iutenligne

Le catalogue de ressources pédagogiques
de l'enseignement technologique universitaire.

I.U.T. de Mulhouse – G.E.I.I.

RES3 - Réseaux

CM 5 – TD 3 – TD 4 :
Couches transport et réseau
Modèles TCP/IP et UDP/IP

IUT Institut Universitaire de Technologie de Mulhouse

Planning

- *CM 1 : Généralités Réseaux*
- *CM 2 : Topologie et supports de transmission*
  - *TD 1 : Débit et technologie ADSL*
- *CM 3 : Codage des informations et contrôle d'intégrité*
  - *TD 2 : Codage des informations et contrôle d'intégrité CRC*
- *CM 4 : Modèle OSI / Ethernet*
- **CM 5 : Couches transport et réseau (TCP/IP)**
  - TD 3 : Analyse de trames Ethernet / Adresse IP et masque de sous-réseaux
  - TD 4 : Adressage IP / Routage IP
- CM 6 : Réseaux WLAN et sécurité
  - TD 5 : Réseaux Wifi et sécurité
- CM 7 : Réseaux et bus de terrain
  - TD 6 : Réseaux et bus de terrain
    - TP 1 : Technologie ADSL
    - TP 2 : Analyse de trames et Encapsulation Ethernet
    - TP 3 : Configuration d'un réseau IP / Routage IP / Wifi
    - TP 4 : Réseaux et bus de terrain
    - TP 5 : TP Test
- CM 8 : Contrôle de connaissances

Jean-François ROTH
Enseignant Vacataire IUT de Mulhouse
Formateur/Consultant en réseaux et télécoms depuis 1999
Jean-Francois.ROTH@UHA.fr
JeanFrancoisROTH@MSN.com

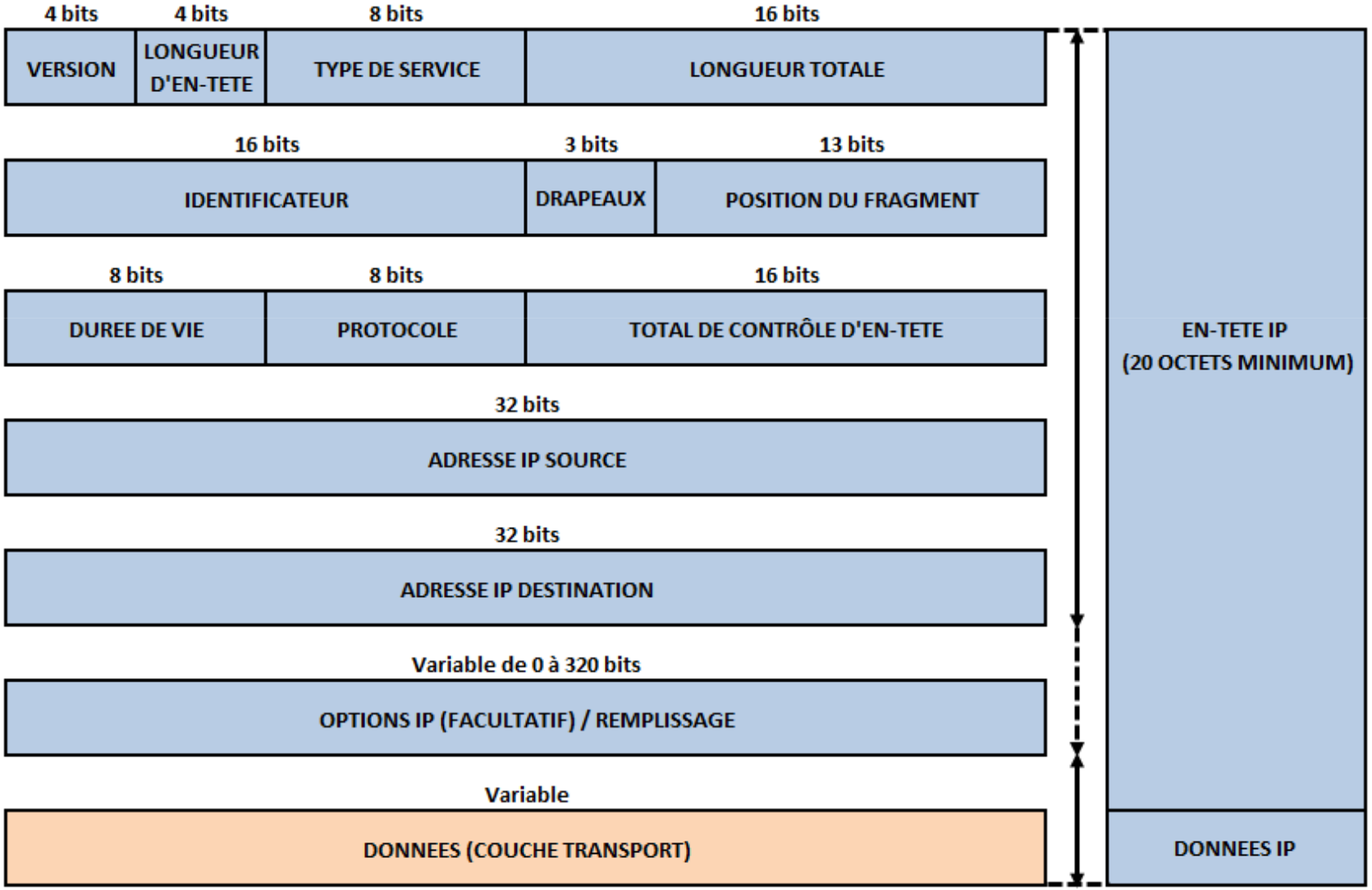
Sommaire

- Modèles TCP/IP et UDP/IP
  - Couche réseau : protocole IP
    - Protocole IP
    - Format de paquet (ou datagramme) IP v4
    - Adressage IP v4
    - Format de paquet (ou datagramme) IP v6
  - Couche réseau : protocole ARP
  - Couche réseau : protocole ICMP
  - Couche réseau : protocole DHCP
  - Couche réseau : routage IP
    - Portée des adresses logiques (réseaux) et physiques
    - Routage statique et routage dynamique
    - Algorithmes de routage
    - Saturation d'un routeur
  - Couche transport : protocole UDP
    - Format de message (ou datagramme) UDP
    - Encapsulation UDP/IP sur Ethernet
  - Couche Transport : protocole TCP
    - Format de segment TCP
    - Encapsulation TCP/IP sur Ethernet

Couche réseau : protocole IP

- Protocole IP (Internet Protocol)
  - Protocole réseau assurant
    - La transmission des données en mode sans connexion
    - L'adressage et le routage des paquets entre stations par l'intermédiaire de routeurs
    - La fragmentation des données
  - Fonctions
    - A l'émission
      - Identification du paquet
      - Détermination de la route à suivre (routage)
      - Vérification du type d'adressage (station ou diffusion)
      - Fragmentation de la trame si nécessaire
    - A la réception
      - Vérification de la longueur du paquet
      - Contrôle des erreurs
      - Réassemblage en cas de fragmentation
      - Transmission du paquet réassemblé au niveau supérieur

- Format de paquet (ou datagramme) IP v4

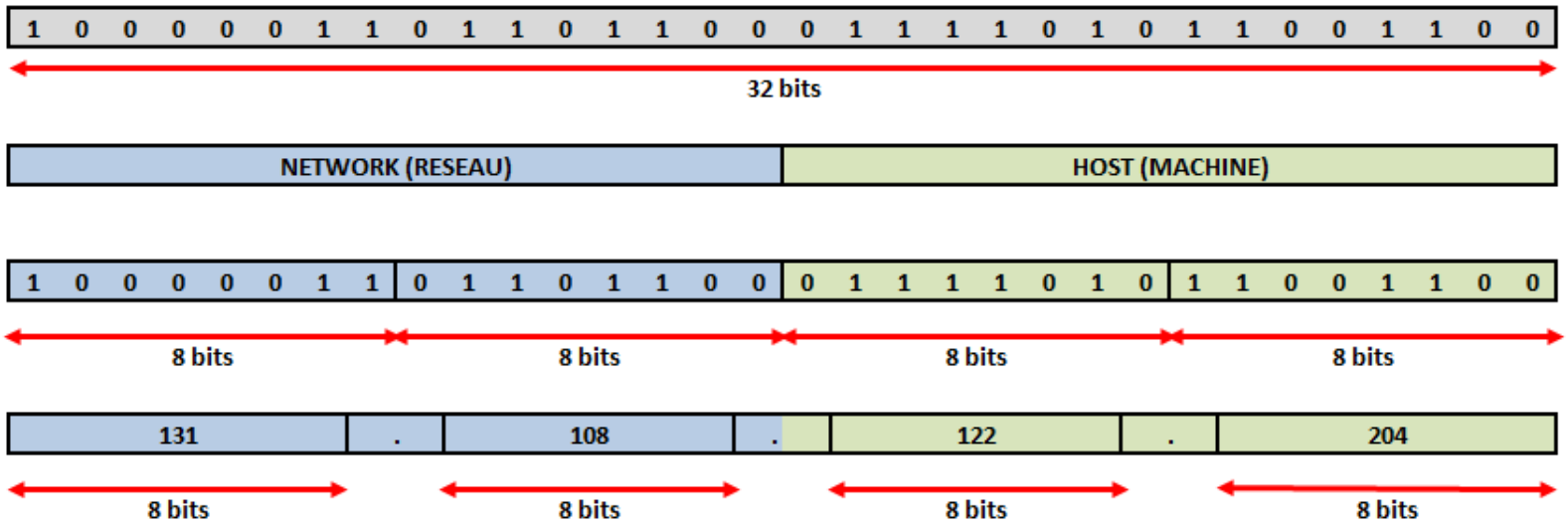


Couche réseau : protocole IP

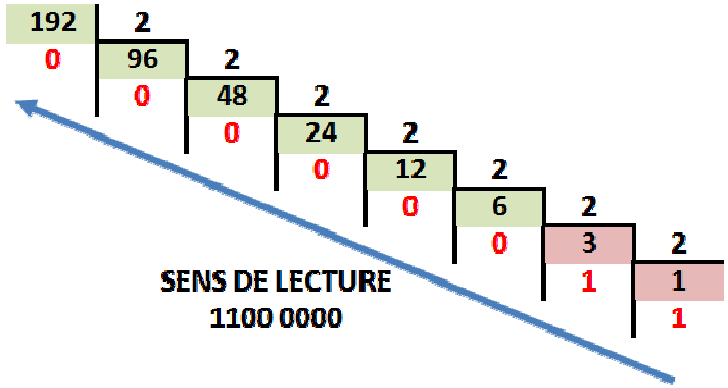
- Format de paquet (ou datagramme) IP v4
  - Descriptif des champs
    - Version : indique la version du protocole IP
      - 4 pour IP v4
    - Longueur de l'en-tête : indique le nombre de mots de 32 bits constituant l'en-tête
      - 5 pour une en-tête de 20 octets
    - Type de Service (TOS) : désigne la qualité de service utilisable par le routeur
      - Indicateur de fiabilité, de priorité, de délai et de débit
      - Champ peu utilisé
    - Longueur totale : longueur du paquet incluant l'en-tête et les données exprimée en octets
      - Permettant de spécifier une taille maximale de 65 535 octets
    - Identificateur : identifie le paquet pour la fragmentation
      - Tous les fragments d'un même paquet sont identifiés par le même numéro
    - Drapeaux : gère la fragmentation sur 3 bits sous la forme "0", "DF", "MF"
      - Le premier bit est positionné à 0
      - Le bit DF (don't fragment) demande au routeur de ne pas fragmenter le paquet
      - Le bit MF (more fragment) est positionné à 1 dans tous les fragments, sauf le dernier
    - Position du fragment (offset) : indique la position du fragment dans le paquet
      - La valeur du premier fragment est 0
      - Les fragments suivant sont exprimés en multiples de 8 octets sauf le dernier, exprimé sur 3 octets
      - Pouvant prendre une valeur maximale de 8189
        - 8189 x 8 octets + 3 octets pour le dernier fragment + 20 octets d'en-tête = 65 535 octets

- Format de paquet (ou datagramme) IP v4
  - Descriptif des champs
    - Durée de vie (Time To Live - TTL) : évite la circulation infinie des paquets sur le réseau
      - Valeur initiale variant de 32 à 256 en fonction de la taille du réseau
      - Décrémentée de 1 à chaque passage par un routeur
      - Un paquet dont la durée de vie passe à 0 est détruit
    - Protocole : indique le protocole de la couche supérieure (encapsulation)
      - 1 pour ICMP, 2 pour IGMP, 6 pour TCP, 17 pour UDP,…
    - Total de contrôle d'en-tête (checksum) : permet de vérifier la validité de l'en-tête
      - Concerne uniquement l'en-tête du paquet, pas les données véhiculées
      - Après calcul, le champ est censé contenir la valeur 0
    - Adresse IP source : adresse réseau de l'émetteur
      - Représentée en décimal pointé : 172.24.91.201
    - Adresse IP destination : adresse réseau du destinataire
      - Représentée en décimal pointé : 172.24.91.202
    - Options : utilisé pour le contrôle ou la mise au point
    - Données : véhicule le contenu du protocole de couche supérieure
      - Protocoles : ICMP, IGMP, TCP, UDP, …

- Adressage IP v4
  - Adressage Internet
    - Chaque machine connectée à un réseau local possède une adresse IP unique dans ce réseau
    - Les adresses sont codées sur 32 bits et exprimées par octet :
      - 4 nombres compris entre 0 et 255 notés en décimal et séparés par des points (notation décimal pointé) :
      - Exemple d'adresse IPv4 :131.108.122.204
    - Les adresses IP se décomposent en deux parties :
      - Le numéro de réseau (Network_ID ou Net_ID)
      - Le numéro de la machine sur le réseau (Host_ID)
        - Pour une adresse accédant à internet (IP publique), une autorité internationale l'ICANN (Internet Corporation for Assigned Names and Numbers) attribue les Net_ID et le FAI (Fournisseur d'Accès Internet) gère les Host_ID



- Adressage IP v4
  - Notation binaire
    - Notation indispensable pour assimiler le fonctionnement de l'adressage IP et des masques
    - Exemple : notation binaire de l'adresse IP 192.168.25.132
      - **192. 168. 25.132** soit **11000000.10101000.00011001.10000100**



1100 0000 :

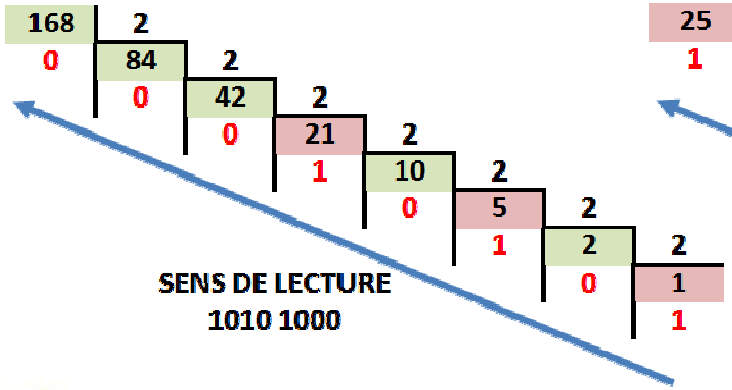
$2^7 \times 1 + 2^6 \times 1 + 2^5 \times 0 + 2^4 \times 0 + 2^3 \times 0 + 2^2 \times 0 + 2^1 \times 0 + 2^0 \times 0$

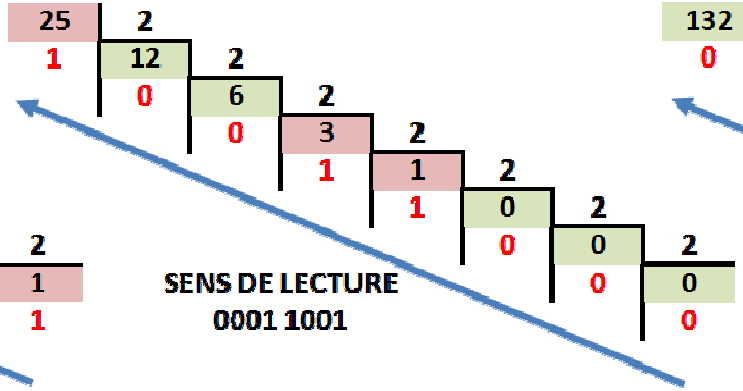
$2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 + 2 \times 2 \times 2 \times 2 \times 2 \times 2 + 0 + 0 + 0 + 0 + 0 + 0$

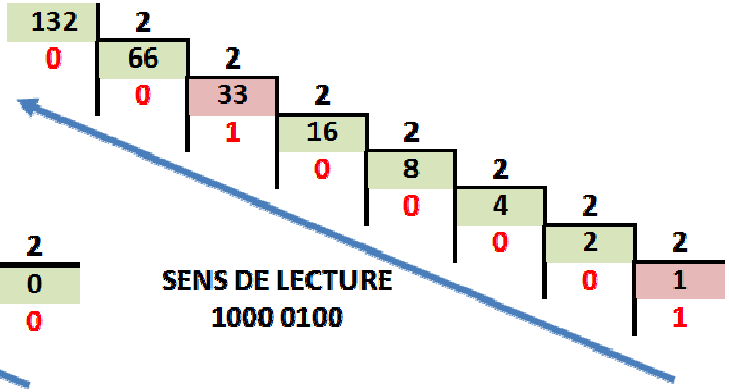
$128 + 64$

192

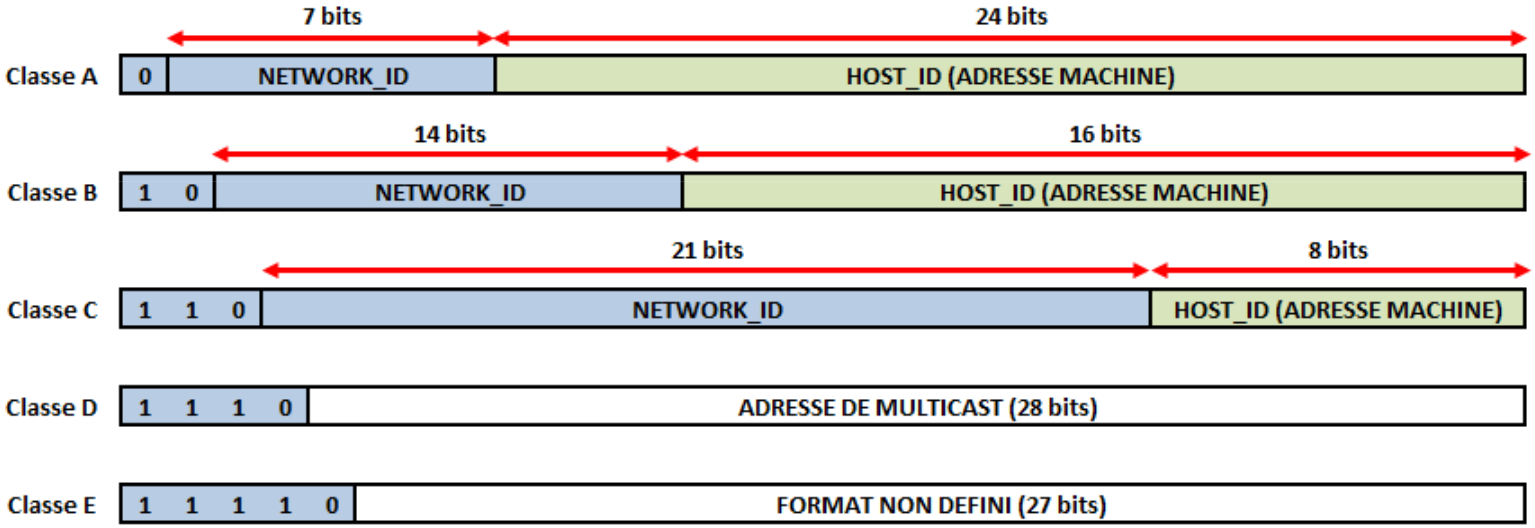
Binaire	1100	0000
Pseudo décimal	12	0
Héxadécimal	C	0







- Adressage IP v4
  - Classes d'adresses
    - Réseaux de plus ou moins grand envergure composés de plages d'adresses successives
      - Pour l'adressage public, en raison du manque d'adresses IP disponibles, les classes sont abandonnées au profit de l'adresse CIDR (Classless InterDomain Routing)

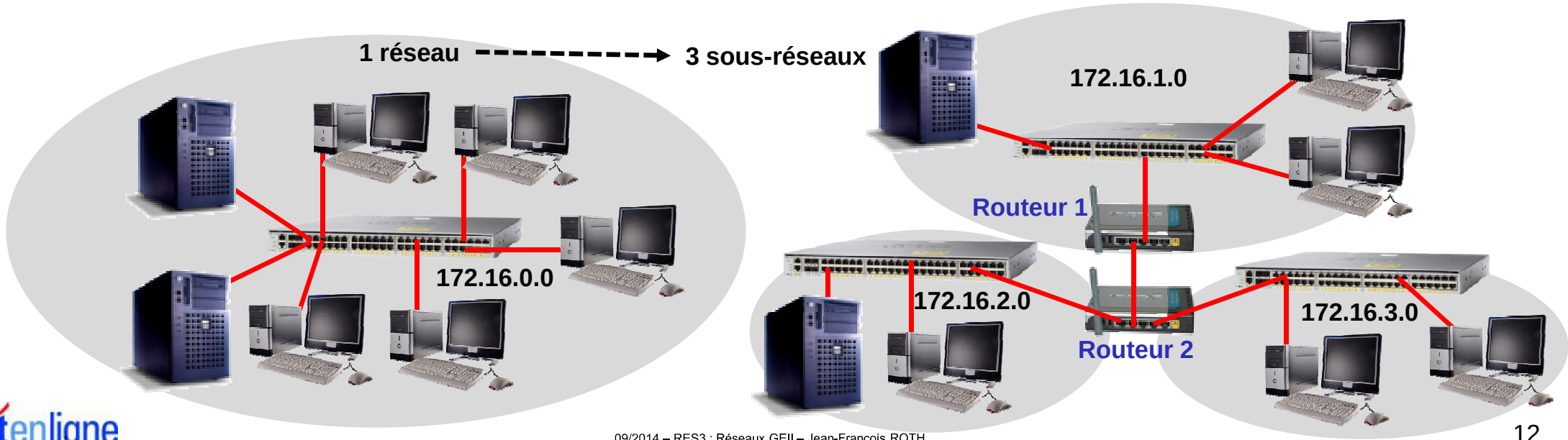


CLASSE	ADRESSES DE RESEAU	NOMBRE DE RESEAUX	NOMBRE DE MACHINES	NOTATION CIDR	MASQUE PAR DEFAUT
A	1.0.0.0 à 126.0.0.0	126	16 777 214	/8	255.0.0.0
B	128.0.0.0 à 191.255.0.0	16 382	65 534	/16	255.255.0.0
C	192.0.0.0 à 223.255.255.0	2 097 150	254	/24	255.255.255.0

