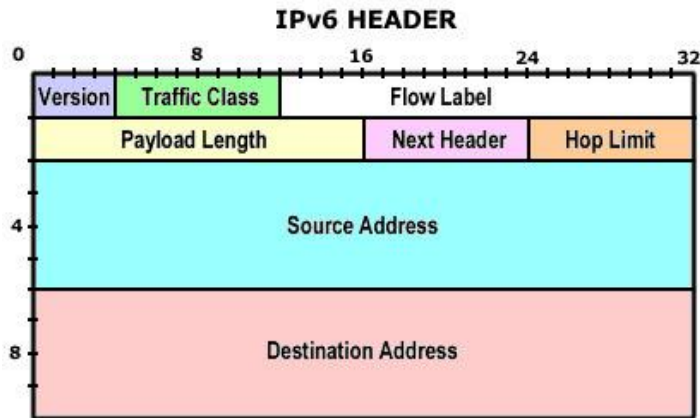
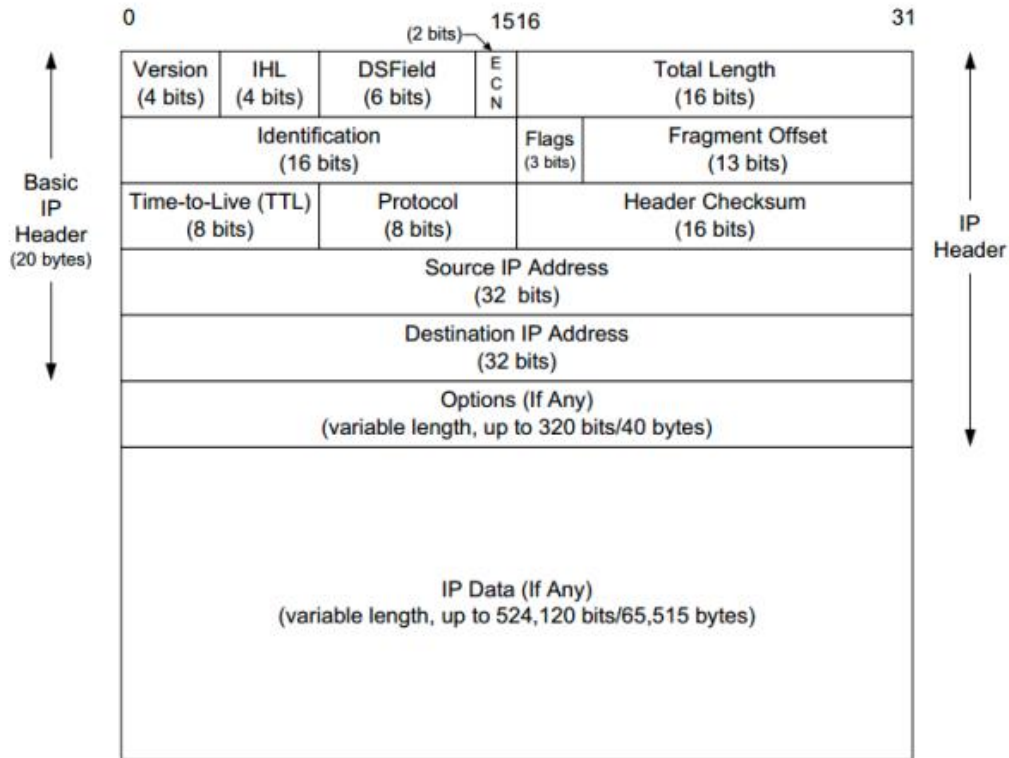


Architecture d'un routeur.

