Épisode 7

FIPA24 - Année scolaire 22/23

Pascal Cotret, ENSTA Bretagne

29 septembre 2022

Objectifs du cours

- Interconnecter des réseaux locaux et des réseaux étendus, pour former Internet ;
- Affecter des adresses aux machines pour les identifier à l'échelle d'Internet ;
- Acheminer de l'information entre plusieurs réseaux.
- Établir un flux d'information continu d'une machine vers une autre ;

Objectifs du cours

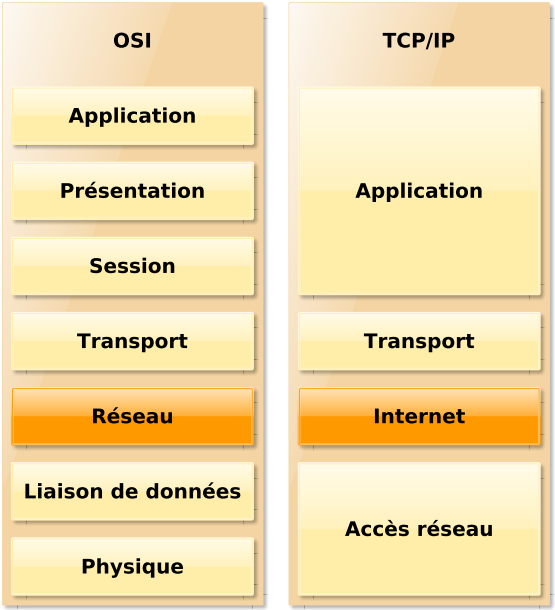
- Établir un flux d'information continu d'une machine vers une autre ;
- Établir, utiliser et fermer une connexion entre deux machines ;
- Garantir la communication complète, ordonnée et efficace d'une grande quantité d'information ;
- Établir une base programmatique pour la conception d'applications réseau.

Objectifs du cours

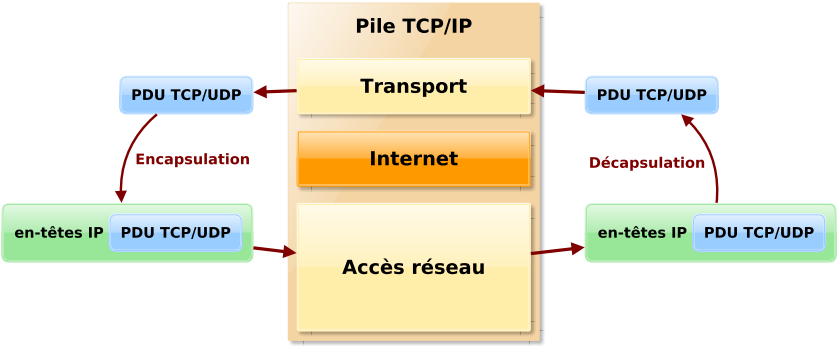
▲ Notions essentielles du cours, **à comprendre / connaître absolument**

★ Notions plus avancées (mais s'en rappeler un minimum !)

Présentation de la couche Internet


OSI
Application
Présentation
Session
Transport
Réseau
Liaison de données
Physique
TCP/IP
Application
Transport
Internet
Accès réseau

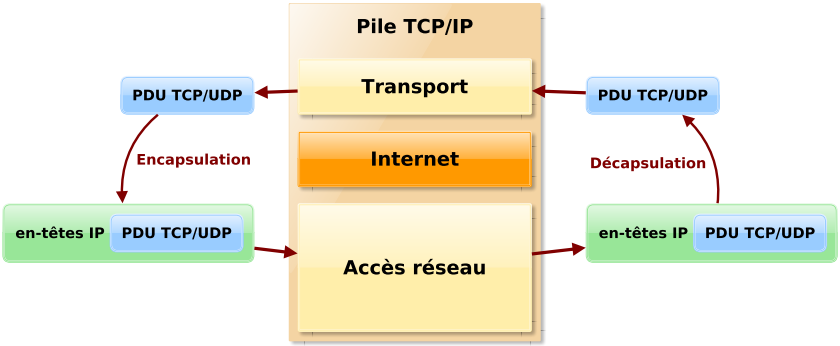
Missions de la couche Internet I



Premier rôle de la couche Internet

- En émission, **encapsuler** les paquets venant de la couche 4 (TCP, UDP) avec les informations de couche 3 (IP) et les transmettre à la couche 2 (Ethernet, 802.11) ;