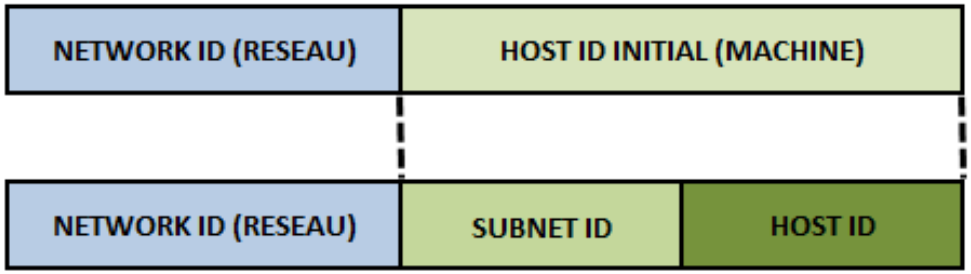
CLASSE	ADRESSES DE RESEAU	NOMBRE D'ADRESSES DE GROUPES	NOTATION CIDR
D	224.0.0.0 à 239.255.255.0	268 435 455	/4
E	240.0 .0.0 à 247.255.255.255	N/A	N/A

- Adressage IP v4
  - Adresses réservées ou particulières
    - Adresse IP = 0.0.0.0
      - Adresse non encore connue
      - Utilisée par une machine pour connaitre sa propre adresse IP au démarrage
    - Host ID avec tous les bits à 0
      - Désigne le réseau (ou sous-réseau) lui-même
      - Exemple : 212.92.27.0 pour une classe C
    - Host ID avec tous les bits à 1
      - Adresse de diffusion (broadcast) :
      - Désigne toutes les machines du réseau concerné
      - Exemple : 157.42.255.255 pour une classe B
    - Adresse IP = 255.255.255.255
      - Adresse de diffusion (broadcast)
      - Désigne toutes les machines mais l'adresse du réseau n'a pas besoin d'être connue
    - Adresse IP = 127.X.Y.Z
      - Adresse de bouclage (localhost ou loopback)
      - Utilisée pour des communications inter-processus sur le même ordinateur ou des tests de logiciels
      - Exemple : 127.0.0.1

- Adressage IP v4
  - Segmentation en sous-réseaux
    - Consiste à diviser le réseau en plusieurs sous-réseaux
      - Réduit le nombre de communications sur un même segment réseau
      - Connecte des réseaux d'architectures hétérogènes
      - Regroupe les ordinateurs en domaines ou sous-domaines
    - L'adressage IP permet de déterminer si un paquet est destiné à
      - Une machine du même réseau
      - Une machine d'un sous-réseau différent sur le même réseau
      - Une machine sur un autre réseau
        - Une passerelle (routeur) est nécessaire pour passer d'un sous-réseau à l'autre



- Adressage IP v4
  - Segmentation en sous-réseaux
    - Découpage du Host ID en deux parties réalisant la segmentation en sous-réseaux
      - Une adresse de sous-réseau (SubNet ID)
      - Une adresse de machine (Host ID)
    - Séparation entre l'adresse de sous-réseau et l'adresse machine
      - Réalisée à l'aide d'un masque de sous-réseau
    - Structuration employée dans les algorithmes de routage
      - Pour déterminer si deux machines se trouvent sur le même sous-réseau



- Adressage IP v4
  - Masque de sous-réseau (ou subnet mask)
    - Codé sur 32 bits et ayant le même format qu'une adresse IP
      - 4 nombres compris entre 0 et 255 notés en décimal et séparés par des points (décimal pointé) :
        - Exemple de masque de sous-réseau : 255.255.255.192
    - Distingue la partie de l'adresse utilisée pour le routage (réseau) et celle utilisable pour numéroter des équipements (ordinateurs, serveurs, imprimantes, …)
      - Les bits à 1 désignent la partie réseau (Net) et sous-réseau (Subnet) de l'adresse
      - Les bits à 0 désignent la partie numérotation des machines sur le sous-réseau (Host)
      - Masque de sous-réseaux par défaut :
        - Classe A : 255.0.0.0, Classe B : 255.255.0.0, Classe C : 255.255.255.0

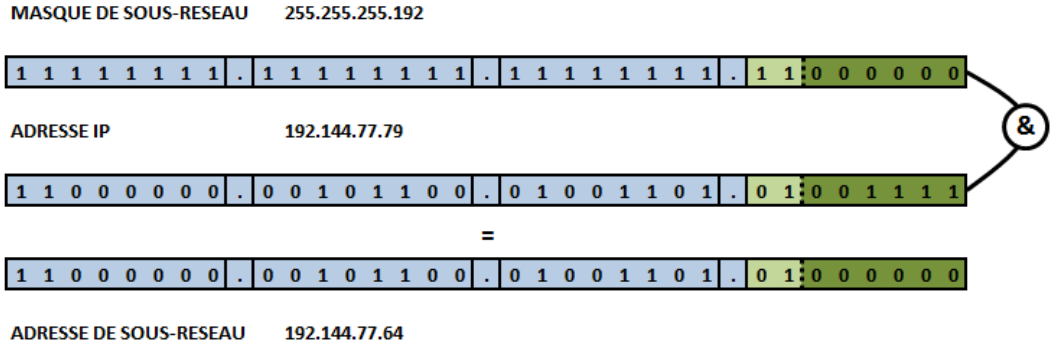
MASQUE DE RESEAU DE CLASSE C PAR DEFAUT :

ADRESSE IP	192.168.1.1
	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 0 0 0 0 1
MASQUE DE SOUS-RESEAU	255.255.255.0
	1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0
ID RESEAU	192.168.1.0
ID HOTES	1 à 254

MASQUE DE SOUS-RESEAU DE CLASSE C :

ADRESSE IP	192.168.1.1
	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 0 0 0 0 1
MASQUE DE SOUS-RESEAU	255.255.255.240
	1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 0 0 0 0
PREMIER ID RESEAU	192.168.1.0
ID HOTES	1 à 14
DEUXIEME ID RESEAU	192.168.1.16
ID HOTES	17 à 30
...	
DERNIER ID RESEAU	192.168.1.240
ID HOTES	241 à 254

- Adressage IP v4
  - Masque de sous-réseau (ou subnet mask)
    - Permet de séparer localement des sous-réseaux correspondant à des entités différentes
      - Exemple : administration, services techniques, …
      - Les sous-réseaux pourront être invisibles de l'extérieur
    - Permet de déterminer si un équipement (ou machine) est compris ou non dans un sous-réseau
      - Appliquer un "ET LOGIQUE" entre l'adresse de l'équipement et le masque permet de déterminer l'adresse de sous-réseau d'un équipement
        - Si deux équipements n'appartiennent pas au même sous-réseau ils doivent communiquer via une passerelle (routeur)
    - Exemple avec l'association adresse IP/masque 192.144.77.79/255.255.255.192 :



A	B	A ET B
0	0	0
0	1	0
1	0	0
1	1	1

    - Les deux premiers bits du dernier octet (bits à 1 du masque) sont utilisés pour identifier le sous-réseau
    - Le masque permet de distinguer 2^2 (car 2 bits à 1), soit 4 adresses de sous-réseaux :
      - 192.44.77.0, 192.44.77.64, 192.44.77.128, 192.44.77.192

- Adressage IP v4
  - Association adresse IP et masque de sous-réseau
    - Relation entre une machine ayant pour adresse 192.168.25.147 et un masque 255.255.255.0
      - Conversion du masque en binaire : 11111111.11111111.11111111.00000000
      - Les bits des trois premiers octets du masque à 1 identifient la partie réseau de l'adresse :
        - Soit 192.168.25.xxx
      - Les bits du dernier octet du masque à 0 indiquent que 8 bits ont été réservés pour l'adresse machine :
        - 2^8 = 256 adresses disponibles sur le réseau 192.168.25.xxx
      - Adresses disponibles pour les machines :
        - La plage d'adresse de 192.168.25.1 à 192.168.25.254
        - L'adresse 192.168.25.0 est réservée pour le réseau et est utilisée lors du routage
        - L'adresse 192.168.25.255 est réservée pour le broadcast et permet une diffusion à toutes les machines du réseau
    - Déterminer le nombre de machines installables dans un réseau
      - Choisir le masque de sous-réseau en fonction du nombre d'équipements à installer dans le réseau

MASQUE APPLIQUE A L'ADRESSE IP : 255.255.255.0 ENTRAINANT LA CREATION D'UN SEUL SOUS-RESEAU

ADRESSE DE SOUS-RESEAU	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
SOUS-RESEAU 1 : 254 ADRESSES DISPONIBLES	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255 ADRESSE DE BROADCAST

- Adressage IP v4
  - Association adresse IP et masque de sous-réseau
    - Exemple avec un masque permettant l'intégration de 60 machines dans le réseau 193.225.34.0
      - Réservation d'une adresse pour le réseau et d'une pour le broadcast, soit une nécessité de 62 adresses
      - La puissance de 2 supérieure à 62 est 64
      - Afin d'identifier 64 adresses, **6** bits sont nécessaires ($64 = 2^6$) :
        - Dans le masque **6** bits seront à **0** pour identifier la partie machine et les **26** autres bits seront à **1**
        - Masque associé : **11111111.11111111.11111111.11000000** soit 255.255.255.192 en décimal
        - Pour prévoir une éventuelle extension, il serait intéressant, si possible, de prévoir quelques adresses supplémentaires

MASQUE APPLIQUE A L'ADRESSE IP : 255.255.255.192 ENTRAINANT LA CREATION DE QUATRE SOUS-RESEAUX

ADRESSE DE SOUS-RESEAU	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
SOUS-RESEAU 1 : 62 ADRESSES DISPONIBLES	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	ADRESSE DE BROADCAST
ADRESSE DE SOUS-RESEAU	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	
SOUS-RESEAU 2 : 62 ADRESSES DISPONIBLES	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	ADRESSE DE BROADCAST
ADRESSE DE SOUS-RESEAU	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	
SOUS-RESEAU 3 : 62 ADRESSES DISPONIBLES	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	ADRESSE DE BROADCAST
ADRESSE DE SOUS-RESEAU	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	
SOUS-RESEAU 4 : 62 ADRESSES DISPONIBLES	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	ADRESSE DE BROADCAST

- Adressage IP v4
  - Détermination de l'appartenance d'une machine à un réseau
    - Déterminer si la machine192.168.25.**47**/255.255.255.**248** appartient au réseau 192.168.25.**32** :
      - Conversion du masque en binaire : 11111111.11111111.11111111.**11111**000
      - La différentiation réseau/machine va se faire sur le quatrième et dernier octet
        - Les trois premiers octets du masque ayant tous leurs bits à 1 ne sont pas significatifs
      - Les **5 premiers bits** du quatrième octet sont à **1** et représentent la partie réseau
      - Pour le réseau, le dernier octet a pour valeur **32** soit **00100**000
      - Pour la machine, le dernier octet a pour valeur **47** soit **00101**111
      - Les **5 premiers bits** de ces deux derniers octets ne sont pas identiques : **00100** différent de **00101**
      - La machine 192.168.25.47 avec le masque 255.255.255.248 n'appartient pas au réseau 192.168.25.32

    - Déterminer si la machine A (192.168.0.20) et la machine B (192.168.0.185) sont sur le même réseau que la machine C (192.168.0.140) en appliquant le masque 255.255.255.128 :
      - Machine A : 192.168.0.**20** ET 255.255.255.**128**
        - **00010100** ET **10000000** = **00000000** = 0
        - La machine A appartient au réseau 192.168.0.0
      - Machine B : 192.168.0.**185** ET 255.255.255.**128**
        - **10111001** ET **10000000** = **10000000** = 128
        - La machine B appartient au réseau 192.168.0.128
      - Machine C : 192.168.0.**140** ET 255.255.255.**128**
        - **10001100** ET **10000000** = **10000000** = 128
        - La machine C appartient au réseau 192.168.0.128
      - Les résultats sont identiques pour la machine C et la machine B :
        - La machine B appartient au même réseau que la machine C mais la machine A appartient à un réseau différent

- Adressage IP v4
  - Détermination de la plage d'adresses à partir d'un masque
    - Le masque doit être associé à une adresse IP pour avoir une signification
    - Le choix de la plage d'adresses sur laquelle un masque est appliqué est important

➢ Exemple avec le masque 255.255.255.128 permettant d'identifier 126 machines :

- Les trois premiers octets des adresses sont fixés par le masque (exemple : 192.237.11.xxx)
- La différentiation du réseau va se faire sur le premier bit du dernier octet de l'adresse
  - Si ce bit est à 0 cela correspondra aux adresses de 0 à 127
  - Si ce bit est à 1 cela correspondra aux adresses de 128 à 255
- Choisir une plage d'adresses allant de 32 à 160 serait une erreur
  - Les adresses de 32 à 127 auraient, en binaire, le premier bit de leur dernier octet à 0
  - Les adresses de 128 à 160 auraient, en binaire, le premier bit de leur dernier octet à 1
  - Elles seraient considérées comme étant dans deux réseaux différents
- L'adressage des 126 machines ne doit pas être choisi aléatoirement
  - Les choix possibles pour la plage d'adresses des machines sont de 1 à 126 ou de 129 à 254

MASQUE APPLIQUE A L'ADRESSE IP : 255.255.255.128 ENTRAINANT LA CREATION DE DEUX SOUS-RESEAUX

ADRESSE DE SOUS-RESEAU	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
SOUS-RESEAU 1 : 126 ADRESSES DISPONIBLES	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
ADRESSE DE SOUS-RESEAU	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
SOUS-RESEAU 2 : 126 ADRESSES DISPONIBLES	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

ADRESSE DE BROADCAST

ADRESSE DE BROADCAST

- Adressage IP v4
  - Détermination des adresses de réseau utilisables
    - Méthode permettant de déterminer les adresses de réseau utilisées pour le routage :
      - Appliquer le masque en fonction du nombre de machines à intégrer dans le réseau
      - Appliquer la formule **256 - valeur octet significatif = X**
        - Un octet significatif d'un masque a une valeur différente de 255
      - L'adresse de réseau devra être un multiple de **X**
    - Exemple avec l'intégration de 50 machines dans un réseau utilisant le masque 255.255.255.**192**
      - Le dernier octet est significatif : 256 – valeur octet significatif = **256 – 192 = 64.**
      - Le dernier octet de l'adresse de réseau doit être un multiple de **64**.
      - Pour la plage 10.0.0.0/255.255.255.192 les adresses de réseau utilisables sont :
        - 10.0.0.0
        - 10.0.0.64
        - 10.0.0.128
        - 10.0.0.192

MASQUE APPLIQUE A L'ADRESSE IP : 255.255.255.192 ENTRAINANT LA CREATION DE QUATRE SOUS-RESEAUX

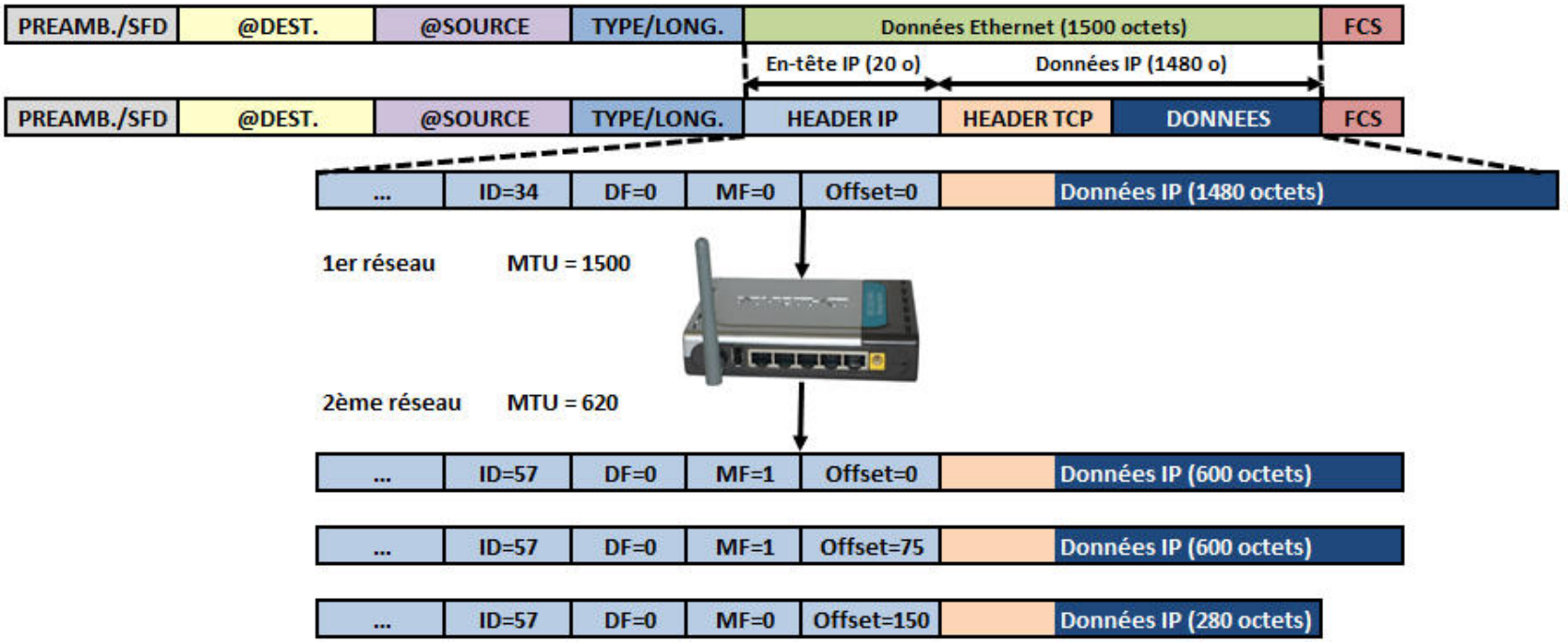
ADRESSE DE SOUS-RESEAU	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
SOUS-RESEAU 1 : 62 ADRESSES DISPONIBLES	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	ADRESSE DE BROADCAST
ADRESSE DE SOUS-RESEAU	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	
SOUS-RESEAU 2 : 62 ADRESSES DISPONIBLES	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	ADRESSE DE BROADCAST
ADRESSE DE SOUS-RESEAU	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	
SOUS-RESEAU 3 : 62 ADRESSES DISPONIBLES	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	ADRESSE DE BROADCAST
ADRESSE DE SOUS-RESEAU	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	
SOUS-RESEAU 4 : 62 ADRESSES DISPONIBLES	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	ADRESSE DE BROADCAST

- Adressage IP v4
  - Découpage d'une plage réseau en somme de plusieurs plages
    - Exemple avec la plage d'adresses de 69.0.0.0 à 79.255.255.255 en optimisant le routage
      - La valeur du premier octet varie de 69 à 79, prenant 11 valeurs
        - Un plage de 11 octets ne peut pas être définie avec un seul réseau et doit être découpée en plusieurs réseaux
        - Une plage doit impérativement être un multiple de 2
        - La première puissance de 2 inférieure à 11 est 8 et le seul multiple de 8 sur cette plage est 72
        - Possibilité de décrire un réseau dont le premier octet varie de 72 à 79
        - Le nombre de plages couvertes étant 8, on applique la formule 256 – 8 = 248
        - Le réseau 72.0.0.0/248.0.0.0 permet de décrire la première plage d'adresses
      - La plage d'adresses allant de 69.0.0.0 à 71.255.255.255, avec un premier octet prenant 3 valeurs
        - La première puissance de 2 inférieure à 3 est 2 et le seul multiple de 2 de cette plage est 70
        - Possibilité de décrire un réseau dont le premier octet varie de 70 à 71
        - Le nombre de plages couvertes étant 2, on applique la formule 256 – 2 = 254
        - Le réseau 70.0.0.0/254.0.0.0 permet de décrire la deuxième plage d'adresses
      - La plage d'adresses allant de 69.0.0.0 à 69.255.255.255
        - Le réseau 69.0.0.0/255.0.0.0 permet de décrire la troisième et dernière plage d'adresses
      - La plage d'origine allant de 69.0.0.0 à 79.255.255.255 est découpée en trois sous-réseaux :
        - 69.0.0.0/255.0.0.0
        - 70.0.0.0/254.0.0.0
        - 72.0.0.0/248.0.0.0
      - Des masques à 255.0.0.0 auraient permis d'utiliser 11 réseaux, mais cette solution n'est pas optimisée pour le routage