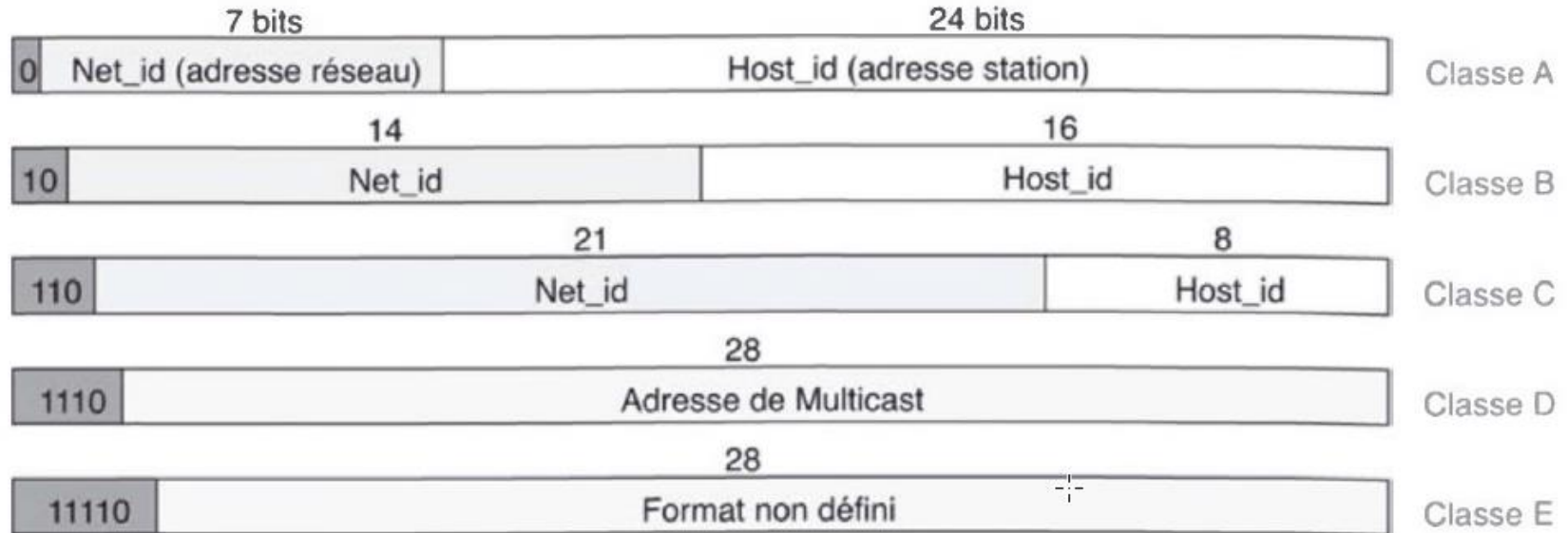
En-tête des 4 couches de TCP/IP



En-tête IPv4



Classes d'adresses IP

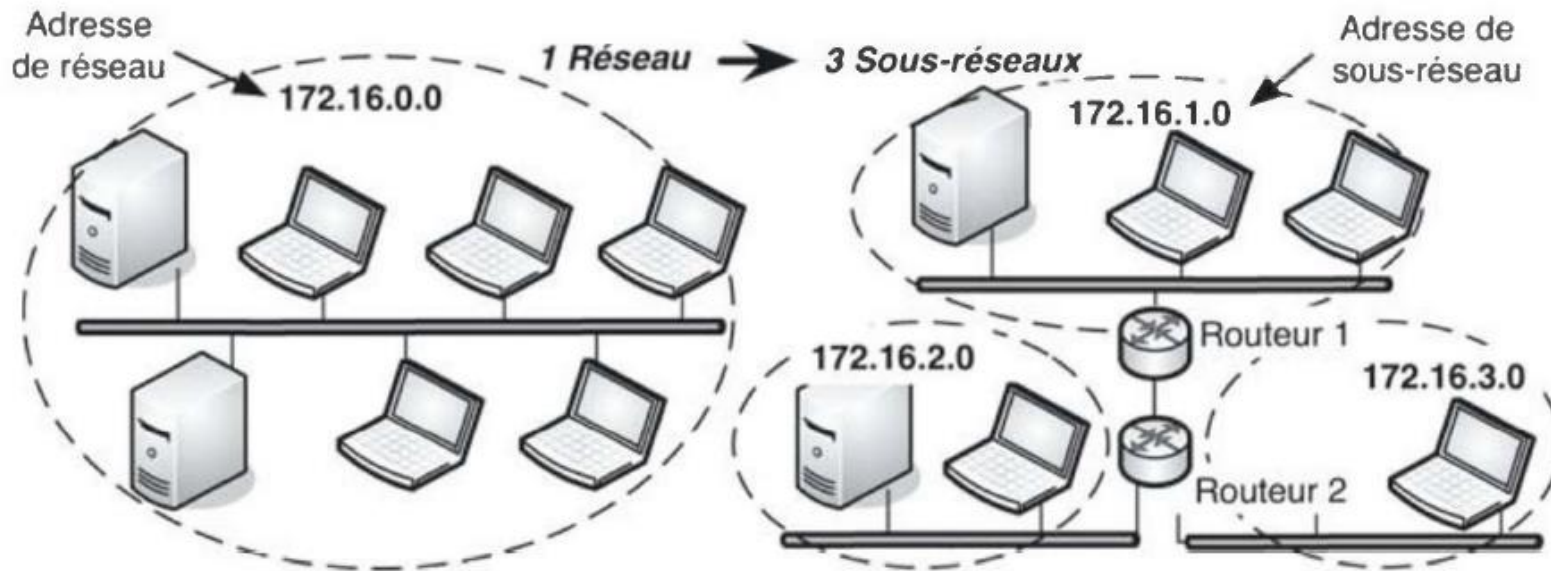


Classe	Début	Fin	Notation CIDR	Masque de sous-réseau par défaut
Classe A	0.0.0.0	127.255.255.255	/8	255.0.0.0
Classe B	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	192.0.0.0	223.255.255.255	/24	255.255.255.0
Classe D (multicast)	224.0.0.0	239.255.255.255	/4	non défini
Classe E (réservée)	240.0.0.0	255.255.255.255		non défini

	Nombre de réseaux	Nombre d'hôtes	Plage d'identificateur de réseau (1 ^{er} octet)
Classe A	$2^7 - 2 = 126$	$2^{24} - 2 = 16777214$	0-127
Classe B	$2^{14} - 2 = 16382$	$2^{16} - 2 = 65534$	128-191
Classe C	$2^{21} - 2 = 2097150$	$2^8 - 2 = 254$	192-223

Résumé des classes d'adresse

Adressage de sous-réseaux (subnetting)




Exemple de segmentation en sous-réseaux.

Subnetting et masques




Réorganisation du *host_id*.

	Net_id	Subnet_id	Host_id = 15
Adresse IP : 192.44.77.79	= 1100 0000 . 0010 1100 . 0100 1101	. 01 00 1111	
Netmask : 255.255.255.192	= 1111 1111 . 1111 1111 . 1111 1111	. 11 00 0000	
Adresse de sous-réseau : 192.44.77.64	= 1100 0000 . 0010 1100 . 0100 1101	. 01 00 0000	

+

Exemple d'utilisation du masque.

Subnetting et masques

	Net_id	Subnet_id	Host_id = 15
Adresse IP : 192.44.77.79	= 1100 0000 . 0010 1100 . 0100 1101	. 01 00 1111	
Netmask : 255.255.255.192	= 1111 1111 . 1111 1111 . 1111 1111	. 11 00 0000	
Adresse de sous-réseau : 192.44.77.64	= 1100 0000 . 0010 1100 . 0100 1101	. 01 00 0000	

+

Exemple d'utilisation du masque.

- 192.44.77.0000 0000 = 192.44.77.0
- 192.44.77.0100 0000 = 192.44.77.64
- 192.44.77.1000 0000 = 192.44.77.128
- 192.44.77.1100 0000 = 192.44.77.192

Les masques de longueur variable VLSM

Exemple

Un routeur possède trois interfaces pour connecter trois réseaux N1, N2 et N3.

L'administrateur réseau impose les conditions suivantes :

- capacité d'adressage de N1, 40 stations ;
- capacité d'adressage de N2, 80 stations ;
- capacité d'adressage de N3, 140 stations ;
- utilisation au mieux du bloc 128.203.0.0 / 20.

La première étape consiste à trouver le nombre de bits pour la partie *host_id*, ce qui correspond à la puissance de 2 immédiatement supérieure au nombre de stations :

- N1 : 40 stations donc 6 bits ($2^5 < 40 < 2^6$) ;
- N2 : 80 stations donc 7 bits ($2^6 < 80 < 2^7$) ;
- N3 : 140 stations donc 8 bits ($2^7 < 140 < 2^8$).

Les masques sont donc :

- N1 : 255.255.255.192 (/26) → 26 bits à 1 ; 6 bits à 0 ;
- N2 : 255.255.255.128 (/25) → 25 bits à 1 ; 7 bits à 0 ;
- N3 : 255.255.255.0 (/24) → 24 bits à 1 ; 8 bits à 0.

Les masques de longueur variable VLSM

On alloue ensuite les blocs d'adresse du plus grand au plus petit :

- Premier bloc, le plus grand : N3.

Masque 255.255.255.0 soit 128.203.0.0/24.

Espace d'adressage de N3 : 128.203.0.0 à 128.203.0.255 (254 stations).

- Deuxième bloc : N2.

Masque 255.255.255.128 (/25).

On utilise le sous-bloc contigu à N3, donc : 128.203.1.0/25.

Espace d'adressage de N2 : 128.203.1.0 à 128.203.1.127 (126 stations).

- Le plus petit sous-réseau : N1.

Masque 255.255.255.192 (/26).

On utilise le sous-bloc contigu à N2, soit : 128.203.1.128/26.

Espace d'adressage de N1 : 128.203.1.128 à 128.203.1.191 (62 stations).

En utilisant cet algorithme, l'adressage IP est optimisé au maximum, C'est la façon dont les ISP gèrent, en principe, leurs espaces d'adressage IP.

Notation CIDR et Supernetting

- La notation CIDR » (Classless Inter-Domain Routing) donne le numéro du réseau suivi par une barre oblique (ou slash, « / ») et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau. Le masque 255.255.224.0, équivalent en binaire à 11111111.11111111.11100000.00000000, sera donc représenté par /19 (19 bits à la valeur 1, suivis de 13 bits 0). Le supernetting est une technique de CIDR qui permet de définir un préfixe réseau englobant plusieurs sous-réseaux.