- Adressage IP v4
  - Découpage d'une plage d'adresses en plusieurs sous-réseaux
    - Exemple avec un réseau 193.225.34.0/255.255.255.0 dans lequel on souhaite créer un sous-réseau de 70 machines, un deuxième de 44 machines et un troisième de 20 machines
      - Pour 70 machines, réserver 126 adresses à l'aide du masque 255.255.255.128 (256 – 128 = 128)
      - Pour 44 machines, réserver 62 adresses à l'aide du masque 255.255.255.192 (256 – 64 = 192)
      - Pour 20 machines, réserver 30 adresses à l'aide du masque 255.255.255.224 (256 – 32 = 224)
        - Pour chaque plage, il est nécessaire d'avoir une adresse pour le routage et une adresse pour le broadcast
      - Placement des trois plages de 128, 64 et 32 adresses dans une plage de 254 adresses disponibles
        - En positionnant toujours la plage la plus grande en premier afin de pouvoir placer la totalité des plages
      - Pour la première plage de 126 adresses :
        - Soit les adresses de 1 à 126 ou de 129 à 254, les deux choix sont envisageables, plage choisie : de 0 à 127
        - Le premier sous-réseau sera caractérisé par 193.225.34.0/255.255.255.128
      - Pour la seconde plage de 62 adresses :
        - Soit les adresses de de 129 à 190 ou de 193 à 254, les deux sont envisageables, plage choisie : de 128 à 191
        - Le second sous-réseau sera caractérisé par 193.225.34.128/255.255.255.192
      - Pour la troisième plage de 30 adresses :
        - Soit les adresses de 193 à 223 ou de 225 à 254 , les deux sont envisageables, plage choisie : de 192 à 223
        - Le dernier sous-réseau sera caractérisé par 193.225.34.192/255.255.255.224
      - Le réseau d'origine 193.225.34.0/255.255.255.0 a été découpé en trois sous-réseaux
        - 193.225.34.0/255.255.255.128
        - 193.225.34.128/255.255.255.192
        - 193.225.34.192/255.255.255.224
        - Une plage de 30 adresses non utilisées de 225 à 254 reste disponible (193.225.34.224/255.255.255.224)

- Adressage IP v4
  - Contigüité des bits à 1 d'un masque
    - Pas obligatoire mais respecter cette règle facilite l'exploitation du réseau
      - En conservant la contiguïté des bits, les adresses des machines au sein du réseau se suivent
      - Avec des bits non contigus, les adresses des machines au sein du réseau ne se suivent plus
    - Exemple avec le masque 255.255.254.1 représentant 11111111.11111111.11111110.00000001
      - Les 8 bits à 0 représentent toujours la partie machine mais ne sont plus à la même position
      - Les machines ayant des adresses dont le dernier bit est à 1 ne seront pas dans le même réseau que celles dont le dernier bit est à 0 :
        - Les machines avec des adresses impaires ne seront pas dans le même réseau que celles avec des adresses paires
        - Différencier les adresses paires et impaires reste simple, mais en cas de mélanges plus complexes entre les bits significatifs, les réseaux deviennent ingérables
    - Respecter la contiguïté des bits significatifs simplifie la gestion des réseaux
      - 11111111 (255 en décimal)
      - 11111110 (254 en décimal)
      - 11111100 (252 en décimal)
      - 11111000 (248 en décimal)
      - 11110000 (240 en décimal)
      - 11100000 (224 en décimal)
      - 11000000 (192 en décimal)
      - 10000000 (128 en décimal)
      - 00000000 (0 en décimal)

- Adressage IP v4
  - Fragmentation des paquets (ou datagrammes) IP
    - Nécessaire si des réseaux connectés à un même routeur ont des longueurs maximales de trames MTU (Maximum Transfer Unit) différentes
    - Exemple :
      - Avec un 1er réseau caractérisé par un MTU de 1500 octets et le 2nd par un MTU de 620 octets :
        - Le routeur découpe le paquet initial en 3 fragments
        - Le routeur positionne le bit MF = 1 pour les 2 premiers fragments et le bit MF = 0 pour le dernier fragment
        - Le premier octet du deuxième fragment correspondra à l'octet 600 (1er fragment : octets 0 à 599)
        - La position du fragment (offset) étant exprimée en multiple de 8 octets, la valeur d'offset pour le deuxième fragment sera de 75 (soit 600/8)



- Adressage IP v4
  - Attribution des adresses
    - Le nombre d'adresses IP attribuées a suivi une croissance exponentielle conduisant à une saturation
      - L'adressage sur 32 bits permettant 2^{32} = 4.29 milliards d'adresses semblait initialement suffisant
    - Les classes d'adresses ont généré un gaspillage important
      - Exemple : les classes A sous utilisées
  - Solutions pour pallier temporairement à la pénurie
    - Réattribution des blocs d'adresses inutilisés grâce au protocole CIDR (Classless InterDomain Routing)
    - Utilisation d'adresses privées et de système de translation d'adresses NAT (Network Address Translation)
  - En parallèle, la norme IP v6 remplace progressivement la version 4
    - Codage des adresses sur 128 bits (soit 16 octets)
    - Utilisée principalement pour les adresses IP publiques (Internet)

- Adressage IP v4
  - La division des classes d'adressage Classless InterDomain Routing (CIDR)
    - Permet une meilleure gestion des adresses existantes
      - Solution palliative alternative à la pénurie d'adresses IP v4 en attendant la généralisation de IP v6
    - Consiste à diviser les classes d'adressages en blocs plus petits
      - Seules les adresses publiques de classes C peuvent encore être attribuées et certaines entreprises ont besoin de plus de 256 adresses
    - Permet d'agréger des classes C ou d'affecter uniquement une partie d'une classe B en utilisant des préfixes
      - Exemple : indiquer aux routeurs qu'un seul sous-réseau correspond à 3 classes C
    - Permet de s'affranchir du découpage arbitraire et peu flexible en classes
      - Allocation des ressources plus fine et les tables de routages sont allégées au cœur du réseau
    - Représentée par l'adresse du réseau suivie du suffixe indiquant le nombre de bit à 1 du masque
      - 193.127.32.0 / 24 désigne le couple 193.127.32.0 & 255.255.255.0
      - 193.127.33.0 / 24 désigne le couple 193.127.33.0 & 255.255.255.0
      - Les deux réseaux 193.127.32.0 et 193.127.33.0 sont agrégés en 193.127.32.0 & 255.255.254.0
      - L'agrégat est noté 193.127.32.0 / 23 désignant le couple préfixe / nombre de bits à 1 du masque

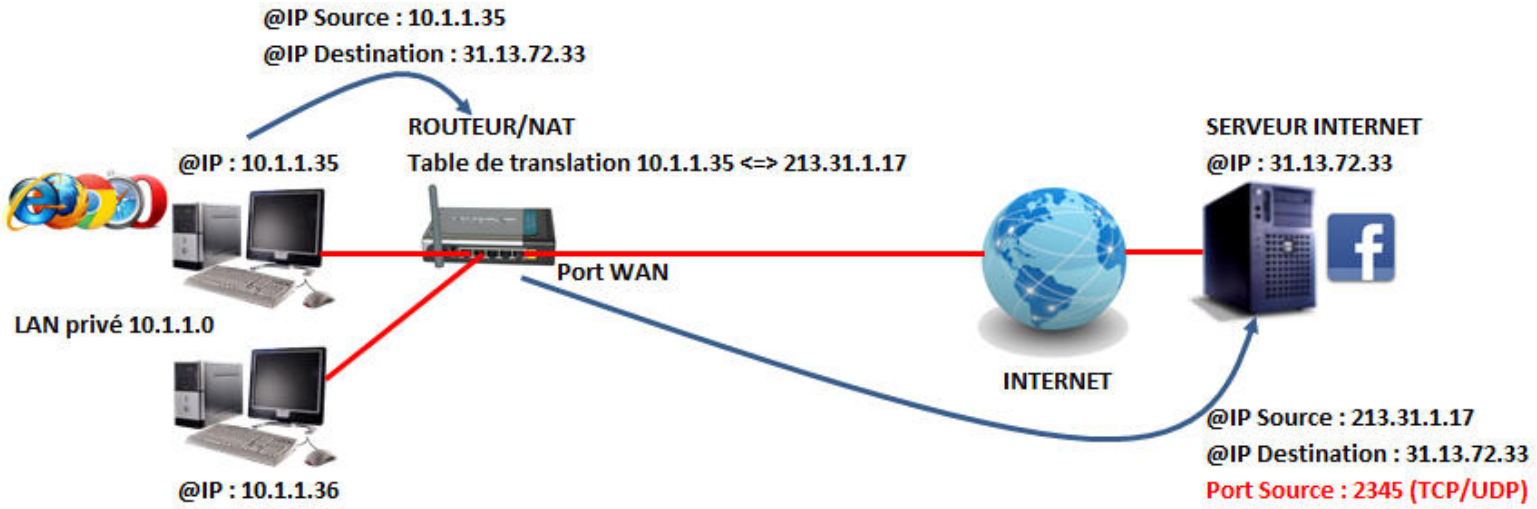
- Adressage IP v4
  - La division des classes d'adressage Classless InterDomain Routing (CIDR)
    - Les suffixes réseau étant de taille variable, les Fournisseurs d'Accès Internet (FAI) peuvent allouer à leurs clients un espace d'adressage adapté à leur besoin

    - Exemples
      - Pour un FAI disposant du bloc d'adresses 206.0.64.0 / 1 :
        - 2^{14} (16384) adresses individuelles ou 64 réseaux de 256 machines
      - Un client d'un FAI demandant 800 adresses peut se voir assigner :
        - Soit une classe B et dans ce cas environ 64700 adresses sont alors perdues (solution inadaptée)
        - Soit 4 classes C et dans ce cas 4 routes devront être rentrées dans ses tables de routage (solution inadaptée)
        - Soit le bloc 206.0.68.0 / 22 soit 1024 adresses (solution adaptée utilisant CIDR)

    - Association préfixe et masque de sous-réseau
      - La notation CIDR étant rapide à écrire, elle peut également être utilisée pour représenter les masques

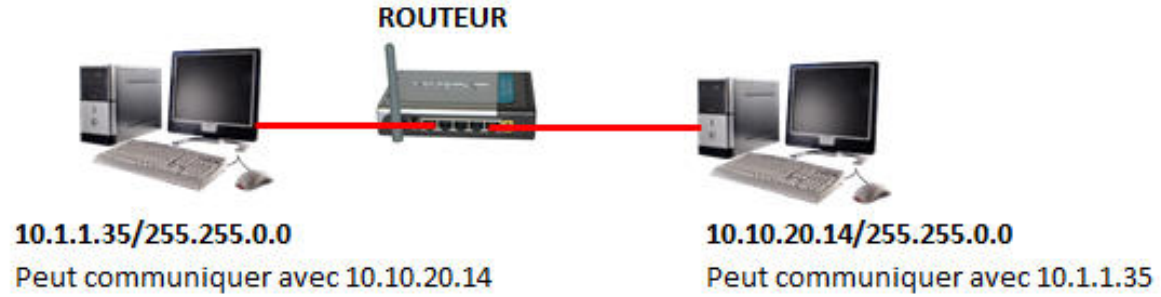
Préfixe	Masque	Nb de sous-réseaux	Nb d'hôtes
/24	255.255.255.0	1	254
/25	255.255.255.128	2	126
/26	255.255.255.192	4	62
/27	255.255.255.224	8	30
/28	255.255.255.240	16	14
/29	255.255.255.248	32	6
/30	255.255.255.252	64	2

- Adressage IP v4
  - La translation d'adresse Network Address Translation (NAT)
    - Translation statique
      - Consiste à associer une adresse IP publique à une adresse IP privée interne au réseau
      - La passerelle (routeur) associe une adresse IP publique routable sur Internet à une adresse IP privée et réaliste la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP
    - Translation dynamique
      - Solution palliative alternative à la pénurie d'adresses IP v4
      - Permet de partager une ou plusieurs adresse(s) IP routable(s) entre plusieurs machines d'un réseau privé
      - Toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP
      - Partage des différentes adresses IP sur une ou plusieurs adresses IP routables en utilisant le mécanisme de translation de port (Port Address Translation ou PAT)
        - Affectation d'un port source différent à chaque requête afin de maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des équipements sur Internet adressées à l'adresse IP de la passerelle



- Adressage IP v4
  - Règle de visibilité
    - Deux machines connectées via un concentrateur (couche 1) ou commutateur (couche 2) avec des adresses de réseaux différents ne peuvent pas communiquer ensemble

    - Deux machines connectées via un routeur (couche 3) correctement paramétré avec des adresses de réseaux différents peuvent communiquer ensemble



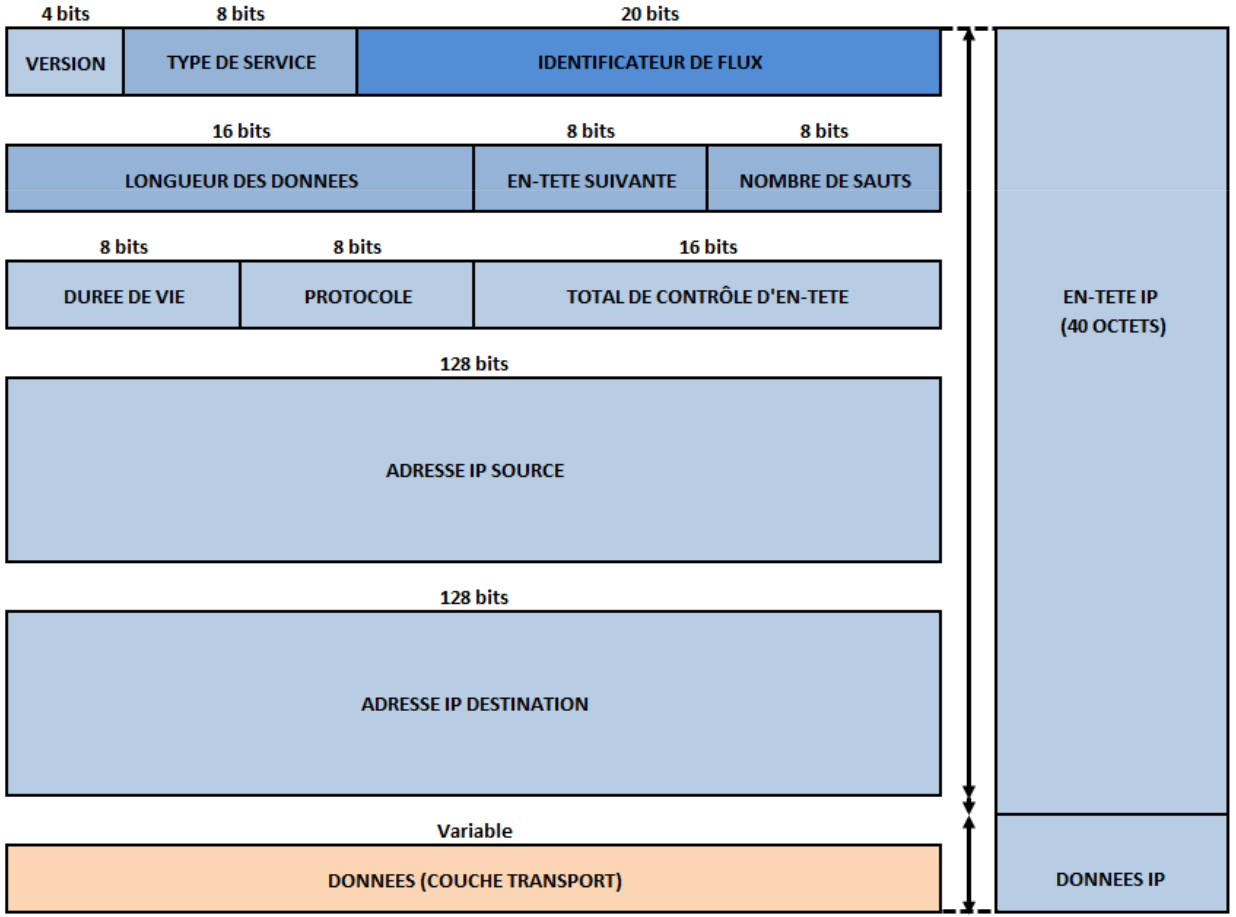
- Adressage IP v4
  - Exemple d'analyse IP

```
Frame 75: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: Dell_ef:ea:36 (00:21:70:ef:ea:36), Dst: Hewlett-_5d:a3:95 (00:12:79:5d:a3:95)
Internet Protocol Version 4, Src: 10.30.2.107 (10.30.2.107), Dst: 10.30.2.164 (10.30.2.164)
    Version: 4
    Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 1500
    Identification: 0x0d6e (3438)
  Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  Header checksum: 0xce63 [correct]
    Source: 10.30.2.107 (10.30.2.107)
    Destination: 10.30.2.164 (10.30.2.164)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 56866 (56866), Dst Port: healthd (1281), Seq: 2921, Ack: 1, Len: 1460
FTP Data
```

```
0000  00 12 79 5d a3 95 00 21  70 ef ea 36 08 00 45 00   ..y]...! p..6..E.
0010  05 dc 0d 6e 40 00 80 06  ce 63 0a 1e 02 6b 0a 1e   ...n@... .c...k..
0020  02 a4 de 22 05 01 2f 87  9a 33 1a b7 1f 6c 50 10   ..."../. .3...lP.
0030  80 00 e3 53 00 00 a6 f1  01 6b 40 06 04 60 75 43   ...S.... .k@..`uC
0040  60 04 24 30 02 1e 38 02  38 d0 02 05 70 4a dc 90   `.$0..8. 8...pJ..
0050  06 97 b1 05 2f a0 05 18  b0 82 2c d8 82 18 f0 02   ..../... ..,.....
0060  66 81 24 c3 14 05 7b a0  07 dc 40 07 7c c0 ff 07   f.$...{. ..@.|...
0070  76 b0 83 3b b8 75 dc 90  04 39 c8 83 3b c8 01 dc   v..;.u.. .9..;...
0080  00 05 54 b0 02 48 88 84  74 50 82 64 10 06 dc b0   ..T..H.. tP.d....
0090  02 47 20 84 3b b8 02 4f  78 04 3a 28 85 98 b3 05   .G .;..O x.:(....
00a0  6e c2 0a 42 c0 02 5e e1  00 0e 30 3a 8c e4 15 32   n..B..^. ..0:...2
00b0  d8 14 de 30 08 78 50 0d  32 58 07 6c 58 07 ce 84   ...0.xP. 2X.lX...
00c0  24 24 a1 02 30 12 63 62  58 87 62 18 20 2c 10 05   $$..0.cb X.b. ,..
00d0  2d 20 08 53 10 16 76 58  42 76 28 16 c5 f5 15 dc   - .S..vX Bv(.....
00e0  d0 02 27 90 06 5a 11 88  09 62 69 75 78 56 43 d7   ..'..Z.. .biuxVC.
00f0  0a 6f 80 16 6a 60 02 37  d5 16 3f 30 06 2d 80 45   .o..j`.7 ..?0.-.E
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 162 Displayed: 59 Marked: 0 Load time: 0:00.015 | Profile: Default

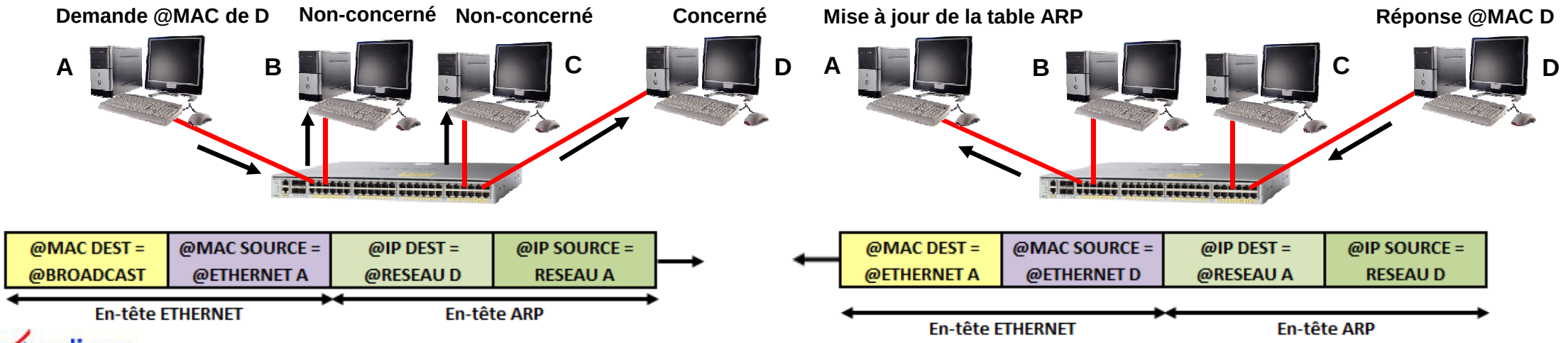
- Format de paquet (ou datagramme) IP v6
  - En-tête IP v6
    - L'en-tête du paquet IP v6 est de taille fixe : 40 octets
      - La taille minimale de l'en-tête IP¨v4 est de 20 octets
        - Des options, rarement implémentées en pratique, pouvant l'augmenter jusqu'à 60 octets



- Format de paquet (ou datagramme) IP v6
  - Signification des champs
    - Version (4 bits) : fixé à la valeur du numéro de protocole réseau
      - 6 pour IP v6
    - Classe de trafic (8 bits) : utilisé pour la qualité de service
      - Annonce le type de paquet et spécifie le comportement souhaité de la part des routeurs
    - Identificateur de flux (20 bits) : identifie les paquets appartenant à un même flux de données
      - Le routeur n'a qu'à lire ce champ pour déterminer l'appartenance d'un paquet
        - Permet un acheminement plus rapide des paquets
      - Contenu lié aux adresses source et destination ainsi qu'aux ports source et destination
    - Longueur des données (16 bits) : contient la longueur des données en octets
      - Ne prend pas en compte la longueur de l'en-tête (contrairement à IP v4).
    - En-tête suivante (8 bits) : identifie le protocole de niveau supérieur ou une extension
      - Indique le protocole de niveau supérieur (encapsulation) : ICMP, UDP, TCP, ...
        - Même convention qu'en IP v4
      - Extension : des options peuvent être précisées dans un ou plusieurs en-têtes complémentaires
    - Nombre de sauts (8 bits) : équivalent du TTL dans IP v4
      - Décrémenté de 1 à chaque passage dans un routeur
      - Le paquet est détruit si la valeur du champ atteint 0
    - Adresse IP source (128 bits) : adresse réseau source
    - Adresse IP destination (128 bits) : adresse réseau destination
    - Un en-tête IP v6 peut être suivi d'un ou plusieurs en-têtes d'extension (complémentaire)
      - Exemple : l'en-tête de routage permettant à la source de spécifier un chemin déterminé à suivre

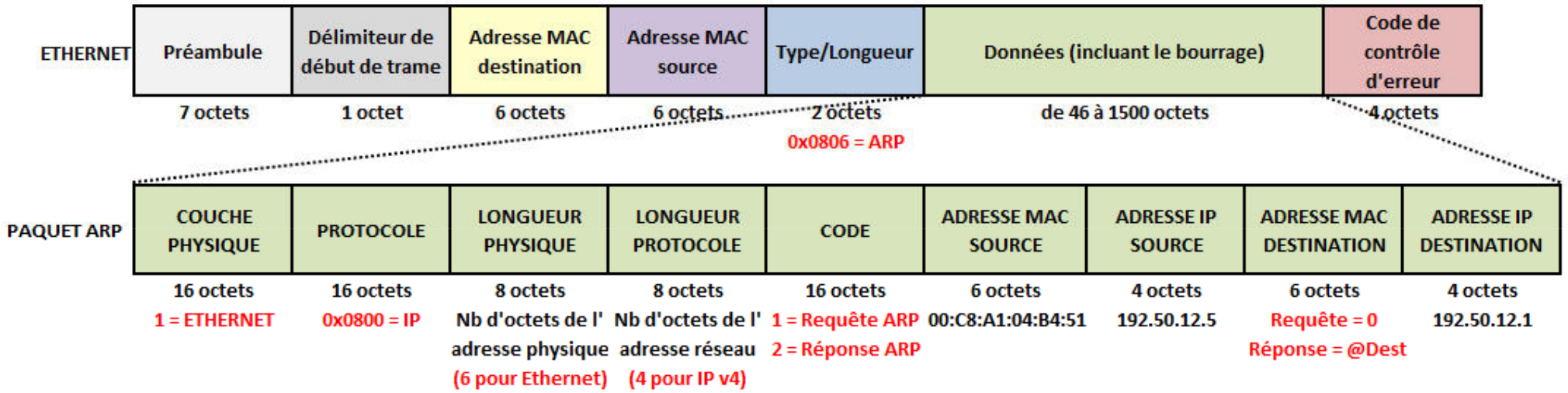
- Format de paquet (ou datagramme) IP v6
  - Apports d'IP v6
    - Capacités d'adressage plus importants :
      - Adresse sur 128 bits au lieu de 32 bits pour IP v4
      - Exemple : FEDC:BA98:7654:3210:EDBC:A987:6543:210F
    - Hiérarchie d'adressage plus riche en prenant en compte différentes configurations
    - Auto configuration (plug-and-play) possible des adresses
    - Gestion de la mobilité (IP mobile)
    - En-tête de base plus simple (moins de champs) facilitant le traitement dans les routeurs
    - En-tête d'extension pouvant être rajoutées pour prendre en compte de nouvelles fonctionnalités
    - Mécanisme de sécurité (authentification et confidentialité)
    - Possibilité de routage commandé par la source
    - Possibilité d'identification de flot (flow label)
  - Fonctionnement d'IP v6
    - Fonctionnement très similaire à celui d'IP v4
    - Les protocoles de transport TCP et UDP sont pratiquement inchangés
    - Se résume par la formule "96 bits de plus, rien de magique"

- Protocole ARP (Address Resolution Protocol)
  - Réalise la correspondance entre adresses réseaux (IP) et adresses physiques (MAC)
    - L'adresse physique (MAC) est associée à la carte réseau
    - L'adresse réseau (IP) n'est nécessaire que lorsque une machine se connecte à un réseau IP
  - Exemple avec a machine émettrice A souhaitant envoyer un paquet au destinataire D
    - La machine A connait l'adresse IP du destinataire D mais pas son adresse MAC
      - Le paquet doit être encapsulé dans une trame de niveau 2 (Ethernet, Wifi, …)
      - La machine A envoie une requête ARP dans une trame ayant avec une adresse MAC de diffusion générale (broadcast) pour que toutes les stations du réseau la reçoive
      - La couche ARP de la machine destinataire D reconnaît que cette requête lui est destinée et répond par une réponse ARP contenant son adresse MAC alors que les autres stations ignorent la requête
      - La réponse ARP est reçue par la machine A; lui permettant de mettre à jour sa table ARP et d'envoyer directement les futurs paquets à la bonne adresse MAC de destination



Couche réseau : protocole ARP

- Protocole ARP (Address Resolution Protocol)
  - Encapsulation ARP sur Ethernet



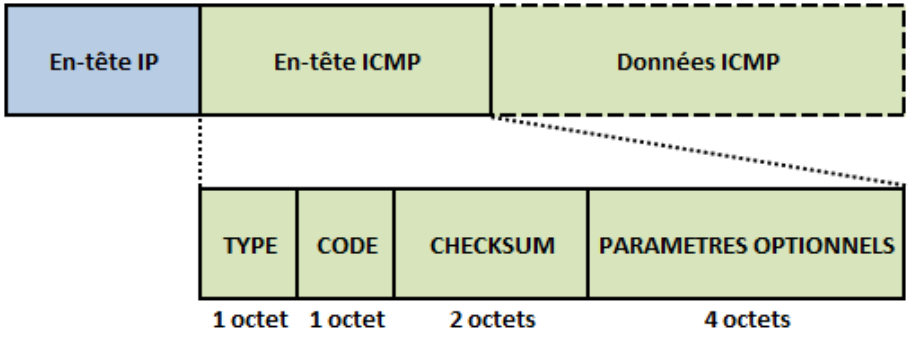
Couche réseau : protocole ICMP

- Protocole ICMP (Internet Control Message Protocol)
  - Contrôle le trafic IP
    - Contrôle de flux
      - Le destinataire envoie un message de congestion si les datagrammes arrivent trop vite pour être traités
      - Ce message indique à la source de suspendre temporairement l'envoi
    - Détection de destination inaccessible
      - L'équipement détectant le problème envoie un message "Destination Unreachable" à la source
    - Redirection des voies
      - Message de redirection envoyé par une passerelle
      - Permet d'indiquer à une machine d'utiliser une autre passerelle, constituant un meilleur choix
    - Vérification des machines hôtes à distance
      - Message d'écho ICPM envoyé par une machine-hôte à l'aide d'une commande de type "PING"
      - Permet de vérifier que l'adresse et la couche IP du système distant sont opérationnelles
        - Exemple : PING 192.50.12.1 permet de vérifier que l'adresse réseau est présente et opérationnelle sur le réseau
    - Détection du temps expiré
      - Les paquets circulant en boucle sont identifiés grâce au champs TTL (Time To Live) de l'en-tête IP
    - Détection de paramètre incorrect
      - La structure du paquet IP n'est pas conforme

Couche réseau : protocole ICMP

- Protocole ICMP (Internet Control Message Protocol)
  - Format du paquet ICMP
    - Type : indique le type de message de contrôle ICPM (echo request, destination unreachable, …)
    - Code : donne des informations complémentaires sur le message
      - 0 pour un paquet de type 3 signifie Network Unreachable (routeur ou lien en panne)
      - 1 pour un paquet de type 3 signifie Host Unreachable (machine absence du réseau ou hors-service)
    - Checksum : permet une détection d'erreur sur l'en-tête ICMP
    - Paramètres : contenu dépendant du type de message
      - Le type 3 n'utilise pas ce champ
      - Les types 0 et 8 l'utilisent pour stocker un identifiant et un numéro de séquence
    - Données : permet de vérifier la bonne réception et compréhension du message
      - Par défaut, recopie l'en-tête IP et les 64 premiers bits du datagramme déclencheur du message ICPM
      - Séquence quelconque pour les messages de type "Echo"

TYPE	MESSAGE TYPE	DESCRIPTION
3	DESTINATION UNREACHABLE	Le paquet ne peut pas être délivré
11	TIME EXCEEDED	Le champ TTL de l'en-tête IP est arrivé à 0
12	PARAMETER PROBLEM	Champ non valide dans l'en-tête IP
4	SOURCE QUENCH	Incite le récepteur du paquet à ralentir
5	REDIRECT	Demande à un routeur de rediriger le paquet
8	ECHO REQUEST	Demande à un hôte si il est présent et opérationnel
0	ECHO REPLY	L'hôte répond en renvoyant le même paquet
13	TIMESTAMP REQUESTED	Identique à ECHO REQUEST avec un horodatage
14	TIMESTAMP REPLY	Identique à ECHO REPLY avec un horodatage

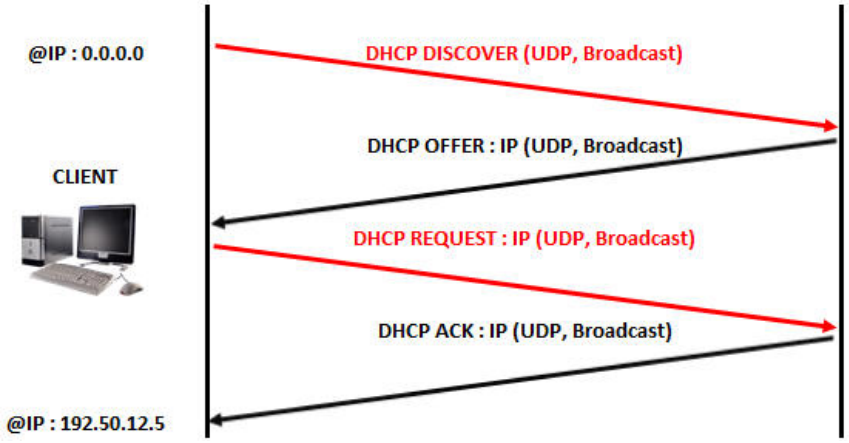


Couche réseau : protocole DHCP

- Protocole DHCP (Dynamic Host Configuration Protocol)
  - Protocole de configuration dynamique d'hôte
    - Permet d'allouer à la demande des adresses IP aux machines se connectant au réseau
  - Avantages
    - Gestion centralisée des adresses IP
    - Les machines clientes ne nécessitent pas de configuration IP manuelle
    - Le nombre de machines du réseau peut être supérieur au nombre d'adresses IP disponibles
  - Fonctionnement
    - Axé sur une base de données du serveur DHCP contenant
      - Une table d'adresses IP valides
      - Une table d'adresses IP réservées
      - Des paramètres de configuration valides pour tous les clients du réseau
        - Masques, adresses particulières, …
      - La durée des baux
        - Le bail défini la période de temps durant laquelle l'adresse IP attribuée peut être utilisée

Couche réseau : protocole DHCP

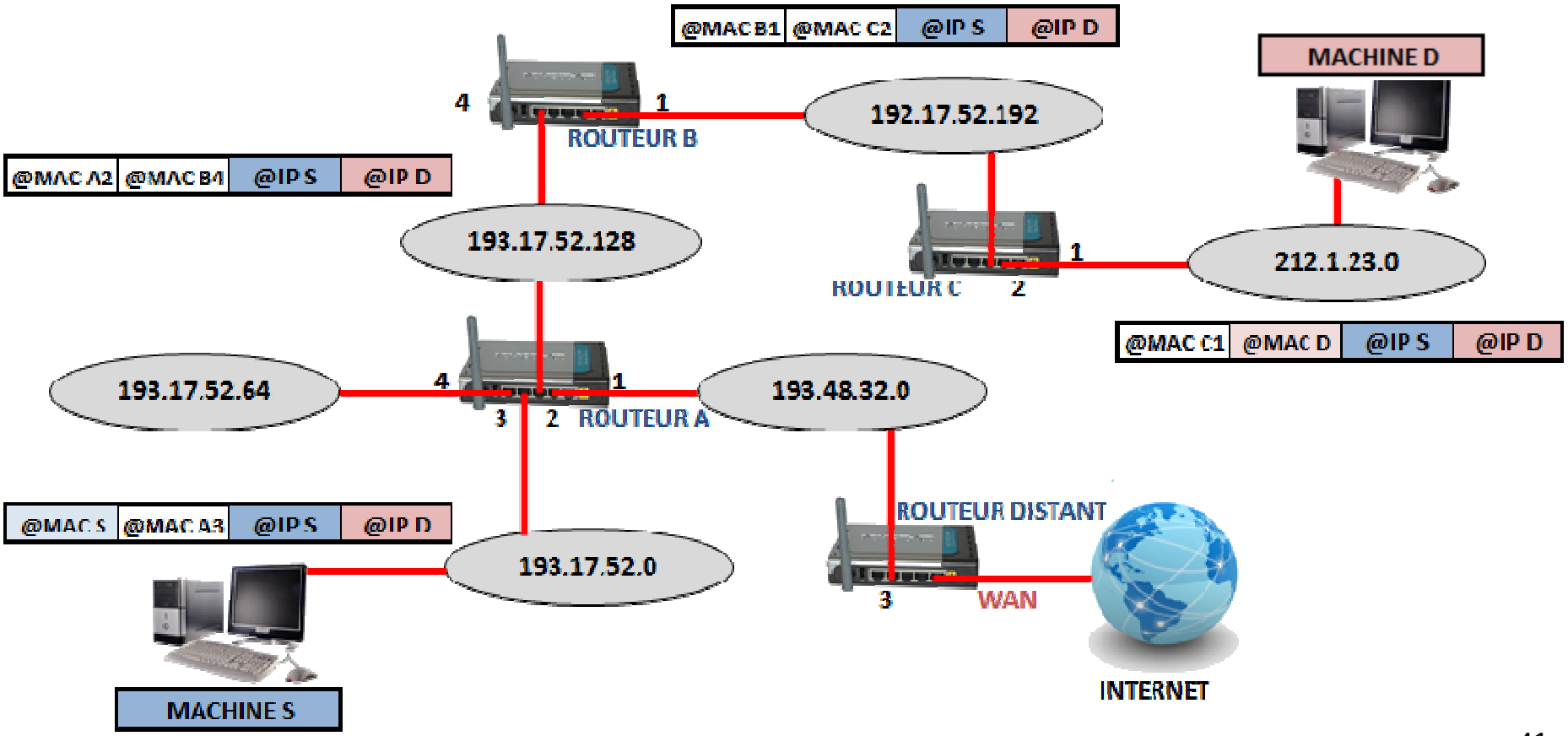
- Protocole DHCP (Dynamic Host Configuration Protocol)
  - Processus d'attribution dynamique d'une adresse IP
    - Découverte (Discover)
      - Le client envoie une trame de diffusion sur le réseau vers un serveur DHCP
      - L'adresse IP du client en attente d'attribution est l'adresse réservée 0.0.0.0
    - Offre (Offer)
      - Tous les serveurs DHCP disponibles répondent au client en lui faisant une offre