Route summarization

- 201.1.0.0/22
 - 201.1.4.0/23
 - 201.1.6.0/24
 - 201.1.7.0/24
- Same Difference starts here

Octet 3 in binary

00000000
00000100
00000110
00000111

Same Difference starts here

21 bits the same so
use /21 for summary

Adresses IP privées / publiques

IANA: Internet Assigned Numbers Authority

FAI : Fournisseur d'Accès à Internet

IETF: Internet Engineering Task Force

NAT (Network Address Translation)

CIDR (Classless Interdomain Routing)

VLSM (Variable-Length subnet mask)

Classe A

De 0.0.0.0 à 127.255.255.255

Classe B

De 128.0.0.0 à 191.255.255.255

Classe C

De 192.0.0.0 à 223.255.255.255

Adressages IP privés (Non-Routable)

Classe A

De 10.0.0.0 à 10.255.255.255

Classe B

De 172.16.0.0 à 172.31.255.255

Classe C

De 192.168.0.0 à 192.168.255.255

Adressages IP publiques (Routable)

Classe A

- De 1.0.0.0 à 9.255.255.255
- De 11.0.0.0 à 126.255.255.255

Classe B

- De 128.0.0.0 à 172.15.255.255
- De 172.32.0.0 à 191.255.255.255

Classe C

- De 192.0.0.0 à 192.167.255.255
- De 192.169.0.0 à 223.255.255.255

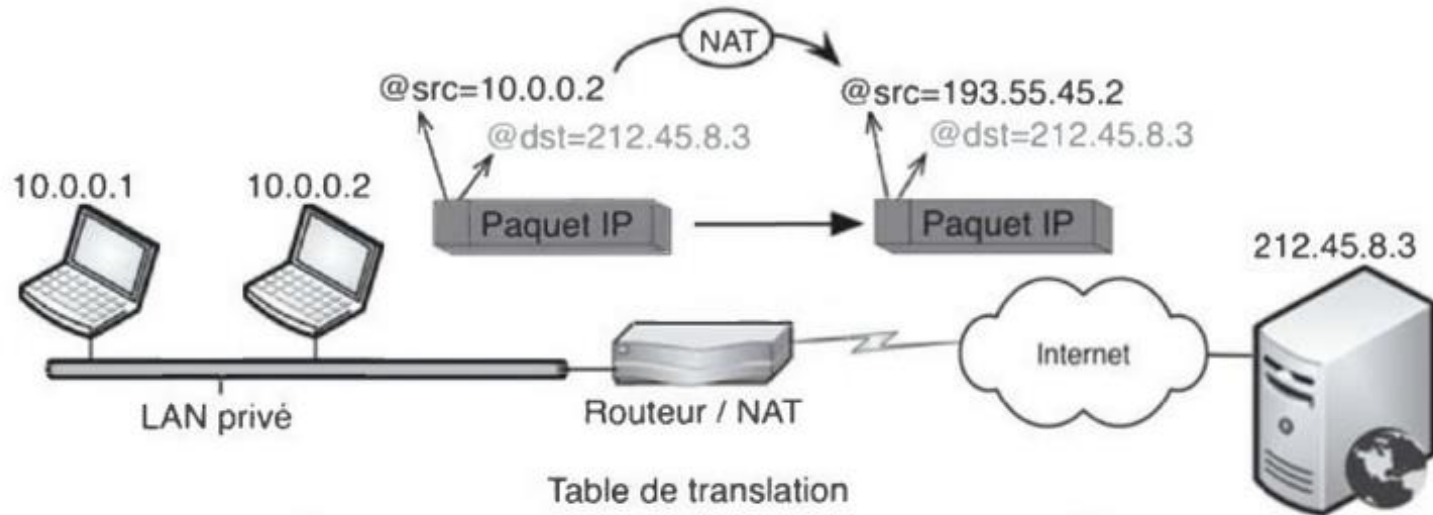


Table de translation

Interne		Externe	
@src	@dst	@src	@dst
10.0.0.2	212.45.8.3	193.55.45.2	212.45.8.3

Exemple de translation d'adresses.

Réseaux privés et la translation d'adresses NAPT

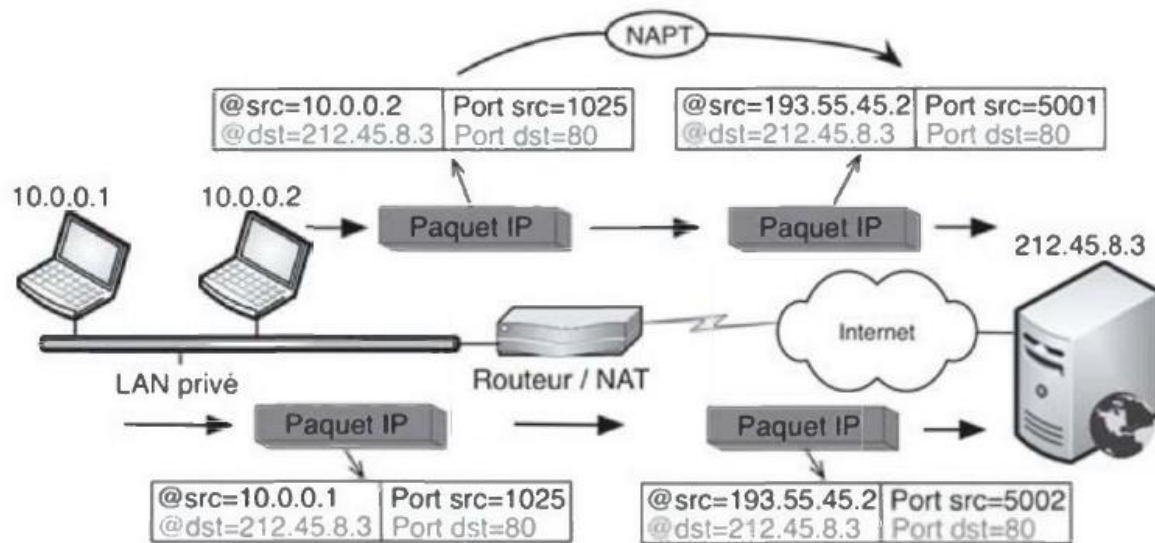


Table de translation

Interne				Externe			
@src	@dst	Port src	Port dst	@src	@dst	Port src	Port dst
10.0.0.1	212.45.8.3	1025	80	193.55.45.2	212.45.8.3	5001	80
10.0.0.2	212.45.8.3	1025	80	193.55.45.2	212.45.8.3	5002	80

Exemple de translation d'adresse et de port.

Adressage IPV6 versus IPV4

IPv4

vs.