    - Demande (Request)
      - Le client répond à un serveur DHCP en lui précisant qu'il accepte l'offre proposée
    - Accusé de réception (ACK)
      - Le serveur DHCP confirme le bail avec sa durée et les options associées



ETAPE	DESCRIPTION
DHCP DISCOVER	Localiser les serveurs DHCP disponibles
DHCP OFFER	Réponse du serveur DHCP à un paquet DHCP DISCOVER contenant les premiers paramètres
DHCP REQUEST	Requêtes diverses du client (Exemple : demande de prolongation du bail)
DHCP ACK	Réponse du serveur DHCP contenant des paramètres et l'adresse IP du client
DHCP NAK	Réponse du serveur DHCP pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau
DHCP DECLINE	Le client annonce au serveur DHCP que l'adresse est déjà utilisée
DHCP RELEASE	Le client libère son adresse IP
DHCP INFORM	Le client demande des paramètres locaux

- Principe du routage IP
  - Définition du routage d'un paquet
    - Consiste à trouver le chemin vers le destinataire à partir de son adresse IP
  - Fonctionnement du routage d'un paquet
    - La machine émettrice (ou source) applique le masque de sous-réseau
      - Permet de déterminer si un routage est nécessaire ou pas
    - Notion de passerelle
      - Un paquet ne trouvant pas sa destination dans le réseau local est dirigé vers une passerelle (routeur)
        - Permet de le rapprocher de sa destination finale ou de l'acheminer vers sa destination finale
      - Chaque routeur possède une adresse par interface physique et logique (réseau) par réseau
    - Notion de passerelle par défaut
      - Chaque machine doit connaitre l'adresse d'un routeur par défaut
      - Permet au paquet d'une machine de sortir de son réseau d'appartenance pour atteindre un autre réseau
    - Notion de table de routage
      - Chaque routeur doit connaitre l'adresse du routeur suivant
      - Nécessité de gestion d'une table de routage de manière statique ou dynamique
        - Permet la détermination du chemin que va prendre le paquet

- Principe du routage IP
  - Portée des adresses logiques (réseaux) et physiques
    - Une adresse réseau ou logique (IP) a une portée de bout en bout
    - Une adresse physique (MAC) a une portée locale dans son réseau ou sous-réseau
      - La machine S connait l'adresse IP de la station D et l'adresse MAC de l'interface 3 du routeur A
        - Informations obtenues à l'aide du protocole ARP



- Principe du routage IP
  - Routage statique
    - Table de routage établie au départ
      - Des entrées peuvent être ajoutées manuellement avec la commande "route add"
    - Type de routage simple utilisable pour un petit réseau local avec une connexion externe
  - Routage dynamique
    - Table de routage mise à jour périodiquement à l'aide de protocoles spécifiques
      - Routing Information Protocol (RIP)
        - Utilise une technique de diffusion (broadcast) périodique et les transferts se font à l'aide de datagrammes UDP
        - Exemple : le routeur B indique au routeur A qu'il est directement connecté au réseau 192.17.52.192 et qu'il connait le réseau 212.1.23.0 via le routeur C
      - Exterior Gateway Protocol (EGP)
        - Limite la transmission de la table au routeur voisin (dialogue) et les transferts se font à l'aide de datagrammes IP
      - Open Shortest Path First (OSPF)
        - Basé sur le calcul d'un vecteur de distance permettant d'ouvrir le chemin le plus court en priorité
        - Utilisé pour les réseaux de grande taille
  - Algorithmes de routage
    - Algorithmes à vecteurs de distance (Vector-Distance)
      - Les informations échangées permettent à chaque routeur de retenir la plus courte distance (le plus petit nombre de sauts) pour atteindre une destination en utilisation l'équation de Bellman-Ford
    - Algorithmes à état de lien (Link-State)
      - Basés sur la transmission d'une carte complète des liens possibles entre les routeurs qui calculent chacun localement les meilleures routes pour une destination

- Principe du routage IP
  - Exemple :
    - La machine 193.17.52.13 envoie un paquet à 212.1.23.47 engendrant un routage en 4 étapes
      - La machine source utilise son masque et en déduit que la destination se trouve dans un autre réseau
        - La machine source adresse le paquet au routeur A qui est son routeur par défaut
      - Le routeur A reçoit le paquet, récupère l'adresse de destination et consulte sa table de routage
        - Le routeur A dirige en conséquence le paquet vers le routeur B
      - Le routeur B suit le même processus et transmet le paquet au routeur C
      - Le routeur C délivre le paquet à la destination, celle-ci se trouvant sur un réseau connecté au routeur

Table de routage du routeur A

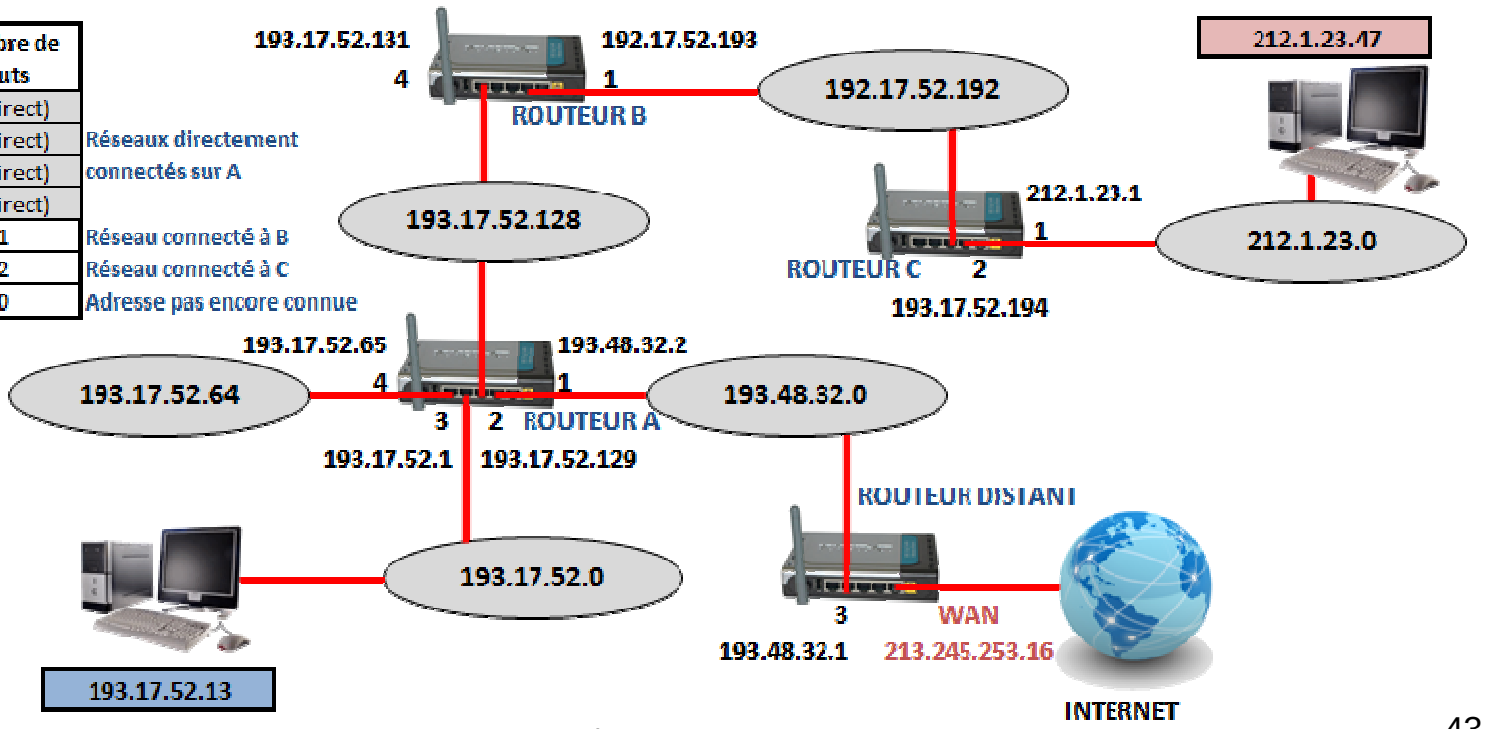
Adresse du réseau destination	Adresse du prochain routeur	Interface empruntée	Nombre de sauts
193.17.52.128	193.17.52.129	Ethernet 2	0 (direct)
193.48.32.0	193.48.32.2	Ethernet 1	0 (direct)
193.17.52.0	193.17.52.1	Ethernet 3	0 (direct)
193.17.52.64	193.17.52.65	Ethernet 4	0 (direct)
193.17.52.192	193.17.52.131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

Réseaux directement connectés sur A

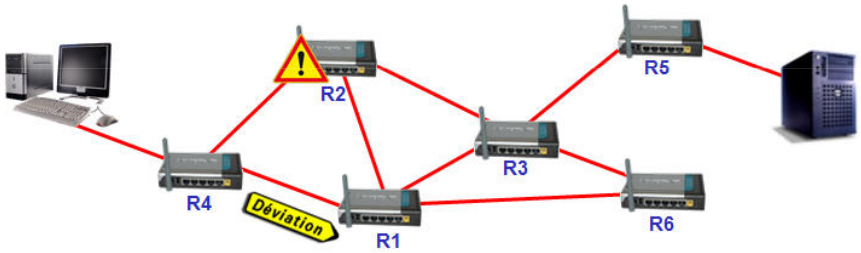
Réseau connecté à B

Réseau connecté à C

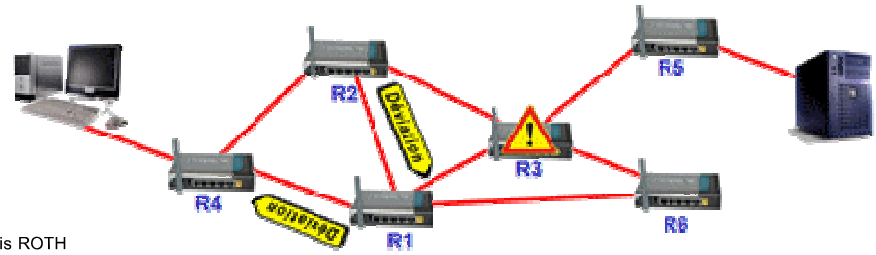
Adresse pas encore connue



- Principe du routage IP
  - Saturation d'un routeur
    - Dans un réseau maillé (Internet) plusieurs chemins sont possibles pour une même destination
      - Un paquet arrivant sur un routeur est mis en mémoire en attendant d'être routé
        - Si le débit entrant amène la saturation d'un routeur, le routeur en amont doit trouver un autre chemin pour les paquets
        - Le routeur ne peut pas retenir les paquets sortants au risque de bloquer tous les paquets en attente d'émission
      - Exemple avec la saturation de la file du routeur R2 obligeant le routeur R4 à trouver un autre chemin
        - Les paquets traverseront les routeurs R4, R1, R3 et R5 pour arriver à destination



    - La saturation de la file du routeur R3 entraine le re-routage des paquets et une situation critique
      - Le routeur R2 est informé via la protocole RIP par le routeur R3 qu'il ne peut plus lui adresser de paquets
        - Le routeur R2 va envoyer les paquets vers le routeur R1
      - Le routeur R1 également informé par le routeur R3, va envoyer les paquets vers le routeur R4
        - Les paquets vont tourner entre les routeurs R1, R2 et R4 sans jamais atteindre leur destination, encombrant le trafic
      - Le champ "durée de vie" (Time To Live) de l'en-tête IP est décrémenté à chaque traversée d'un routeur
        - Au passage à 0 du compteur Time To Live, le paquet est détruit par le routeur

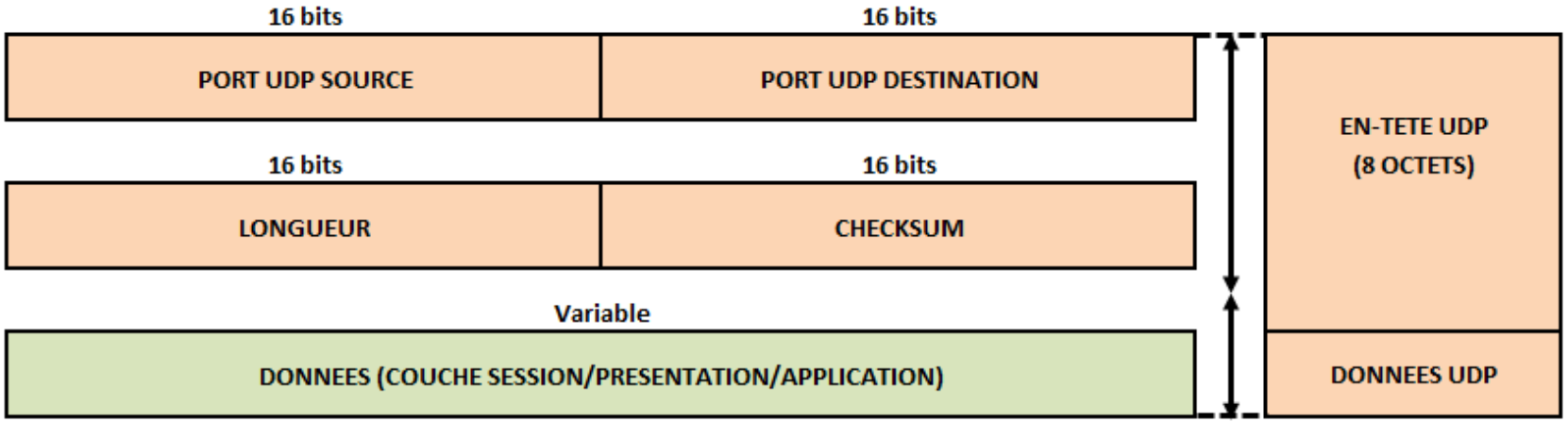


Couche transport : protocole UDP

- Protocole UDP (User Datagram Protocol)
  - Protocole de niveau transport
    - Identifié par la valeur 17 dans le champ "protocole" du paquet IP
    - Permet la transmission de données de manière très simple et rapide entre deux entités
      - Chaque entité est définie par une adresse IP et un numéro de port
    - Fonctionne sans négociation (contrairement au protocole TCP)
      - Pas de procédure de connexion préalable à l'envoi des données (Handshaking)
      - Aucune garantie de la bonne livraison des datagrammes à destination
      - Aucune garantie de leur ordre d'arrivée
      - Les datagrammes peuvent éventuellement être reçus en plusieurs exemplaires
    - Utilisation
      - Nécessité de transmettre des données très rapidement et où la perte d'une partie de ces données n'a pas grande importance
      - Nécessité de transmettre des petites quantités de données, là où la connexion TCP est inutilement gourmande en ressources
      - Exemples
        - Voix sur IP : perte d'un paquet tolérable dans la mesure où des mécanismes de substitution des données manquantes existent, mais la rapidité de transmission est primordiale pour la qualité d'écoute
        - Protocoles DNS, SNMP, TFTP, le streaming, les jeux en réseau, la commande traceroute, …

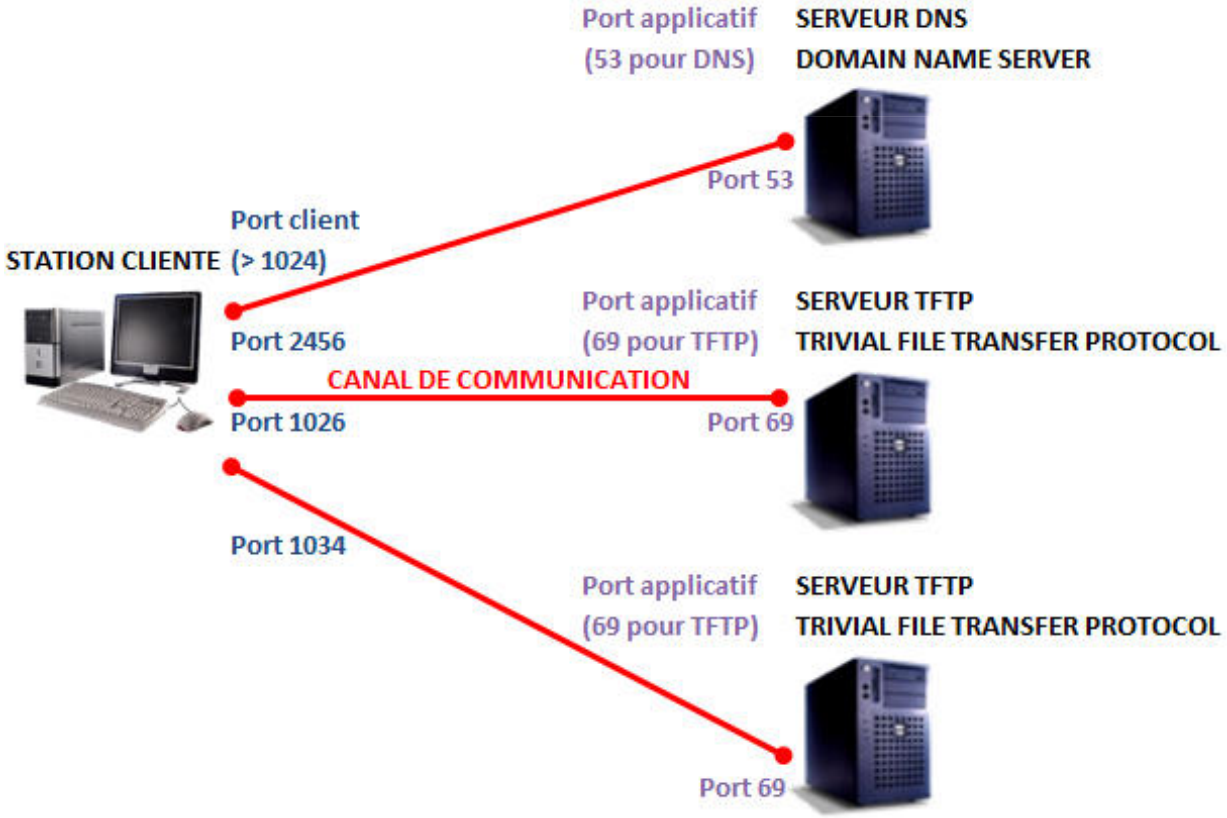
Couche transport : protocole UDP

- Format de message (ou datagramme) UDP
  - Port source : indique depuis quel port le paquet a été envoyé
  - Port destination : indique à quel port le paquet doit être envoyé
  - Longueur : indique la longueur totale du message (données et en-tête) en octets
  - Checksum : permet de s'assurer de l'intégrité du paquet reçu
    - Calculé sur l'ensemble de l'en-tête UDP et des données ainsi que sur une partie de l'en-tête IP
    - Une valeur à 0 indique que le contrôle d'intégrité n'est pas géré



Couche transport : protocole UDP

- Affectation des ports UDP
  - Ports source et destination
    - Identifient les applications s'exécutant sur les machines locales et distantes dans une communication de type client/serveur
      - Une application serveur "écoute" un port qui lui est propre
      - Une application cliente A désirant communiquer avec une application serveur B "parle" par le port B

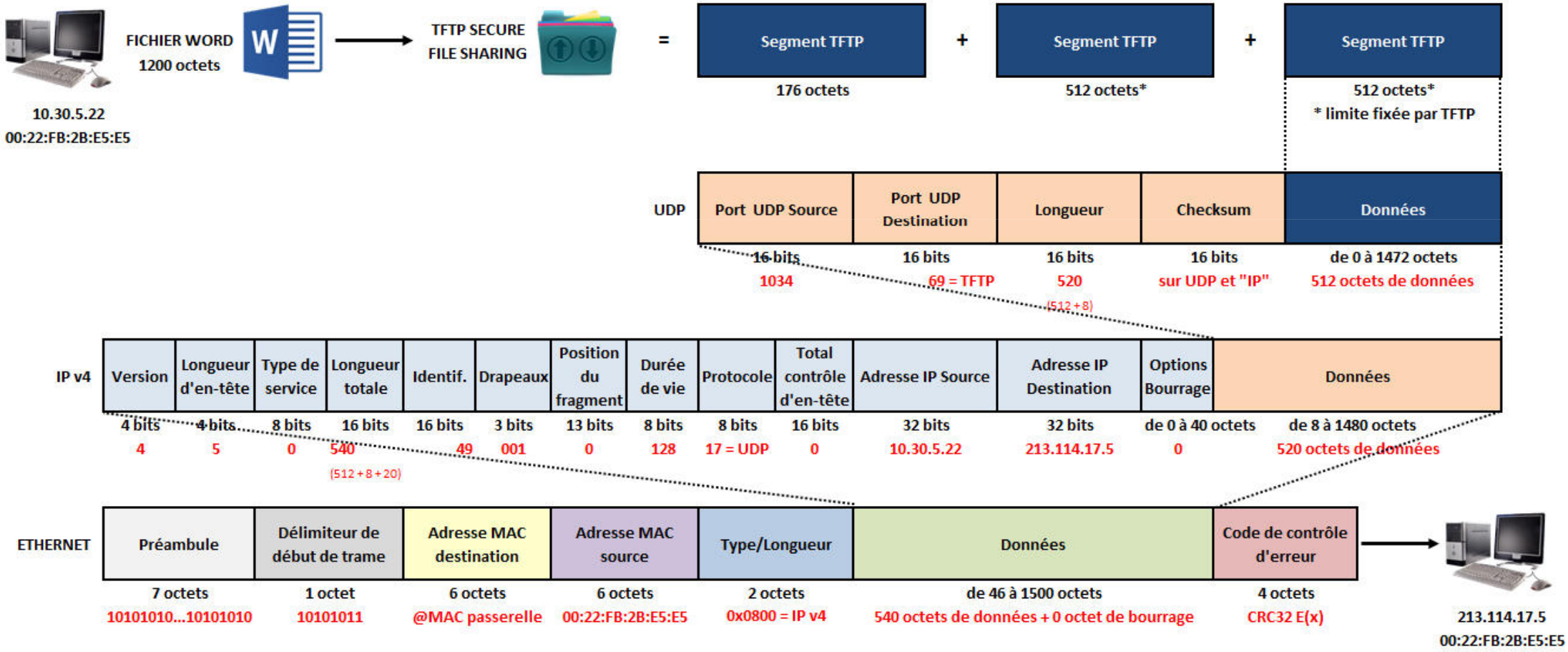


Numéro de port	Protocole (application)
20	FTP (File Transfer Protocol)
21	FTP (File Transfer Protocol avec contrôle)
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (Domain Name Server)
67	Serveur de protocole Bootp/DHCP
68	Client de protocole Bootp/DHCP
69	TFTP (Trivial File Transfer Protocol)
70	Gopher
80	HTTP (HyperText Transfer Protocol)
110	POP (Post Office Protocol)
119	NNTP (Network News Transfer Protocol)
123	NTP (Network Time Protocol)
161	SNMP (Simple Network Management Protocol)
162	SNMP TRAP
179	BGP (Border Gateway Protocol)

Les valeurs supérieures à 1024 correspondent à des ports clients et sont affectées à la demande par la machine qui effectue une connexion UDP

Couche transport : protocole UDP

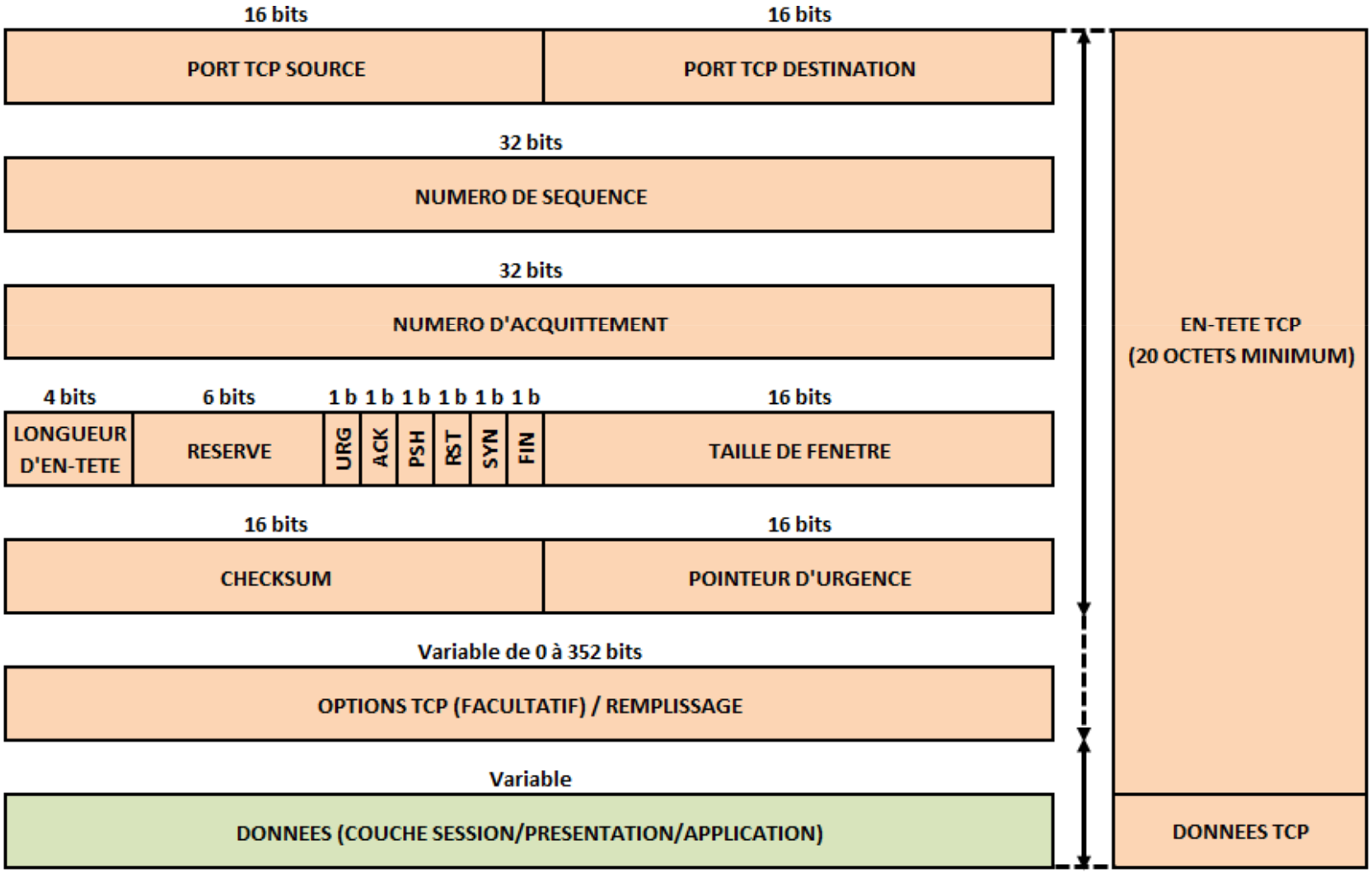
- Encapsulation UDP/IP sur Ethernet
  - Transfert d'un fichier Microsoft Word à l'aide de l'application TFTP Secure File Sharing



Couche transport : protocole TCP

- Protocole TCP (Transmission Control Protocol)
  - Protocole de niveau transport de bout en bout
    - Identifié par la valeur 6 dans le champ "protocole" du paquet IP
    - Permet la transmission de données de manière fiable en mode connecté
      - Etablissement et fermeture de la connexion virtuelle
      - Acquittement des paquets reçus et retransmission si absence d'acquittement (récupération sur erreur)
    - Le flux d'octets est découpé en segments dont la taille dépend de la MTU du réseau
      - Segmentation et réassemblage des données (S-PDU)
        - Les données sont segmentées et comptabilisées lors de l'encapsulation puis délivrées dans le même ordre
        - Réalisation d'un re-séquencement si la couche IP ne les délivre pas dans l'ordre
    - Multiplexage des données issues de plusieurs processus hôtes en un même segment
      - Les numéros de ports constituent le mécanisme d'adressage de la couche transport
        - Identification du processus de la couche application utilisé pour l'émission et celui utilisé pour la réception
    - Contrôle de flux avec fenêtrage
      - A l'initiation des échanges, la taille de fenêtre est réduite
        - Si aucune erreur ne survient, la taille de fenêtre augmente suivant une règle définie.
        - Si des erreurs surviennent, la taille de fenêtre diminue de façon à augmenter le nombre des contrôles
      - La combinaison des numéros de séquence et d'acquittement avec la fenêtre permet de contrôler la quantité de données à transmettre avant d'acquitter les données
    - Gestion des priorités des données et de la sécurité de la communication

- Format de segment TCP

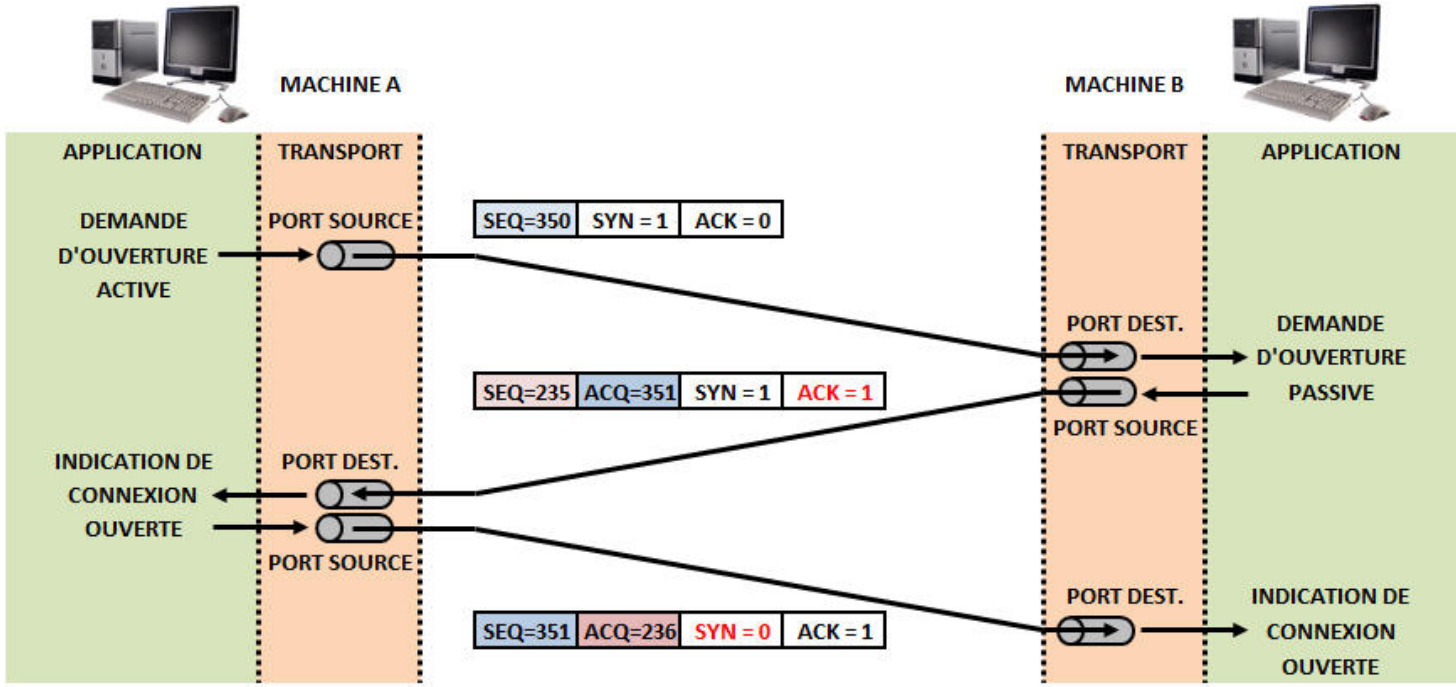


- Format de segment TCP
  - Descriptif des champs
    - Port Source / Port Destination : Identifient les applications de l'émetteur/récepteur
    - Numéro de séquence : numéro du premier octet transmis dans le segment
      - Permet de s'assurer que les données ont été reçues dans l'ordre dans lequel elles ont été envoyées
    - Numéro d'acquittement : numéro de séquence identifiant le prochain octet attendu par l'émetteur
      - Permet de s'assurer que les données ont été correctement reçues
    - Longueur d'en-tête : nombre de mots de 32 bits contenus dans l'en-tête TCP
    - Les bits de contrôle définissant la fonction des messages et la validité de certains champs :
      - URG = 1 indique que les données du segment sont urgentes et doivent être délivrées immédiatement
      - ACK = 1 indique que le numéro de séquence est valide et contient le prochain octet de données attendu
      - PSH = 1 indique une fin de message et que les données doivent être transmises à la couche supérieure
      - RST = 1 indique un arrêt ou un refus de connexion suite à la détection d'une erreur irrécupérable
      - SYN = 1 indique une demande de synchro de numéro de séquence : demande d'ouverture de connexion
      - FIN = 1 indique que l'émetteur n'a plus de données à transmettre : demande de fermeture de connexion
    - Taille de fenêtre : nombre d'octets de données à transmettre à partir de celui indiqué par le champ numéro d'acquittement
    - Checksum : correspond à une somme de contrôle de l'en-tête et des données
    - Priorité : indique le numéro de séquence de l'octet qui suit les données urgentes (si URG = 1)
    - Options : permet, par exemple, de définir la taille maximale d'un segment

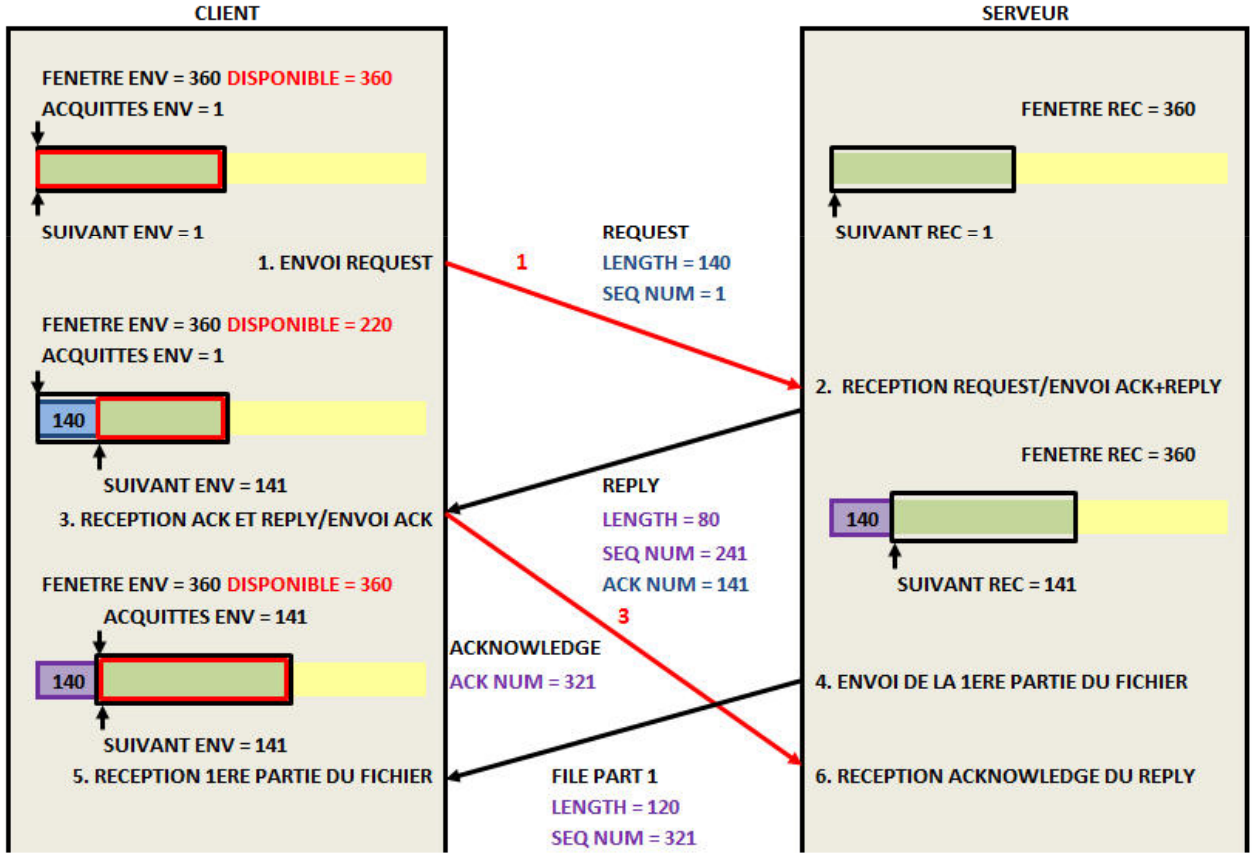
Couche transport : protocole TCP

- Principe de fonctionnement
  - Une session TCP fonctionne en 4 phases
    - Etablissement de la connexion
      - Poignée de main en trois temps (handshaking)
    - Transfert des données
    - Transmission des données à la couche supérieure
    - Fermeture de la connexion
      - Poignée de main en quatre temps (handshaking)

- Principe de fonctionnement
  - Ouverture d'une connexion TCP (poignée de main en 3 temps)
    - Demande d'ouverture de connexion transmise à la couche transport positionnant le bit SYN à 1
    - Un numéro de séquence initial à l'émission (Initial Send Sequence number) est délivré au moment de la demande par un compteur incrémenté toutes les 4 ms
      - Exemple d'ouverture de connexion TCP entre la machine A et la machine B avec ISS = 350 :
        - La machine A envoie son numéro de séquence (ISS), le bit SYN à 1 et le bit ACK à 0
        - La machine B répond avec son propre numéro de séquence, un acquittement à ISS+1 et les bits SYN et ACK à 1
        - La machine A confirme avec un numéro de séquence identique à l'acquittement de la machine B, un acquittement égal à la séquence de B+1, le bit SYN à 0 et le bit ACK à 1

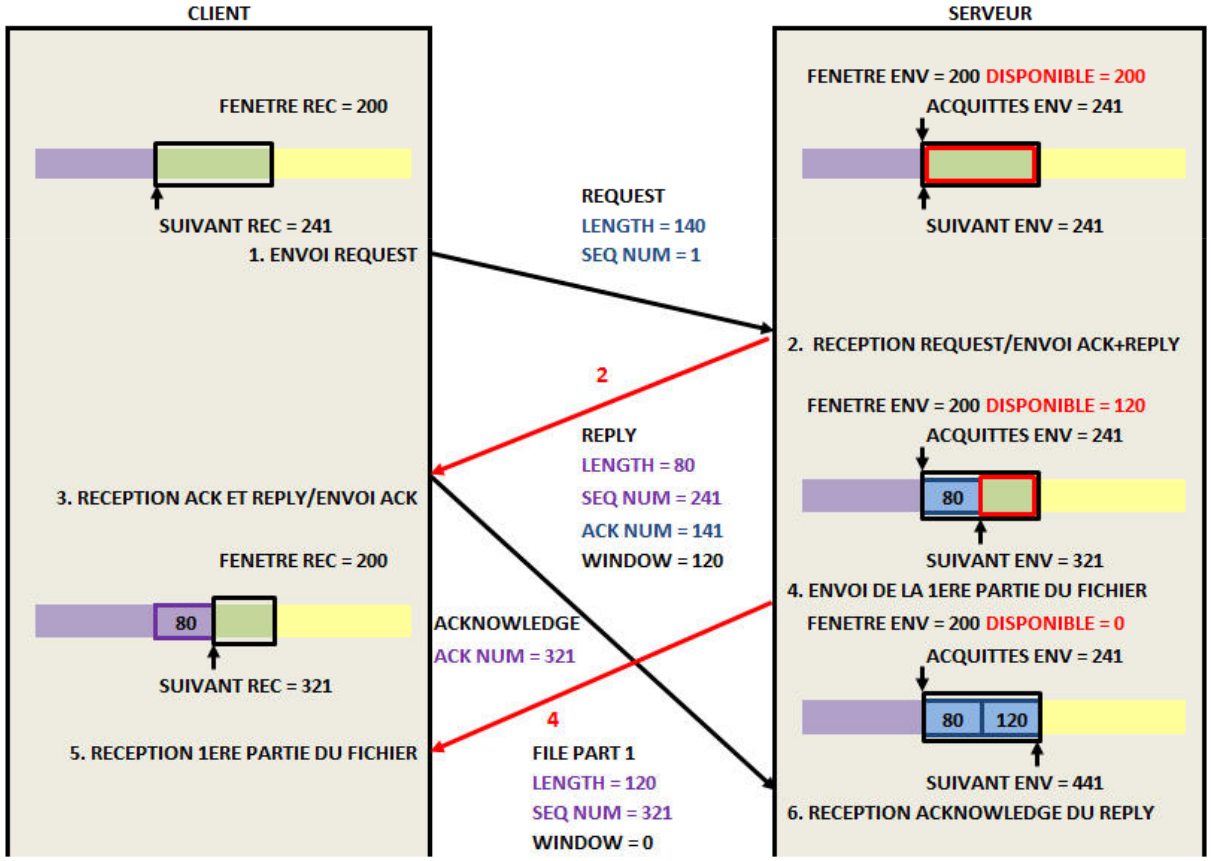


- Principe de fonctionnement
  - Transfert de données et fenêtre glissante TCP (sliding window)
    - Contrôle de flux réalisé dans les deux sens à l'aide des numéros d'acquittement (Ack Num)
      - Emetteur : Client / Récepteur : Serveur

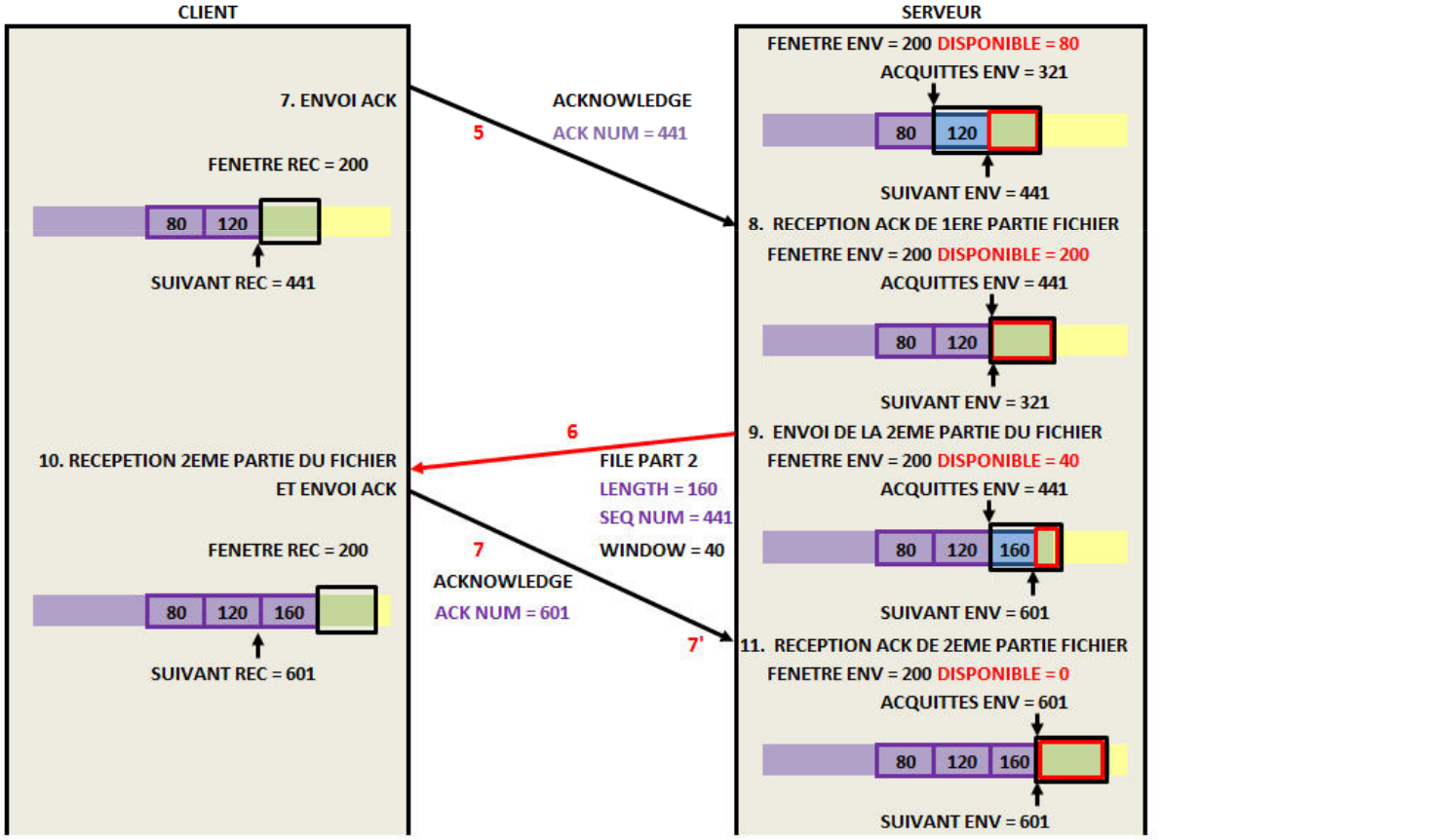


1. REQUETE DE 140 OCTETS ET FENETRE RESTANTE DE 220 OCTETS
3. ENVOI DE L'ACCUSE DE RECEPTION AVEC
ACK NUM CLIENT = LENGTH SERVER + SEQ NUM SERVER
ACK NUM CLIENT = 80 + 241 = 321

- Principe de fonctionnement
  - Transfert de données et fenêtre glissante TCP (sliding window)
    - Contrôle de flux réalisé dans les deux sens à l'aide des numéros d'acquittement (Ack Num)
      - Emetteur : Serveur / Récepteur : Client



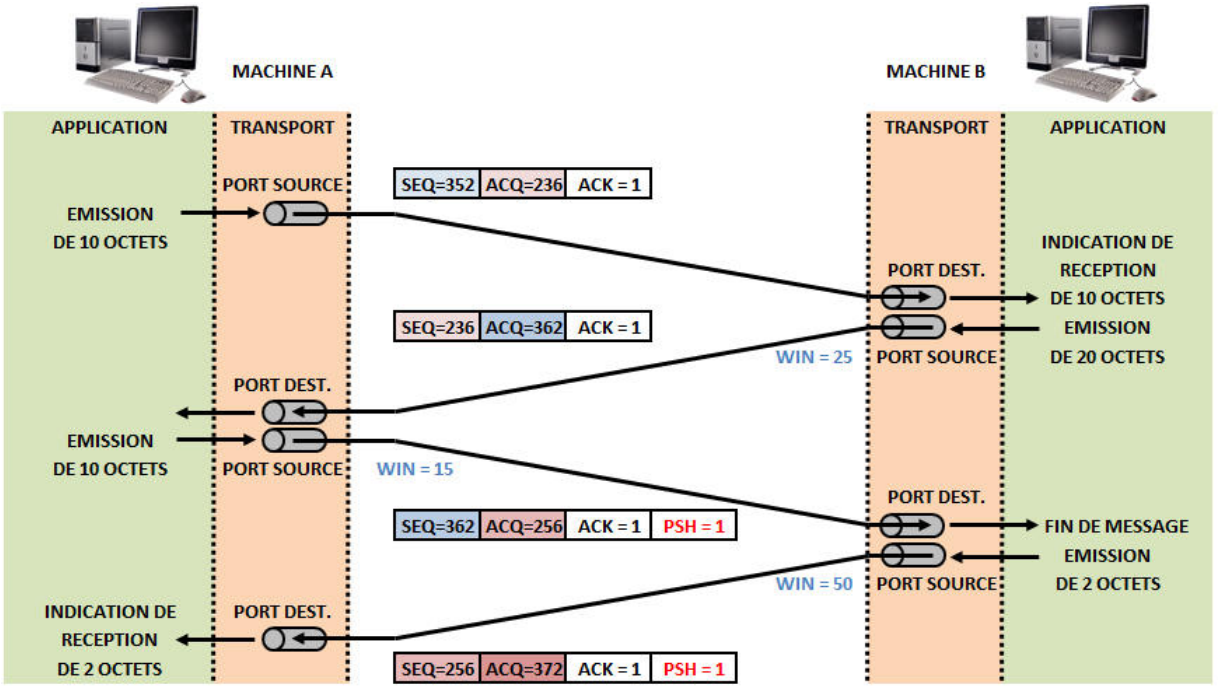
- Principe de fonctionnement
  - Transfert de données et fenêtre glissante TCP (sliding window)
    - Contrôle de flux réalisé dans les deux sens à l'aide des numéros d'acquittement (Ack Num)
      - Emetteur : Serveur / Récepteur : Client



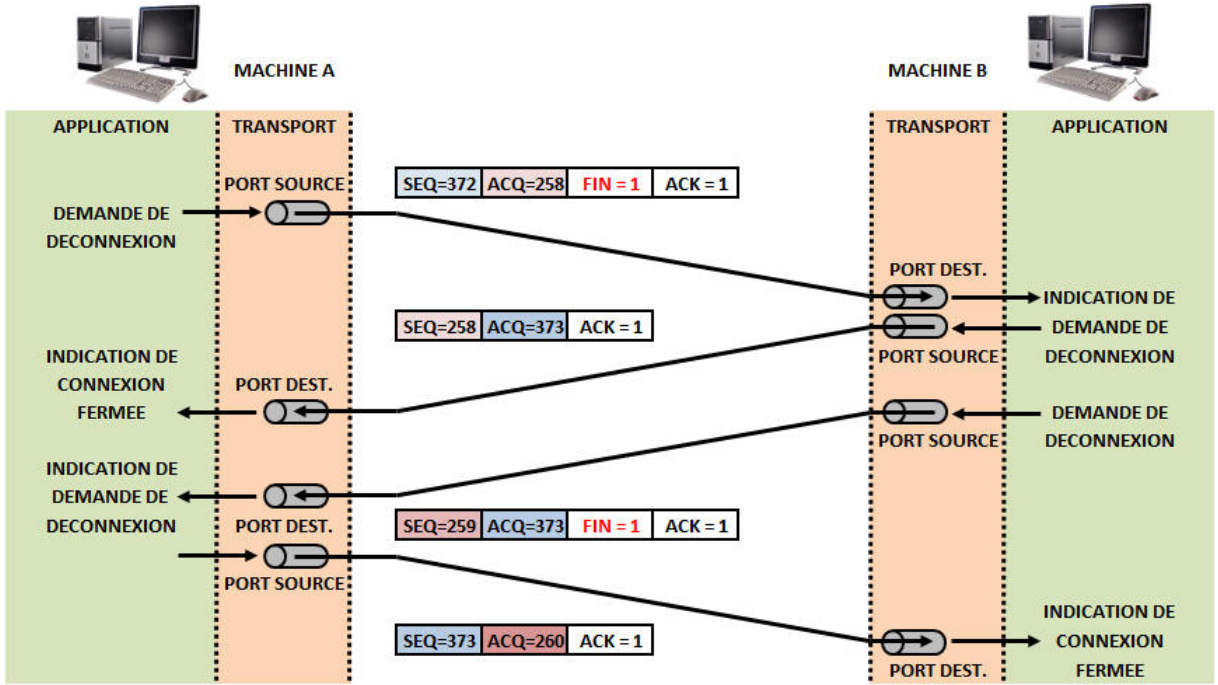
5. ACQUITTEMENT DU TRANSFERT DES 120 OCTETS AVEC
ACK NUM CLIENT = LENGTH CLIENT + SEQ NUM CLIENT = 141 + 1 = 141
7. ACQUITTEMENT DU TRANSFERT DES 160 OCTETS AVEC
ACK NUM CLIENT = LENGTH CLIENT + SEQ NUM CLIENT = 160 + 441 = 601

6. SUITE DU TRANSFERT SUR 160 OCTETS (SEQ NUM SERVER = ACK NUM CLIENT)
AVEC FENETRE RESTANTE DE 40 OCTETS
WINDOW = 200 - 160 = 40 OCTETS
7'. LA FENETRE REPASSE A 200 OCTETS

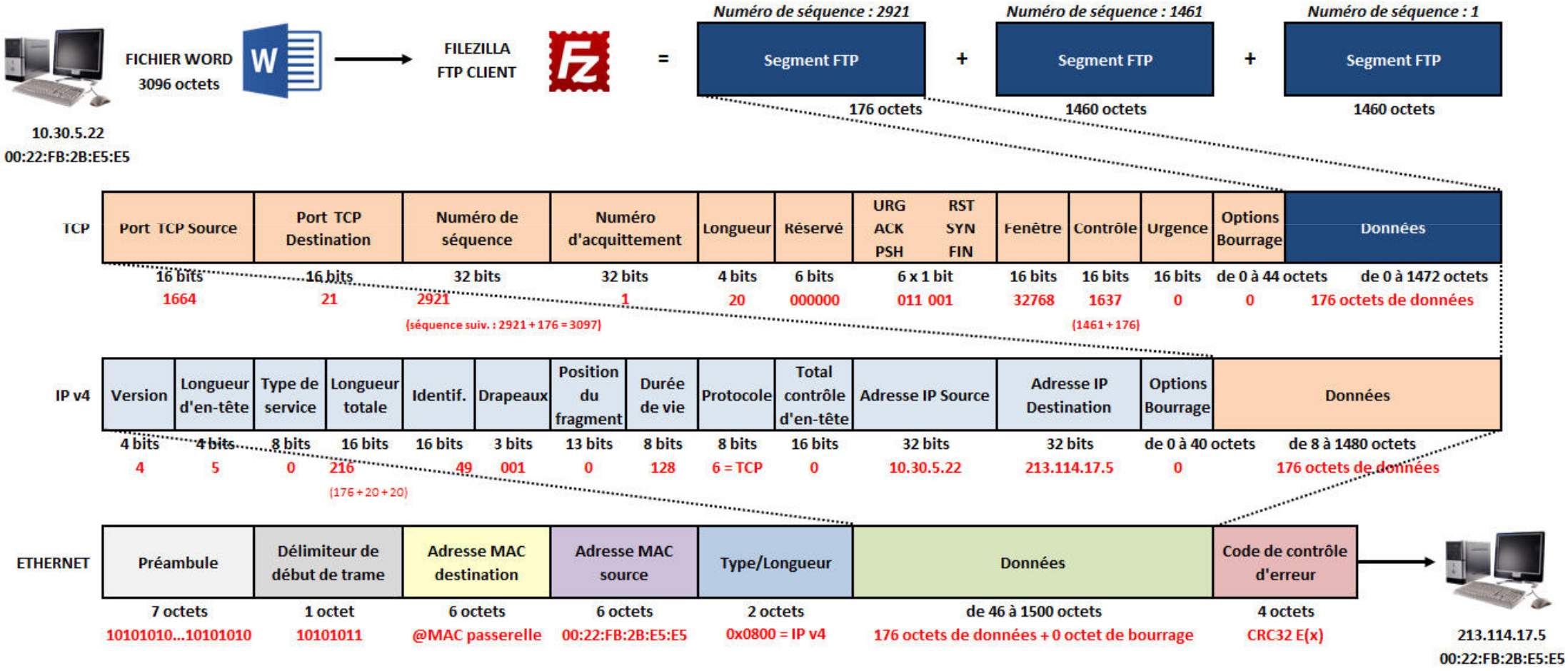
- Principe de fonctionnement
  - Transmission de données TCP à la couche supérieure
    - Opération réalisée lorsque le récepteur reçoit un en-tête TCP dont le bit PSH est positionné à 1
    - Caractéristiques de chaque paquet :
      - Pour numéro de séquence : le numéro d'acquittement du dernier paquet reçu
        - SEQ = numéro d'acquittement du paquet reçu
      - Pour numéro d'acquittement : le numéro de séquence du dernier paquet reçu incrémenté du nombre d'octets de données qu'il contenait
        - ACQ = numéro de séquence du paquet reçu + nombre d'octets reçus



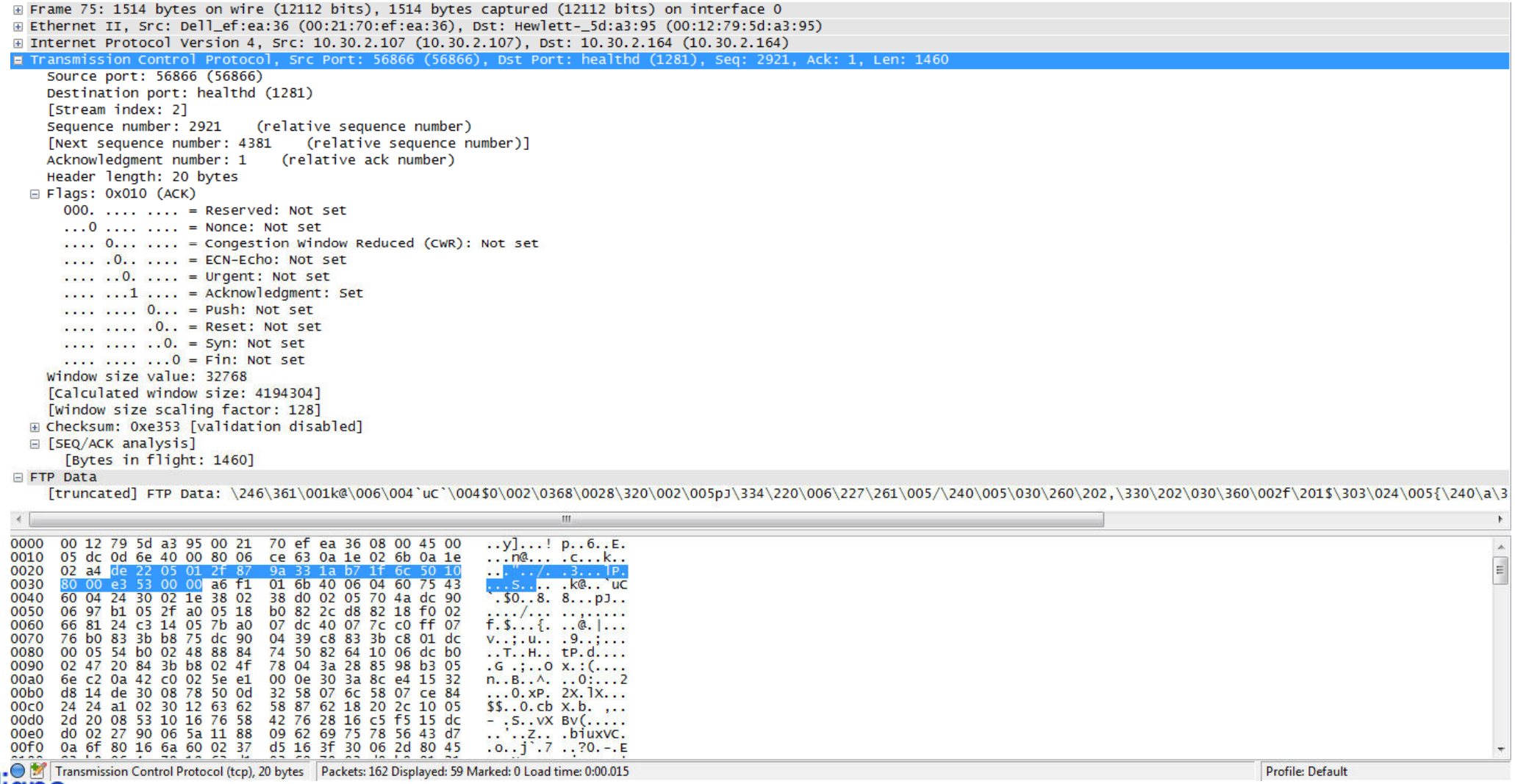
- Principe de fonctionnement
  - Fermeture d'une connexion TCP (poignée de main en 4 temps)
    - Opération réalisée lorsque le récepteur reçoit un en-tête TCP dont le bit FIN est positionné à 1
    - La demande est traitée dans les deux sens aux niveaux supérieurs avant acquittement
      - La machine A demande la déconnexion avec une séquence, un acquittement et les bits FIN et ACK à 1
      - La machine B répond avec une séquence égale à l'acquittement de A, un acquittement égal à la séquence de A+1 et le bit ACK à 1
      - La machine B demande à son tour la déconnexion avec le même acquittement et les bits FIN et ACK à 1
      - La machine A répond avec une séquence égale à l'acquittement de B, un acquittement égal à la séquence de B+1 et le bit ACK à 1



- Encapsulation TCP/IP sur Ethernet
  - Transfert d'un fichier Microsoft Word à l'aide de l'application Filezilla FTP Client



- Le protocole TCP (Transmission Control Protocol)
  - Exemple d'analyse



Planning

- *CM 1 : Généralités Réseaux*
- *CM 2 : Topologie et supports de transmission*
  - *TD 1 : Débit et technologie ADSL*
- *CM 3 : Codage des informations et contrôle d'intégrité*
  - *TD 2 : Codage des informations et contrôle d'intégrité CRC*
- *CM 4 : Modèle OSI / Ethernet*
- *CM 5 : Couches transport et réseau (TCP/IP)*
  - **TD 3 : Analyse de trames Ethernet / Adresse IP et masque de sous-réseaux**
  - TD 4 : Adressage IP / Routage IP
- CM 6 : Réseaux WLAN et sécurité
  - TD 5 : Réseaux Wifi et sécurité
- CM 7 : Réseaux et bus de terrain
  - TD 6 : Réseaux et bus de terrain
    - TP 1 : Technologie ADSL
    - TP 2 : Analyse de trames et Encapsulation Ethernet
    - TP 3 : Configuration d'un réseau IP / Routage IP / Wifi
    - TP 4 : Réseaux et bus de terrain
    - TP 5 : TP Test
- CM 8 : Contrôle de connaissances

- Exercice 1 (15 minutes) :
  - A l'aide du tableau ci-dessous, convertissez les adresses IP suivantes en binaire
    - 145.32.59.24
      - 10010001.00100000.00111011.00011000
    - 200.42.129.16
      - 11001000.00101010.10000001.00010011
    - 14.82.19.54
      - 00001110.01010010.00010011.000110110
  - A l'aide du tableau ci-dessous, convertissez les adresses IP suivantes en décimal et trouvez la classe associée à chaque adresse IP
    - 11001001. 11011110. 01000011. 01110101
      - Adresse IP : 201.222.67.117, Classe : 201 est compris entre 192 et 223, soit adresse de classe C
    - 01001010. 00011011. 10001111. 00010010
      - Adresse IP : 74.27.143.18, Classe : 74 est compris entre 1 et 126, soit adresse de classe A
    - 10000011. 00011101. 00101000. 00000111
      - Adresse IP : 131.29.40.7, Classe : 131 est compris entre 128 et 191, soit adresse de classe B

128	64	32	16	8	4	2	1

- Exercice 2 (15 minutes) :
  - Les adresses IP suivantes peuvent elles être assignées à des machines ? Précisez la classe, l'adresse de sous-réseau et l'adresse machine pour chaque adresse IP valide
    - 141.115.4.5/255.255.255.240
      - Adresse valide de classe B
      - Détermination de la partie réseau : ET LOGIQUE entre l'adresse en binaire et le masque en binaire
        - 10001101 ET 11111111 = 10001101
        - 01110011 ET 11111111 = 01110011
        - 00000100 ET 11111111 = 00000100
        - 00000101 ET 11110000 = 00000000
      - Adresse de sous-réseau : 141.115.4.0 et adresse machine : 5
    - 6.324.12.15/255.255.255.240
      - Adresse non valide (324 > 254)
    - 141.115.0.0/255.255.255.224
      - Adresse non valide (adresse de sous-réseau utilisée pour le routage ne pouvant être associée à une machine)
    - 192.25.36.117/255.255.255.224
      - Adresse valide de classe C
      - Détermination de la partie réseau : ET LOGIQUE entre l'adresse en binaire et le masque en binaire
        - 11000000 ET 11111111 = 11000000
        - 00011001 ET 11111111 = 00011001
        - 00100100 ET 11111111 = 00100100
        - 01110101 ET 11100000 = 01100000
      - Adresse de sous-réseau : 192.25.36.96 et adresse machine 117

- Exercice 3 (40 minutes) :
  - En considérant la trace suivante, obtenue par l'analyseur de protocoles WireShark installé sur la machine émettrice de la première trame Ethernet
    - Remarque : les trames (frames en anglais) sont données sans préambule, ni SFD, ni CRC

Frame Number : 1