IPv6

Deployed 1981

32-bit IP address

4.3 billion addresses

Addresses must be reused and masked

Numeric dot-decimal notation

192.168.5.18

DHCP or manual configuration

Deployed 1998

128-bit IP address

7.9×10^{28} addresses

Every device can have a unique address

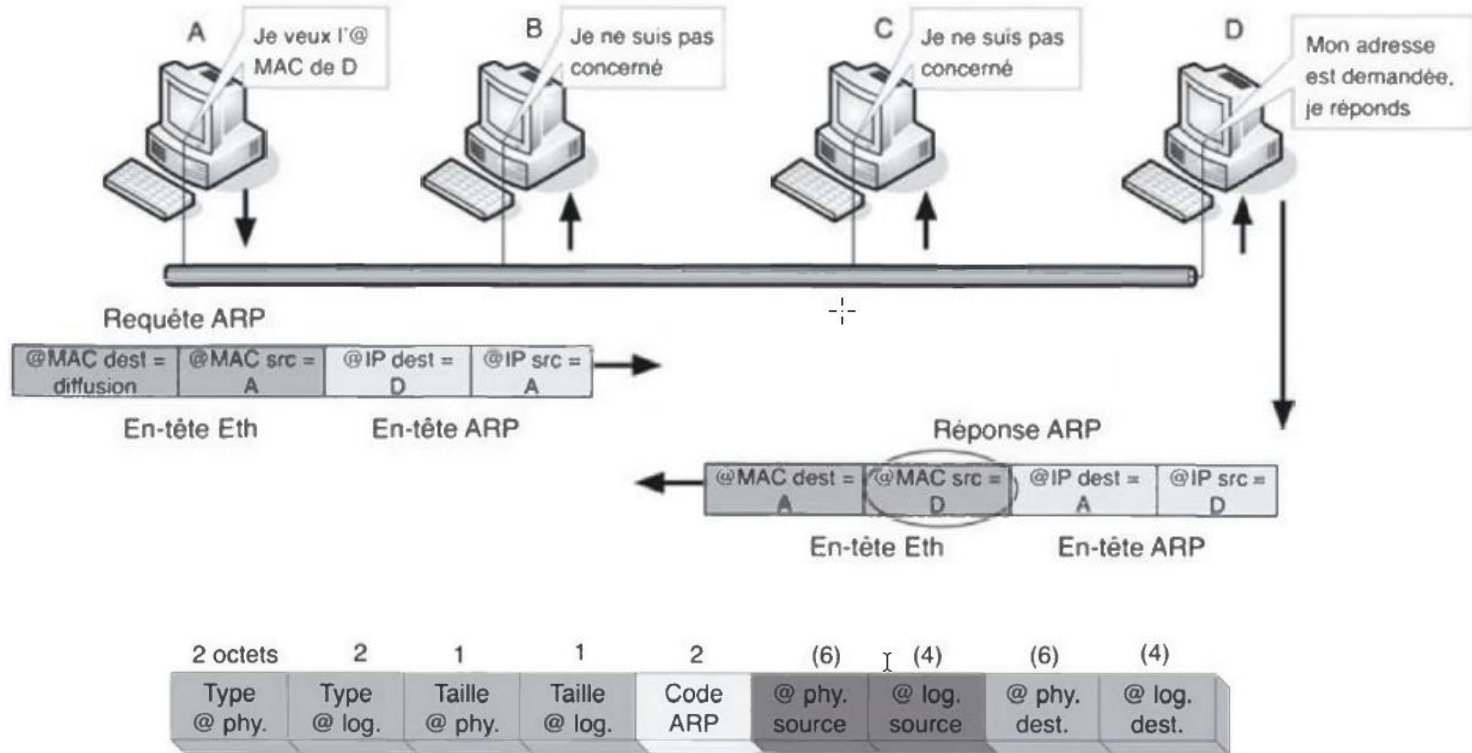
Alphanumeric hexadecimal notation

50b2:6400:0000:0000:6c3a:b17d:0000:10a9

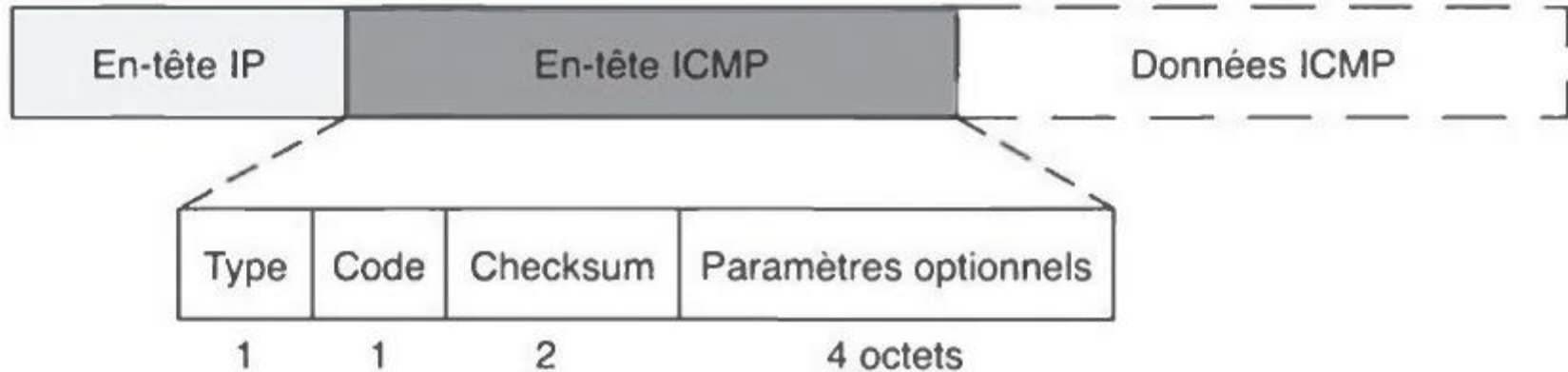
(Simplified - 50b2:6400::6c3a:b17d:0:10a9)

Supports autoconfiguration

Le protocole ARP

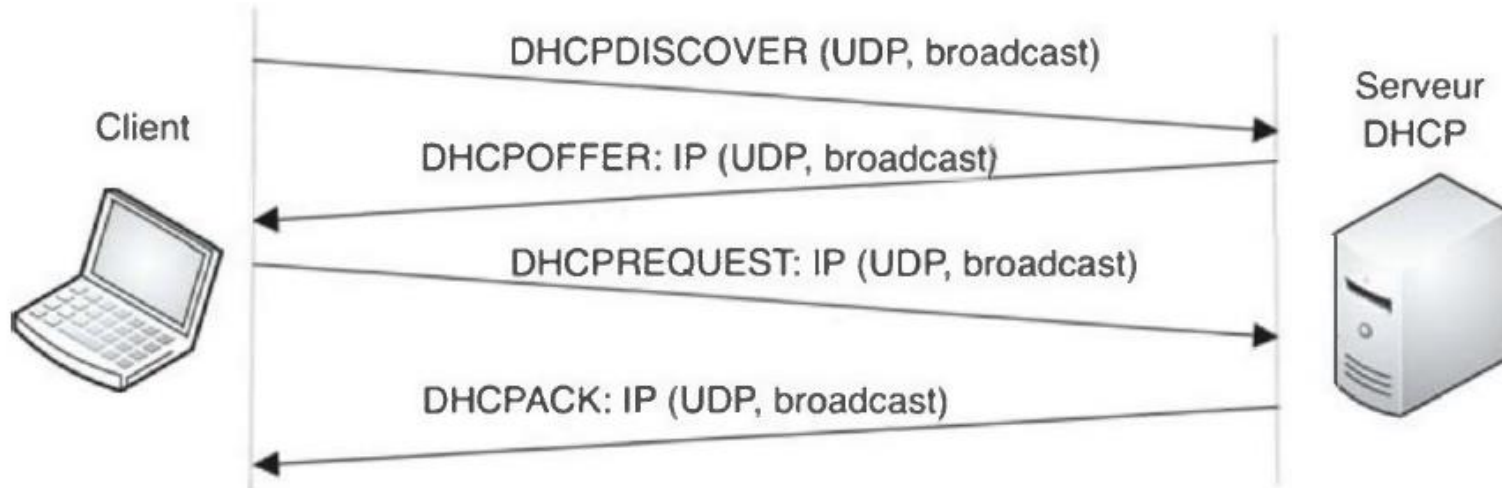


Format de l'en-tête ARP.

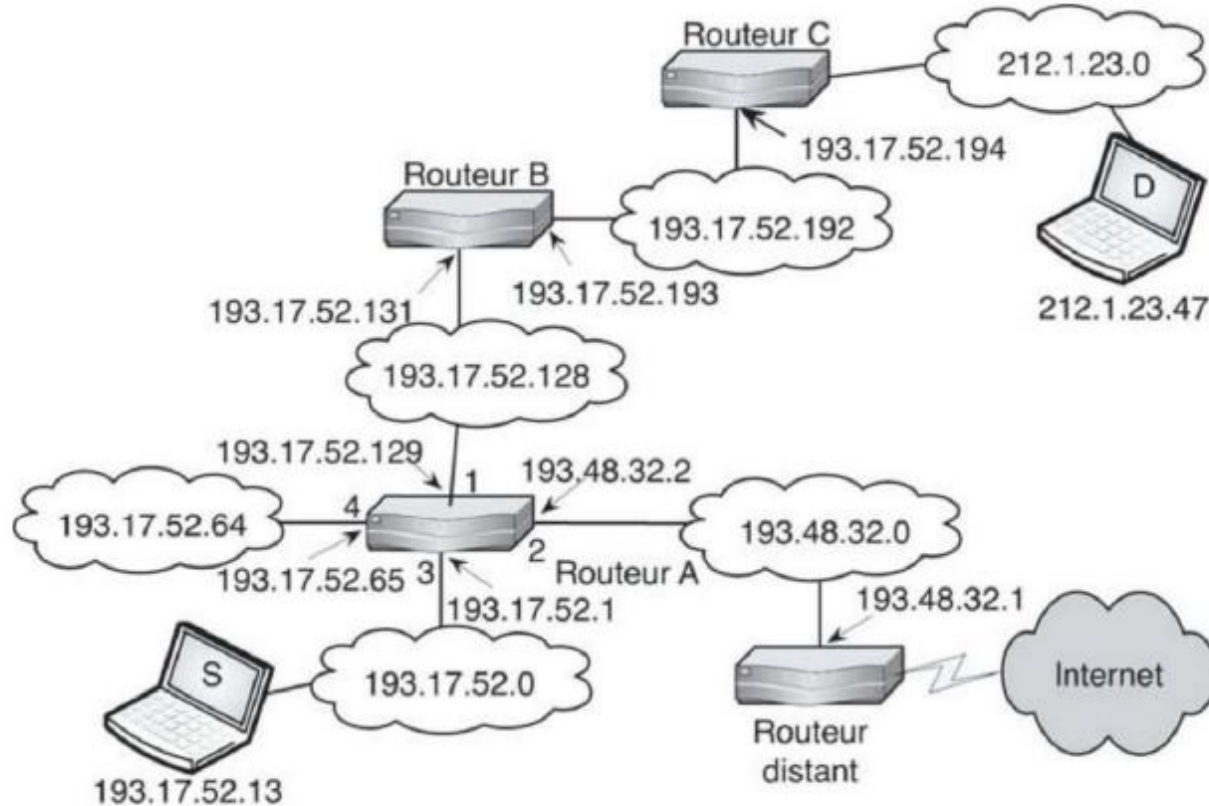


Format du paquet ICMP.

Le protocole DHCP



Échange DHCP.

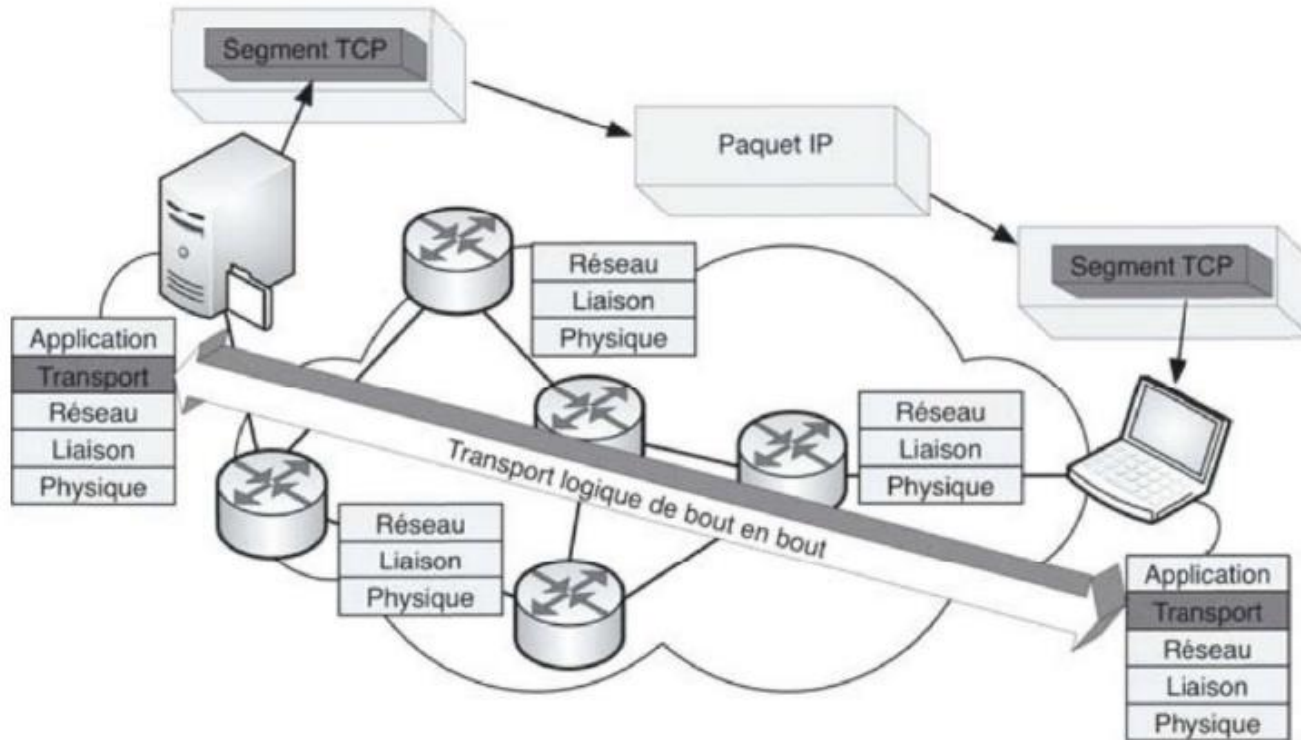


Exemple d'interconnexion.

Exemple de table de routage.

Adresse du réseau destination	Masque du réseau destination	Adresse du prochain routeur	Interface empruntée	Nombre de sauts
193.17.52.128	255.255.255.192	193.17.52.129	Ethernet 1	0 (direct)
193.48.32.0	255.255.255.0	193.48.32.2	Ethernet 2	0 (direct)
193.17.52.0	255.255.255.192	193.17.52.1	Ethernet 3	0 (direct)
193.17.52.64	255.255.255.192	193.17.52.65	Ethernet 4	0 (direct)
193.17.52.192	255.255.255.192	193.17.52.131	Ethernet 1	1
212.1.23.0	255.255.255.0	193.17.52.131	Ethernet 1	2
0.0.0.0	0.0.0.0	193.48.32.1	Ethernet 2	0

Le protocole de bout en bout (TCP)



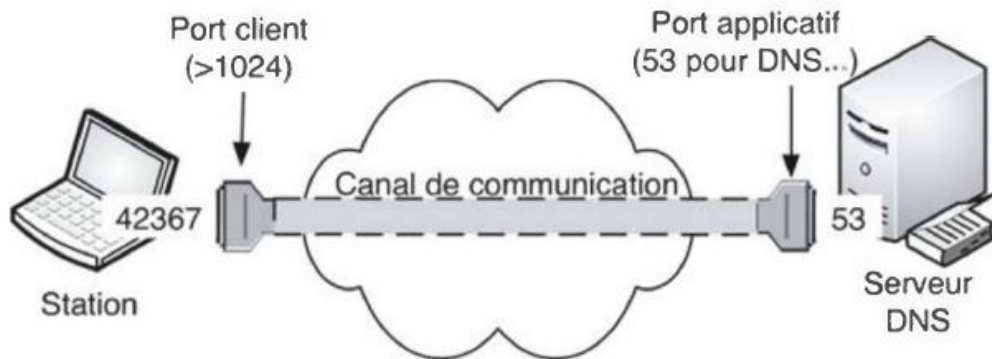
Présence de la couche transport.