```
0000 00 0a b7 a3 4a 00 00 01 02 6f 5e 9b 08 00 45 00
0010 00 28 00 00 40 00 40 01 82 ae 84 e3 3d 17 c2 c7
0020 49 0a 08 00 75 da 9c 7a 00 00 d4 45 a6 3a 62 2a
0030 09 00 ff ff ff ff 00 00 00 00 00 00
```

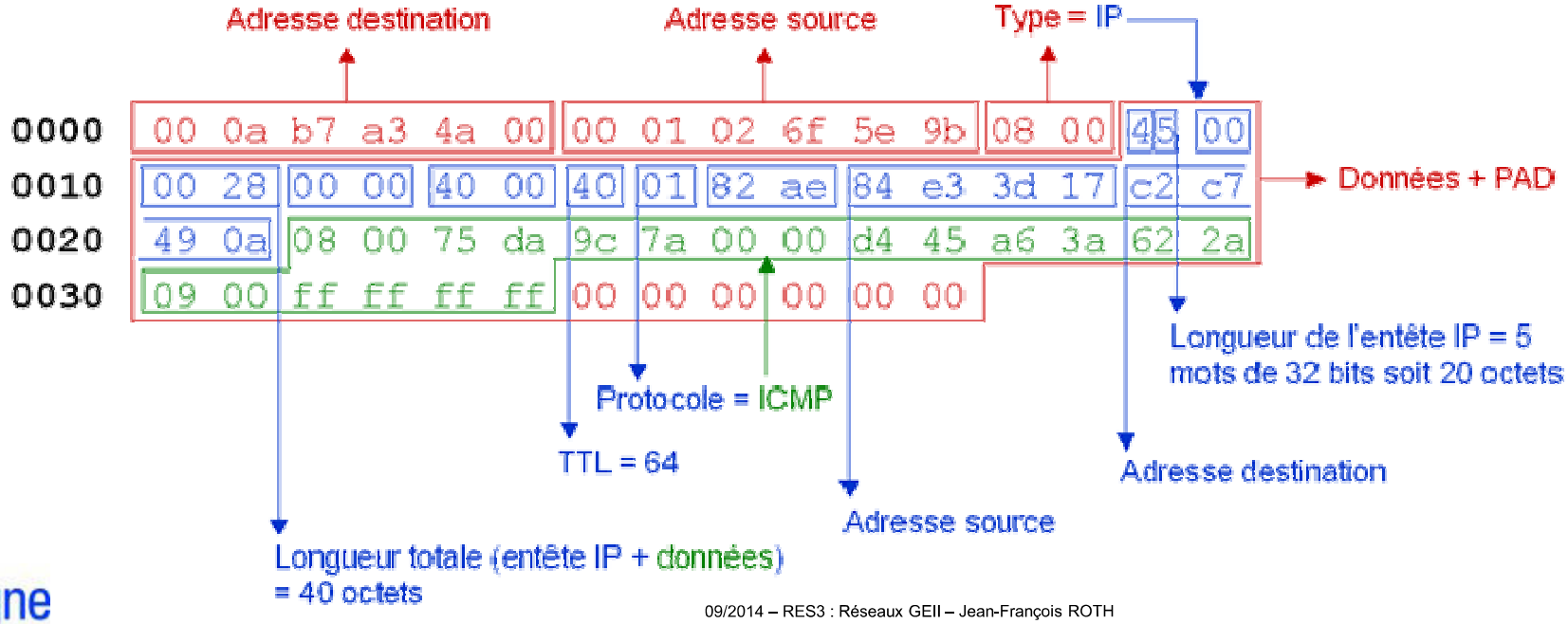
Frame Number : 2

```
0000 00 01 02 6f 5e 9b 00 0a b7 a3 4a 00 08 00 45 00
0010 00 28 d0 92 00 00 3a 01 5a db c2 c7 49 0a 84 e3
0020 3d 17 00 00 7d da 9c 7a 00 00 d4 45 a6 3a 62 2a
0030 09 00 ff ff ff ff 00 00 00 00 00 00
```

1. Quel est le protocole réseau utilisé pour réaliser l'échange de ces trames?
2. Quelle est l'adresse réseau de la machine ayant initié l'échange ? Quelle est sa classe d'adresse ?
3. Quelle est l'adresse physique de la machine ayant initié l'échange ?
4. Quelle est l'adresse réseau de la machine ayant répondu ? Quelle est sa classe d'adresse ?
5. Quelle est l'adresse physique de la machine ayant répondu ?
6. En supposant que la route de retour coïncide avec la route de l'aller, combien de routeurs séparent la machine source de la machine destination ?
7. Expliquez pourquoi dans les deux trames, la fin du paquet ne coïncide pas avec la fin de la trame ?
8. Quel genre de programme, d'application, ou de commande a pu générer cet échange sur le réseau ?

- Exercice 3 (40 minutes) :

1. Le protocole réseau est IP v4 car le champ type de la trame Ethernet est à 08 00
2. Adresse IP (réseau) de la machine ayant initiée l'échange : 84.e3.3d.17 = 132.227.61.23, classe B
3. Adresse MAC (physique) de la machine ayant initiée l'échange : 00:01:02:6f:5e:9b
4. Adresse IP (réseau) de la machine ayant répondu : c2.c7.49.0a = 194.199.73.10, classe C
5. Adresse MAC (physique) de la machine ayant répondu : 00:0a:b7:a3:4a:00
6. TTL de la trame 1 = 0x40 (64) ; TTL de la trame 2 = 0x3a (58), 64 – 58 = 6 routeurs
7. Dans les deux datagrammes IP, le champ Total Length vaut 0x28 (40), c'est-à-dire que les deux datagrammes ne représentent que 40 octets chacun. Or le champ données de la trame Ethernet doit contenir au moins 46 octets, il y a donc un bourrage « padding » de 6 octets (à 0x00) qui a été ajouté.
8. Le protocole encapsulé est ICMP (champ Protocol vaut 0x01) ; il s'agit vraisemblablement d'un message ICMP de demande d'écho, et un message ICMP de réponse d'écho, engendré par la commande ping



- Exercice 4 (20 minutes) :
  - Un administrateur réseau souhaite découper le réseau 195.84.90.0 en 8 sous-réseaux (remarque : sans respecter la RFC 950, recommandant de ne pas utiliser les sous-réseaux dont les bits sont tous à 0 ou tous à 1).
    - Quelle est la valeur du masque de sous-réseau, respectant la classe de sous-réseau par défaut ?
    - Pour chaque sous-réseau, indiquez l'adresse du sous-réseau et l'adresse de broadcast.
- Exercice 5 (20 minutes) :
  - Quelle(s) adresse(s) IP se trouvent sur le même sous-réseau que 130.12.127.231 si le masque de sous-réseau est 255.255.192.0 (remarque : sans respecter la RFC 950, recommandant de ne pas utiliser les sous-réseaux dont les bits sont tous à 0 ou tous à 1) en respectant la classe de sous-réseau par défaut) ?
    - 130.12.63.232
    - 130.22.130.1
    - 130.12.64.23
    - 130.12.167.127

- Exercice 4 (20 minutes) :

195.84.90.0 est une adresse réseau de classe C car 195 est compris entre 192 et 223

Les 3 premiers octets du masque du sous-réseau identifient le réseau (Network ID) d'une adresse de classe C
Le dernier octet permet de définir les numéros de sous-réseaux (Subnet ID) et les adresses machines (Host ID)

Pour obtenir 8 sous-réseaux il convient de définir un masque de sous-réseau sur 3 bits ($8 = 2^3$)
Le masque vaut 11111111 11111111 11111111 11100000_2 soit sous forme décimale pointée : 255.255.255.224

Le masque étant défini sur 3 bits, les différentes valeurs possibles du masque sur le dernier octet sont : 000, 001, 010, 011, 100, 101, 110, et 111 (en ne respectant pas les recommandations RFC 950, sinon il faudrait écarter les valeurs 000 et 111)

Faire varier les 3 premiers bits du dernier octet permet d'obtenir les 8 adresses de sous-réseaux
Au niveau du dernier octet, les 5 derniers bits à 0 désignent l'adresse de sous-réseau et les 5 derniers bits à 1 l'adresse de broadcast

Sous-réseau 1 :
0 0 0 0 0 0 0 0 = 0 soit 195.84.90.0
0 0 0 ..... hôtes du 1er sous-réseau
0 0 0 1 1 1 1 1= 31 soit 195.84.90.31

Sous-réseau 2 :
0 0 1 0 0 0 0 0 = 32 soit 195.84.90.32
0 0 1 ..... hôtes du 2e sous-réseau
0 0 1 1 1 1 1 1 = 63 soit 195.84.90.63

Sous-réseau 3 :
0 1 0 0 0 0 0 0 = 64 soit 195.84.90.64
0 1 0 ..... hôtes du 3e sous-réseau
0 1 0 1 1 1 1 1 = 95 soit 195.84.90.95

Sous-réseau 4 :
0 1 1 0 0 0 0 0 = 96 soit 195.84.90.96
0 1 1 ..... hôtes du 4e sous-réseau
0 1 1 1 1 1 1 1 = 127 soit 195.84.90.127

Sous-réseau 5 :
1 0 0 0 0 0 0 0 = 128 soit 195.84.90.128
1 0 0 ..... hôtes du 5e sous-réseau
1 0 0 1 1 1 1 1 = 159 soit 195.84.90.159

Sous-réseau 6 :
1 0 1 0 0 0 0 0 = 160 soit 195.84.90.160
1 0 1 ..... hôtes du 6e sous-réseau
1 0 1 1 1 1 1 1 = 191 soit 195.84.90.191

Sous-réseau 7 :
1 1 0 0 0 0 0 0 = 192 soit 195.84.90.192
1 1 0 ..... hôtes du 7e sous-réseau
1 1 0 1 1 1 1 1 = 223 soit 195.84.90.223

Sous-réseau 8 :
1 1 1 0 0 0 0 0 = 224 soit 195.84.90.224
1 1 1 ..... hôtes du 8e sous-réseau
1 1 1 1 1 1 1 1 = 255 soit 195.84.90.255

- Exercice 5 (20 minutes) :

L'adresse IP 130.12.127.231 est une adresse de classe B car 130 est compris entre 128 et 191.
Le 3ème octet est donc utilisé pour identifier les sous-réseaux car les deux premiers correspondent au 16 bits du champ NetID
Le masque 255.255.192.0 permet de définir 2^2 (192 = **11**00 0000) soit 4 sous-réseaux de 2^{14} – 2 hôtes chacun (11111111 11111111 11**000000 00000000**).

Recherche des adresses de sous-réseau et de broadcast :
Pour rappel 256 – valeur octet significatif = X et l'adresse réseau devra être un multiple de X, dans ce cas 256 – 192 = 64

sous-réseau 1 : 130.12.0.0	broadcast du sous-réseau 1 : 130.12.63.255
sous-réseau 2 : 130.12.64.0	broadcast du sous-réseau 2 : 130.12.127.255
sous-réseau 3 : 130.12.128.0	broadcast du sous-réseau 3 : 130.12.191.255
sous-réseau 4 : 130.12.192.0	broadcast du sous-réseau 4 : 130.12.255.255

130.12.127.231 appartient au sous-réseau 2 car son ET LOGIQUE avec le masque 255.255.192.0 donne 130.12.64.0
130.12.63.232 appartient au sous-réseau 1 car son ET LOGIQUE avec le masque 255.255.192.0 donne 130.12.0.0
130.22.130.1 appartient à un autre réseau car son ET LOGIQUE avec le masque 255.255.192.0 donne 130.22.128.0
130.12.64.23 appartient au sous-réseau 2 car son ET LOGIQUE avec le masque 255.255.192.0 donne 130.12.64.0
130.12.167.127 appartient au sous-réseau 3 car son ET LOGIQUE avec le masque 255.255.192.0 donne 130.12.128.0

Planning

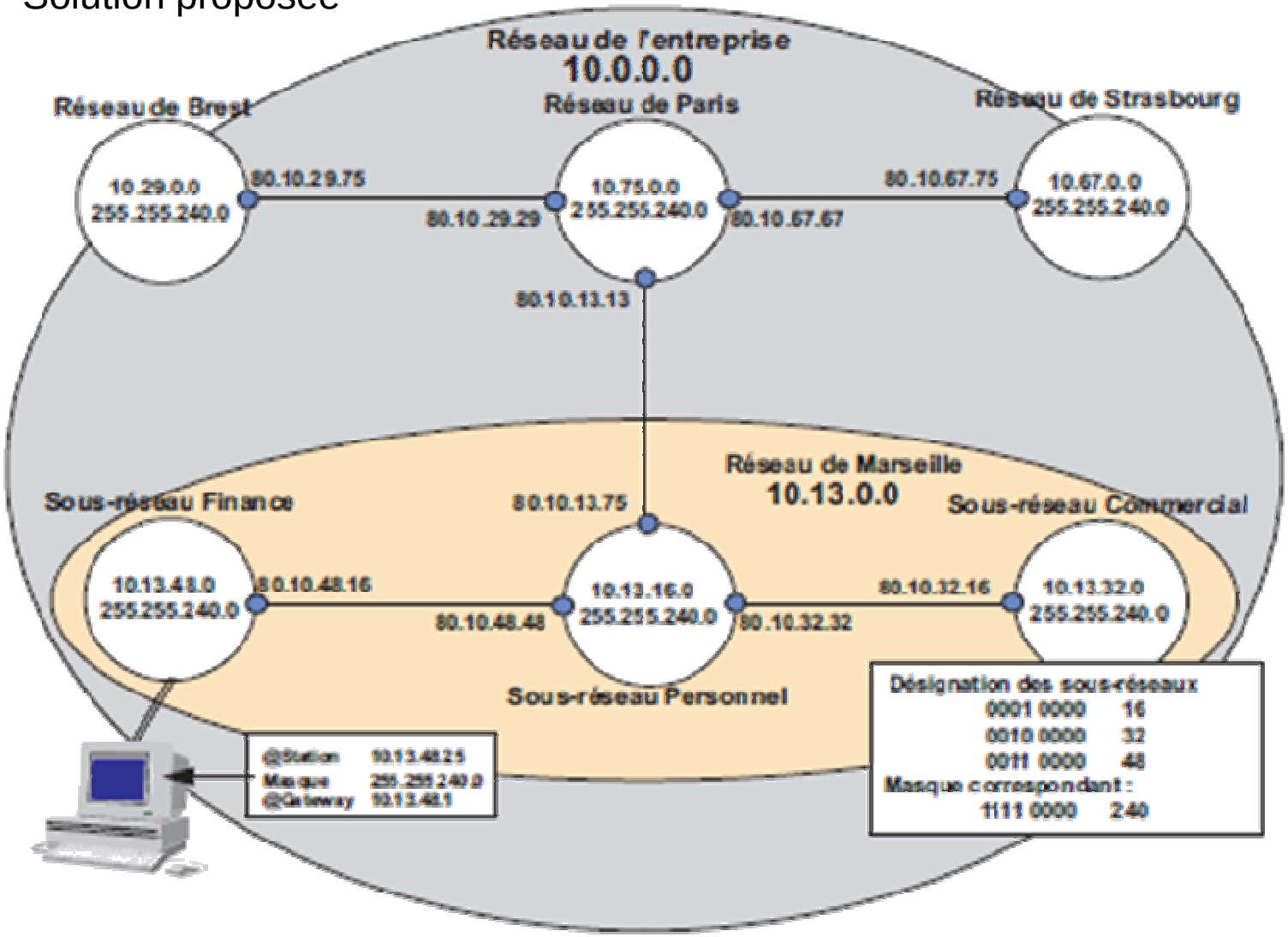
- *CM 1 : Généralités Réseaux*
- *CM 2 : Topologie et supports de transmission*
  - *TD 1 : Débit et technologie ADSL*
- *CM 3 : Codage des informations et contrôle d'intégrité*
  - *TD 2 : Codage des informations et contrôle d'intégrité CRC*
- *CM 4 : Modèle OSI / Ethernet*
- *CM 5 : Couches transport et réseau (TCP/IP)*
  - *TD 3 : Analyse de trames Ethernet / Adresse IP et masque de sous-réseaux*
  - **TD 4 : Adressage IP / Routage IP**
- CM 6 : Réseaux WLAN et sécurité
  - TD 5 : Réseaux Wifi et sécurité
- CM 7 : Réseaux et bus de terrain
  - TD 6 : Réseaux et bus de terrain
    - TP 1 : Technologie ADSL
    - TP 2 : Analyse de trames et Encapsulation Ethernet
    - TP 3 : Configuration d'un réseau IP / Routage IP / Wifi
    - TP 4 : Réseaux et bus de terrain
    - TP 5 : TP Test
- CM 8 : Contrôle de connaissances

- Exercice 1 (15 minutes) :
  - Dans le cas d'une adresse IP de classe B
    - Quel est le nombre de bits utilisés par défaut pour identifier la partie réseau ?
      - Masque par défaut d'une adresse de classe B : 255.255.0.0 = 11111111.11111111.00000000.00000000
      - Nombre de bits consécutifs à 1 : 16 bits
  - Supposez qu'au lieu d'utiliser ce nombre de bits par défaut pour la partie réseau d'une adresse IP de classe B on souhaite en utiliser 22
    - Combien de sous-réseaux est-il possible de définir dans ce cas en respectant la RFC 950 ?
      - Partie réseau = 22 au lieu de 16, soit 22 – 16 = 6 bits sont utilisés pour la partie sous-réseau
      - Nombre de sous-réseaux disponibles = 2^6-2 = 62
        - Par convention 000000 et 111111 sont réservés en respectant la RFC 950
    - Quel est le masque de sous-réseaux correspondant à ce besoin ?
      - Partie réseau + partie sous-réseau = 22 bits
      - Le masque de sous-réseau contient 22 bits à 1 et le reste (10 bits) à 0
      - 11111111.11111111.11111100.00000000 = 255.255.252.0

- Exercice 2 (45 minutes) :
  - Votre entreprise comporte 4 établissements (Paris, Strasbourg, Brest et Marseille) reliés en étoile par des liaisons louées (LL)
  - Compte tenu des informations ci-dessous, établissez le plan d'adressage de votre entreprise :
    - Les liaisons seront adressées en point à point (liaison directe entre deux équipements)
    - Chaque établissement devra pouvoir distinguer 10 sous-réseaux
    - Chaque sous-réseau devra pouvoir comprendre plus de 500 machines mais moins de 1 000.
    - L'établissement devra pouvoir être distingué simplement
    - N'ayant aucun besoin de connexion vers l'extérieur (adresse publique), l'entreprise utilisera des adresses privées de classe A

- Exercice 2 (45 minutes) :
  - Solution proposée
    - Adressage du réseau
      - L'adresse privée 10.0.0.0 est une adresse de classe A
      - Elle comporte un octet d'identification du réseau (Network ID) et 3 octets pour numéroter les sous-réseaux (Subnet ID) et stations (Host ID)
    - Possibilité de distinguer les sites et 10 sous-réseaux dans chaque site
      - Une solution simple consiste à réserver le second octet à l'identification des établissements en adoptant , par exemple, le numéro du département.
    - Numérotation des sous-réseaux
      - Utilisation du 3ème octet
      - Le premier multiple de 2 supérieur au nombre de sous-réseaux (10) est 16 (2^4)
        - Dans ces conditions, l'adresse réseau est 10.0.0.0
        - Le masque de sous-réseau est 11111111 11111111 11110000 00000000 soit 255.255.240.0
    - Adressage des liaisons
      - Deux techniques peuvent être utilisées pour adresser les liaisons :
        - Soit considérer chaque liaison louée comme un réseau (adressage point à point)
        - Soit considérer l'ensemble des liaisons louées du réseau comme appartenant au même réseau.
      - La première technique, plus simple, sera utilisée
      - L'adressage des liaisons louées peut être quelconque
        - Ces adresses ne sont utilisées que par les routeurs pour choisir le port de sortie et ne sont jamais vues de l'extérieur
      - Identification des liaisons par une numérotation significative de classe A :
        - Le premier octet indique le réseau de la liaison louée (exemple 80)
        - Le second qu'il s'agit du réseau 10
        - Les troisième et quatrième octets identifient les extrémités

- Exercice 2 (45 minutes) :
  - Solution proposée



- Exercice 3 (45 minutes) :
  - Réalisez le schéma du réseau à partir des tables de routage suivantes

ROUTEUR R1

RESEAU	MASQUE	PASSERELLE	INTERFACE
172.168.16.0	255.255.255.0		172.168.16.3
172.168.17.0	255.255.255.0		172.168.17.50

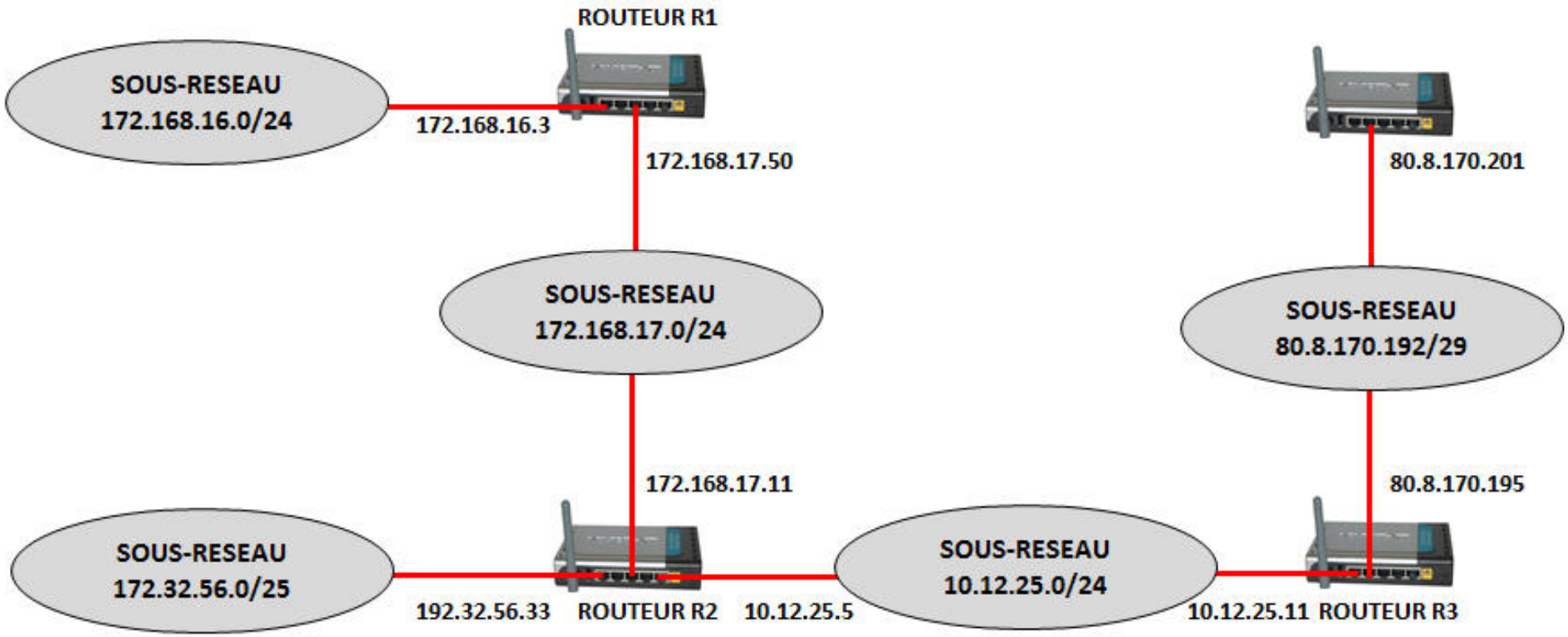
ROUTEUR R2

RESEAU	MASQUE	PASSERELLE	INTERFACE
172.168.0.0	255.255.0.0		172.168.17.11
10.12.25.0	255.255.255.0		10.12.25.5
195.32.56.0	255.255.255.128		195.32.56.33
172.168.16.0	255.255.255.0	172.168.17.50	172.168.17.11
0.0.0.0	0.0.0.0	10.12.25.11	10.12.25.5

ROUTEUR R3

RESEAU	MASQUE	PASSERELLE	INTERFACE
10.12.25.0	255.255.0.0		10.12.25.11
80.8.170.192	255.255.255.248		80.8.170.195
195.32.56.0	255.255.255.128	10.12.25.5	10.12.25.11
172.168.0.0	255.255.0.0	10.12.25.5	10.12.25.11
0.0.0.0	0.0.0.0	80.8.170.201	80.8.170.195

- Exercice 3 (45 minutes) :
  - Réalisez le schéma du réseau à partir des tables de routage suivantes



- Exercice 3 (45 minutes) :
  - Les questions suivantes s'enchainent et les erreurs de configuration sont rectifiées au fur et à mesure.
    - 1. Depuis le poste 172.168.16.21, la commande ping 172.168.16.22 génère la réponse correcte suivante :
      - 64 bytes from 172.168.16.22: icmp_seq=2 ttl=239 time=139 ms
    - Depuis le poste 172.168.16.21, la commande ping 172.168.17.12 génère la réponse :
      - connect: Network is unreachable
    - Pour quelle raison ? Que faire pour résoudre le problème ?
    - 2. Depuis le poste 172.168.17.12, la commande ping 216.239.59.9 n'obtient pas de réponse.
    - Pour quelle raison ? Que faire pour résoudre le problème ?
    - 3. Depuis le poste 172.168.16.22, la commande ping 80.8.170.195 n'obtient pas de réponse
    - Depuis le poste 172.168.16.22, la commande ping 10.12.25.11 n'obtient pas de réponse
    - Depuis le poste 172.168.16.22, la commande ping 195.32.56.33 n'obtient pas de réponse
    - Pour quelle raison ? Que faire pour résoudre le problème ?
    - 4. Depuis 10.12.25.89, la commande ping 172.168.17.12 renvoie une réponse correcte
    - Depuis 172.168.17.12, la commande ping 172.168.16.22 renvoie une réponse correcte
    - Par contre depuis 172.168.16.22 : ping 10.12.25.89 n'obtient pas de réponse.
    - Pour quelle raison ? Que faire pour résoudre le problème ?

- Exercice 3 (45 minutes) :
  - Réponses
    - 1. Le poste 172.168.16.21 peut communiquer avec son propre réseau mais pas avec un autre réseau IP. La réponse au PING indique que le paquet n'a pas pu être routé
      - Solution : configurer une passerelle sur le poste 172.168.16.22
    - 2. L'adresse de la passerelle par défaut du routeur R3 80.8.170.201 n'est pas joignable puisqu'elle ne se trouve pas dans le réseau 80.8.170.192/29
      - Solution : revoir l'adressage de cette passerelle en choisissant une adresse se trouvant dans le réseau
    - 3. Les trames n'étant pas à destination du sous-réseau sont redirigées vers le routeur R1. Celui-ci n'ayant aucun règle de routage appropriée, les paquets sont détruit une fois le TTL à 0
      - Solution : configurer les trois routes dans R1 pour atteindre les sous-réseaux recherchés

RESEAU	MASQUE	PASSERELLE	INTERFACE
80.8.170.192	255.255.255.248	172.168.17.11	172.168.17.50
10.12.25.0	255.255.255.0	172.168.17.11	172.168.17.50
195.32.56.0	255.255.255.128	172.168.17.11	172.168.17.50

      - Solution alternative : définir une route par défaut envoyant les routes non gérées vers la même passerelle
        - Cette règle est toujours interprétée en dernier, quelle que soit sa position dans la table de routage

RESEAU	MASQUE	PASSERELLE	INTERFACE
0.0.0.0	0.0.0.0	172.168.17.11	172.168.17.50

      - Dans les deux solutions, le routeur R2 reçoit les trames et sait comment les traiter

- Exercice 3 (45 minutes) :
  - Réponses
    - 4. La connectivité physique et les éléments d'interconnexions ne sont pas en cause, les postes ont des passerelles par défaut correctes car les deux premiers ping qui sont passés
      - Un ping est composé d'une trame aller (Request) et d'une trame retour (Reply) et fonctionne si la trame Reply arrive à l'expéditeur de la trame Request.
        - Trame Request de 172.168.16.22 envoyée vers 10.12.25.89 (passerelle configurée sur poste)
        - L'adresse n'appartenant pas au sous-réseau, la trame est envoyée vers 172.168.16.3 (R1)
        - Traversée de R1 (règle n°3): de 172.168.17.50 (R1) vers 172.168.17.11 (R2)
        - Traversée de R2 (règle n°2): de 10.12.25.5 (R2) vers 10.12.25.89
        - Conclusion : La trame request atteint son but sans problème
        - Trame Reply de 10.12.25.89 vers 172.168.16.22 (passerelle configurée sur poste)
        - L'adresse n'appartenant pas au sous-réseau, la trame est envoyée vers 10.12.25.5 (R2)
        - Traversée de R2 (règle n°1 : voir masque utilisé) : de 172.168.17.11 vers "????"
        - Le destinataire n'est pas dans le réseau, le routeur ne sait pas quoi faire du paquet, le TTL diminue et le paquet est détruit
        - Conclusion : La trame Reply n'atteint pas R1, et donc pas son destinataire, le ping échoue
      - Solution : Rectification de la première règle du routeur R2, qui devient la 4ème règle de la table :

ROUTEUR R2

RESEAU	MASQUE	PASSERELLE	INTERFACE
~~172.168.0.0~~	~~255.255.0.0~~		~~172.168.17.11~~
10.12.25.0	255.255.255.0		10.12.25.5
195.32.56.0	255.255.255.128		195.32.56.33
172.168.16.0	255.255.255.0	172.168.17.50	172.168.17.11
172.168.17.0	255.255.255.0		172.168.17.11
0.0.0.0	0.0.0.0	10.12.25.11	10.12.25.5

Planning

- *CM 1 : Généralités Réseaux*
- *CM 2 : Topologie et supports de transmission*
  - *TD 1 : Débit et technologie ADSL*
- *CM 3 : Codage des informations et contrôle d'intégrité*
  - *TD 2 : Codage des informations et contrôle d'intégrité CRC*
- *CM 4 : Modèle OSI / Ethernet*
- *CM 5 : Couches transport et réseau (TCP/IP)*
  - *TD 3 : Analyse de trames Ethernet / Adresse IP et masque de sous-réseaux*
  - *TD 4 : Adressage IP / Routage IP*
- CM 6 : Réseaux WLAN et sécurité
  - TD 5 : Réseaux Wifi et sécurité
- CM 7 : Réseaux et bus de terrain
  - TD 6 : Réseaux et bus de terrain
    - TP 1 : Technologie ADSL
    - TP 2 : Analyse de trames et Encapsulation Ethernet
    - TP 3 : Configuration d'un réseau IP / Routage IP / Wifi
    - TP 4 : Réseaux et bus de terrain
    - TP 5 : TP Test
- CM 8 : Contrôle de connaissances