TCP Segment Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Sequence Number							
64	Acknowledgment Number							
96	Data Offset	Res	Flags		Window Size			
128	Header and Data Checksum				Urgent Pointer			
160...	Options							

UDP Datagram Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Length				Header and Data Checksum			

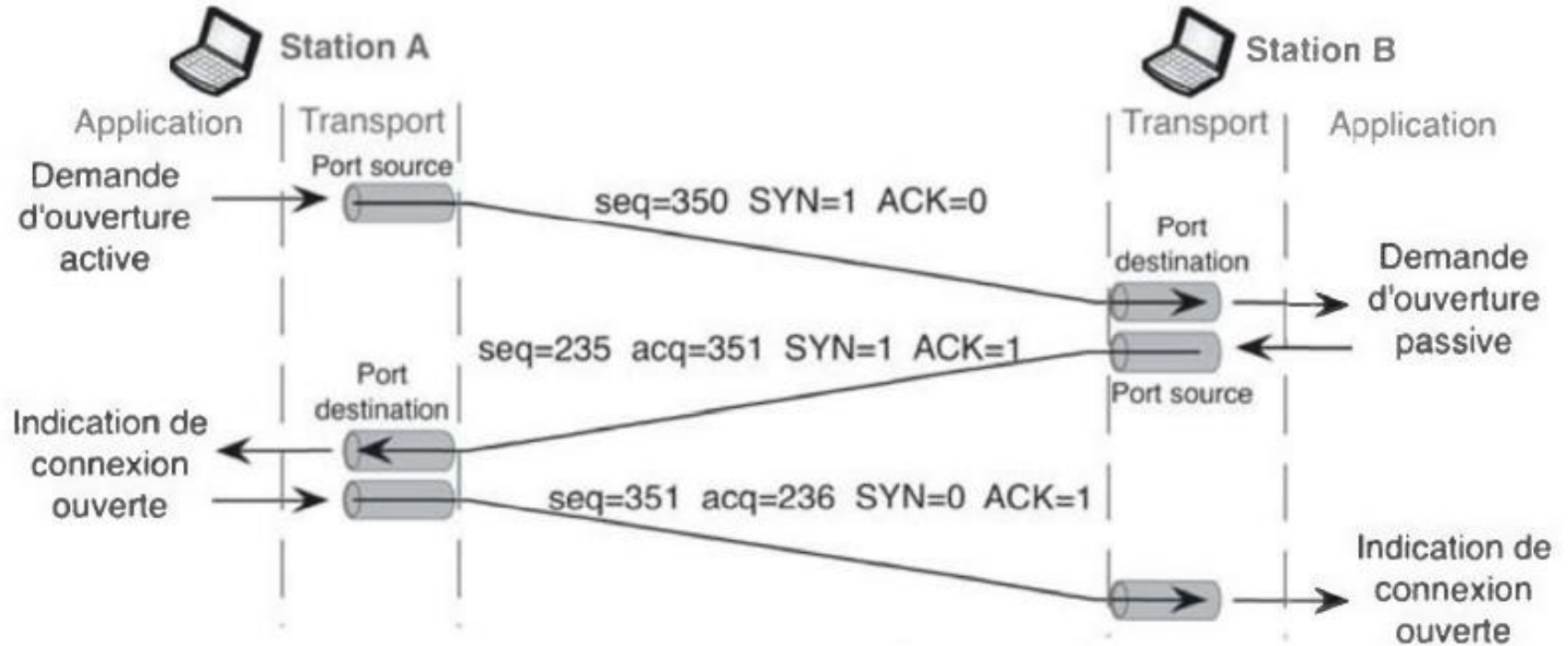


Affectation des numéros de port client et serveur.

Numéros de port UDP et TCP usuels.

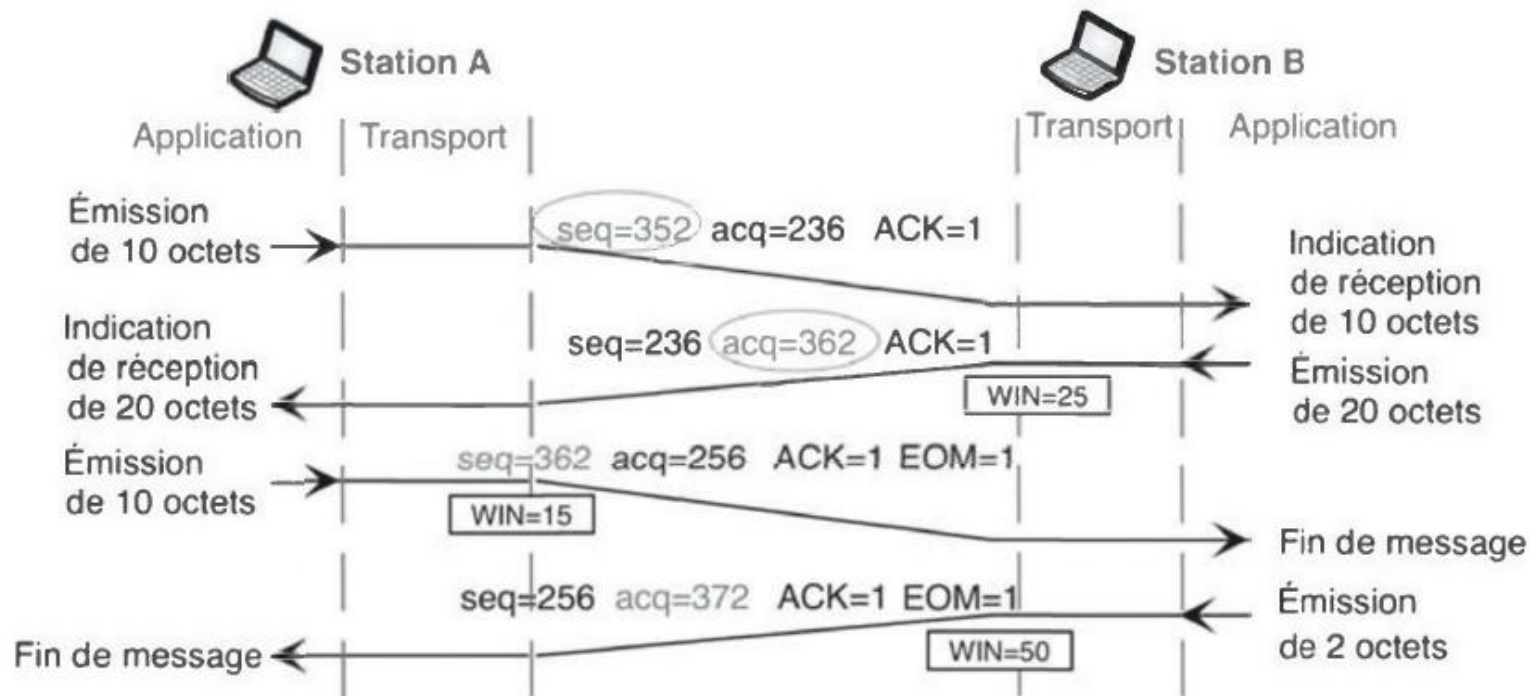
N° de port	7	20	21	22	25	53	80	110	161
Process	Echo	FTP-data	FTP	SSH	SMTP	DNS	HTTP	POP3	SNMP

Ouverture d'une connexion TCP



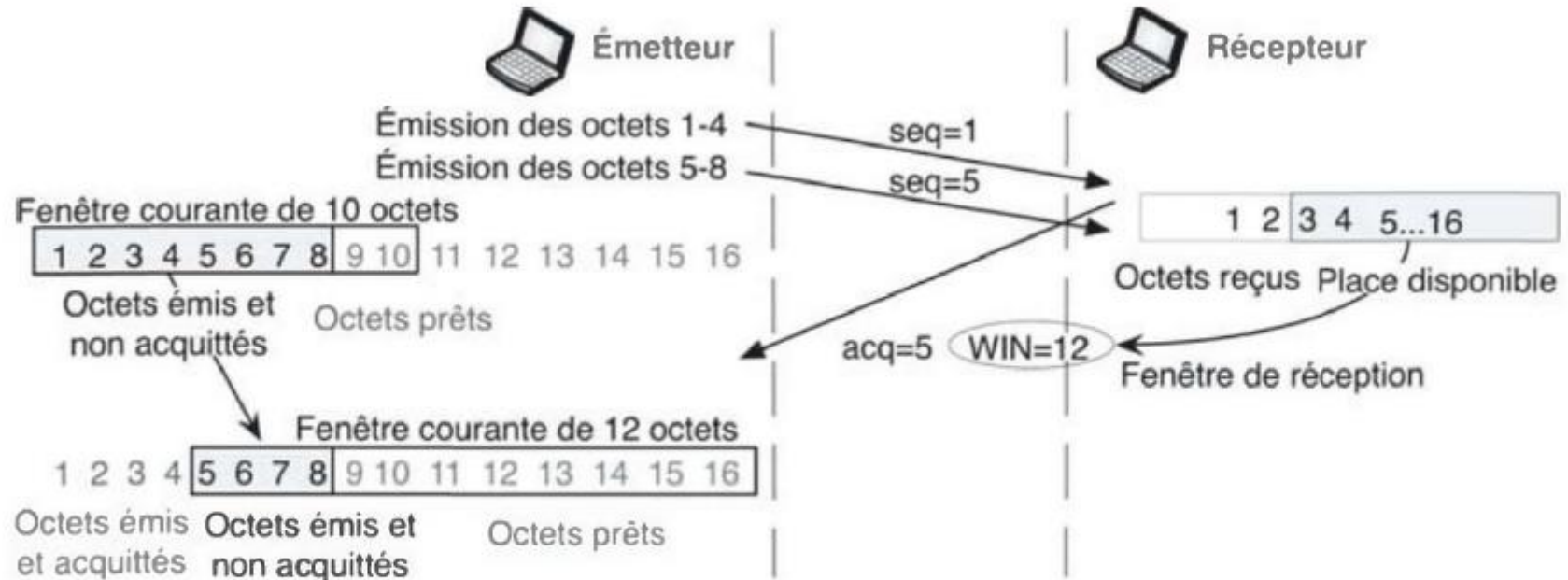
Exemple de connexion réussie.

Transfert de données TCP



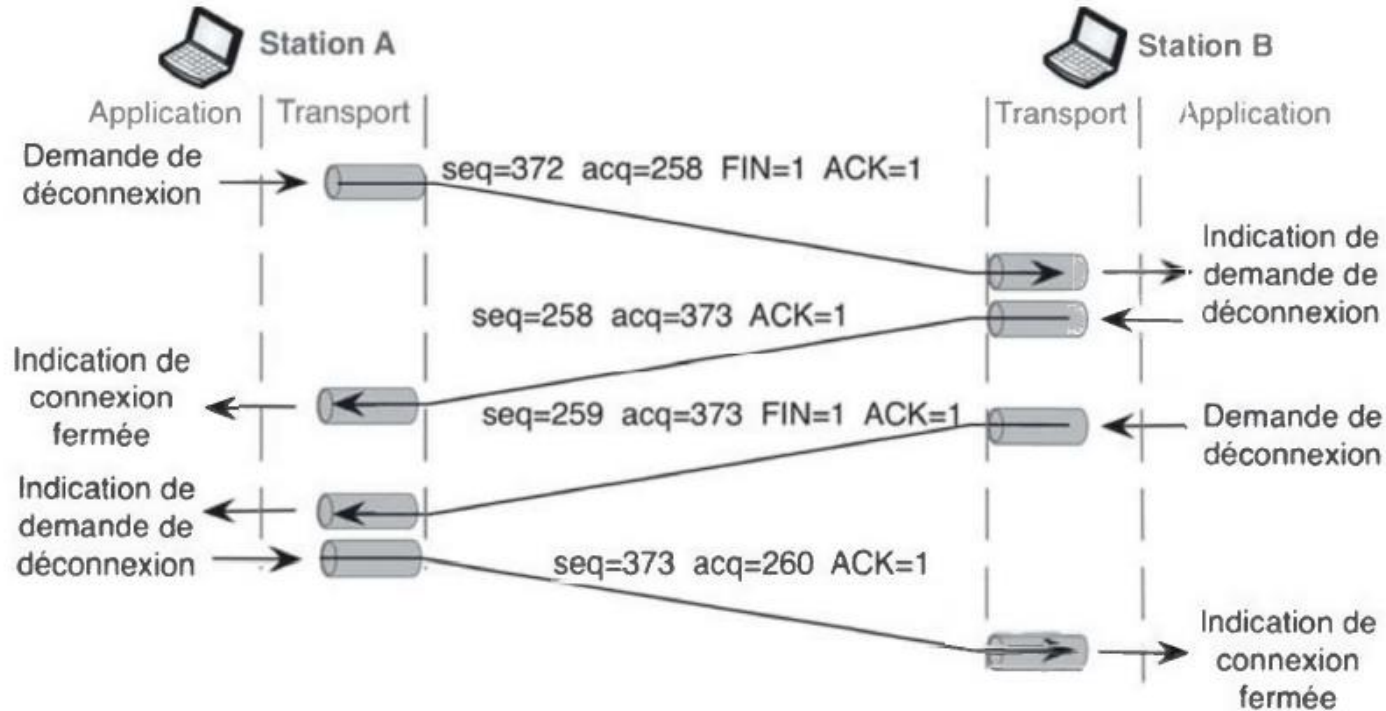
Exemple d'échange TCP.

Fenêtre glissante TCP



Gestion de la fenêtre d'émission.

Fermeture de la connexion TCP



Exemple de fermeture réussie.

Étude d'un échange client-serveur

- Soit la trame provenant d'un échange entre un ordinateur et l'application DropBox

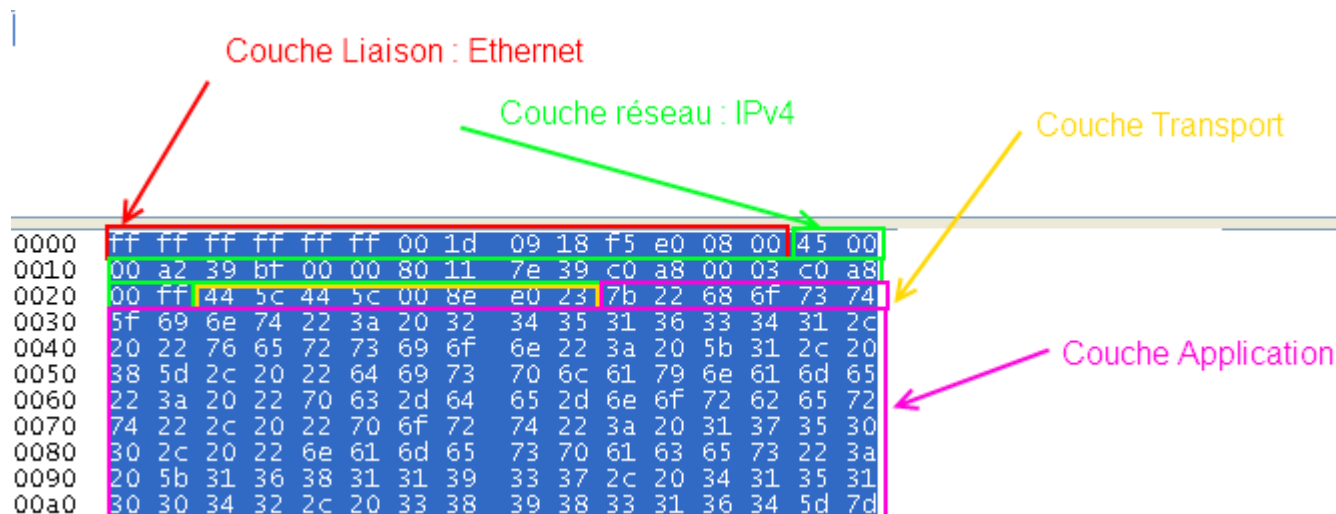
```
⊕ Frame 13: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) on interface 0
⊕ Ethernet II, Src: Dell_18:f5:e0 (00:1d:09:18:f5:e0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊕ Internet Protocol, Src: 192.168.0.3 (192.168.0.3), Dst: 192.168.0.255 (192.168.0.255)
⊕ User Datagram Protocol, Src Port: db-lsp-disc (17500), Dst Port: db-lsp-disc (17500)
⊕ Dropbox LAN sync Discovery Protocol
```

0000	ff ff ff ff ff ff 00 1d 09 18 f5 e0 08 00 45 00E.
0010	00 a2 39 bf 00 00 80 11 7e 39 c0 a8 00 03 c0 a8	..9.....~9.....
0020	00 ff 44 5c 44 5c 00 8e e0 23 7b 22 68 6f 73 74	..D\p\.. .#{ "host
0030	5f 69 6e 74 22 3a 20 32 34 35 31 36 33 34 31 2c	_int": 2 4516341,
0040	20 22 76 65 72 73 69 6f 6e 22 3a 20 5b 31 2c 20	"versio n": [1,
0050	38 5d 2c 20 22 64 69 73 70 6c 61 79 6e 61 6d 65	8], "dis playname
0060	22 3a 20 22 70 63 2d 64 65 2d 6e 6f 72 62 65 72	": "pc-d e-norber
0070	74 22 2c 20 22 70 6f 72 74 22 3a 20 31 37 35 30	t", "por t": 1750
0080	30 2c 20 22 6e 61 6d 65 73 70 61 63 65 73 22 3a	0, "name spaces":
0090	20 5b 31 36 38 31 31 39 33 37 2c 20 34 31 35 31	[168119 37, 4151
00a0	30 30 34 32 2c 20 33 38 39 38 33 31 36 34 5d 7d	0042, 38 983164]]

- La couche Transport utilise le protocole UDP
- La couche Réseau utilise une communication en IPv4
- La couche Liaison utilise l'Ethernet

Étude d'un échange client-serveur

- Nombre d'octets par couche :
 - Couche Liaison : 14 octets
 - Couche Réseau : 20 octets
 - Couche Transport : 8 octets
- On peut décomposer la trame :



Ce qu'il faut retenir!

- Les équipements d'interconnexion des réseaux interviennent à différents niveaux : le **répéteur** ou le **hub** pour la couche physique ; le **pont** ou le **commutateur Ethernet** pour la couche liaison ; le **routeur** pour la couche réseau et la **passerelle** pour l'ensemble des 7 couches.
- Les protocoles **TCP** et **IP** situés respectivement dans les **couches 4 et 3** du modèle OSI sont utilisés sur la majorité des équipements pour l'interconnexion des réseaux locaux et à l'échelle d'Internet.
- **IP** est un protocole de niveau réseau responsable de la fragmentation des données, de la transmission des datagrammes en mode sans connexion, de l'adressage et du routage des paquets entre stations par l'intermédiaire de routeurs.
- Les **adresses IPv4**, codées sur 32 bits, sont exprimées en décimal et séparées par des points (137.15.223.2). Chaque machine possède dans son réseau une adresse unique. Le **masque** de réseau permet de préciser le nombre de bits dédiés à l'identification du réseau (**net_id**) et le nombre de bits réservés pour la numérotation des machines (**host_id**). Organisés à l'origine suivant la dimension en quatre classes (A , B , C et D), les réseaux IP sont aujourd'hui désignés grâce au couple adresse/préfixe (137.15.128.0/19) qui permet de désigner simplement l'importance du réseau. Pour pallier à la pénurie d'adresses IPv4, **l'adressage IPv6** permet d'étendre le nombre d'adresses en les codant sur 128 bits et en utilisant une notation du type : 805B:2D9D:0000:DC28:12F7:000A:765C:D4C8

Ce qu'il faut retenir!

- D'autres protocoles sont associés à IP : **ARP** pour la correspondance entre les adresses IP et les adresses physiques ; **ICMP** pour le contrôle du trafic IP ; **DHCP** pour la transmission dynamique des adresses IP aux clients.
- Le **routing** consiste à trouver des chemins dans les réseaux interconnectés à partir des adresses de destination. Les routeurs concernés doivent être capables de gérer ces chemins dans leurs tables de routage et de maintenir ces dernières à jour à l'aide de protocoles de routage spécifiques (RIP, OSPF, BGP ...).
- Le protocole de niveau transport **UDP** est non connecté et non fiable. Il permet de désigner simplement les numéros de port des applications utilisées avec des temps de réponse courts.
- Le protocole de transport **TCP** fonctionne en mode connecté, ses principales caractéristiques sont la segmentation et le réassemblage des messages, la retransmission en cas d'échec et le contrôle de flux.
- On distingue principalement **trois phases TCP** : l'ouverture de la connexion, le transfert des données et la fermeture. Des bits dans l'en-tête TCP (flags) des segments envoyés et reçus permettent de savoir dans quel état se trouve la machine émettrice ou réceptrice. **Des numéros de séquence et d'acquittement** dans l'en-tête TCP permettent à tout moment de connaître, dans les deux sens, le nombre d'octets envoyés et le nombre d'octets acquittés et donc de réguler le flux des données et de provoquer une retransmission en cas de perte.







THANK YOU

MASTER SYSTÈMES D'INFORMATION,
RÉSEAUX ET NUMÉRIQUE



Dauphine | PSL

UNIVERSITÉ PARIS