Missions de la couche Internet II



Premier rôle de la couche Internet

- En réception, **décapsuler** les datagrammes de couche 3 provenant de la couche 2 et transmettre le paquet de couche 4 au protocole correspondant.

▲ Missions de la couche Internet

Second rôle de la couche Internet

Permettre l'interconnexion de plusieurs réseaux locaux en fournissant :

- Un système d'**adressage** inter-réseaux pour les équipements ;
- Un système d'**acheminement** des messages (routage) entre ces réseaux.

Donc...

En conséquence, les protocoles de la couche Internet doivent être implantés (au minimum) dans les *équipements terminaux* et dans les *routeurs*, qui utilisent les informations de l'en-tête de couche 3 pour prendre les décisions de routage.

Petit bestiaire de la couche Internet I

Principaux protocoles de la couche Internet

- **Internet Protocol (IP)** : au cœur de la couche réseau, il porte l'essentiel de ses missions. Versions IPv4 et IPv6, protocoles IPsec ;
- **Internet Group Management Protocol (IGMP)** : pour la gestion de la multidiffusion (*multicast*) ;
- **Internet Control Message Protocol (ICMP)** : mécanismes de contrôles et de messages d'erreur essentiels au fonctionnement de la couche Internet (avec une variante ICMPv6 spécifique).

Petit bestiaire de la couche Internet II

Je s'appelle route ?

Les **protocoles de routage**, essentiels au routage IP, sont généralement des protocoles de couches supérieures (transport ou application). Nous les évoquerons néanmoins dans le cadre de la couche Internet.

Le protocole IP

Le protocole IP

1. Présentation de la couche Internet

2. Le protocole IP
   - Caractéristiques du protocole IP
   - Format des datagrammes IPv4
   - La fragmentation IPv4
   - ICMP
   - Adressage IPv4

Le protocole IP (*Internet Protocol*) I

IP est le protocole **hégémonique** au niveau réseau / Internet
IP everywhere

Le protocole IP (*Internet Protocol*) II

Quelles variantes pour IP ?

- **IPv4 :** version la plus courante, adresses sur 32 bits, supportée par tous les équipements réseau du monde ;
- **IPv6 :** version moderne, adresses sur 128 bits, nombreuses améliorations par rapport à IPv4 ; supportée par la plupart des équipements réseau mais assez peu déployée.
- **IPsec [3] :** pas une variante d'IP, plutôt un ensemble de protocoles et de standards conçus pour apporter à la couche Internet des fonctionnalités de sécurité (authentification, chiffrement).

Par défaut dans ce cours : IP = IPv4

Le protocole IP (*Internet Protocol*) III

Propriétés du protocole IP

- Mode **non connecté** : pas de lien persistant entre émetteur et destinataire ;
- **Pas de garantie de remise** : le destinataire peut ne pas être disponible, il peut y avoir des pertes sur le parcours ;
- **Pas de garantie d'intégrité** : les données peuvent être altérées sur le parcours ;

Le protocole IP (*Internet Protocol*) IV

Propriétés du protocole IP

- **Pas d'accusé de réception** : on ne sait pas si les données sont arrivées *(mais il y a ICMP...)* ;
- **Pas de garantie sur l'ordonnancement** : les datagrammes peuvent suivre des chemins différents et arriver dans le désordre ;
- **Pas de garantie sur un débit minimum**, sur une **latence maximum** ou sur un **chemin suivi**.

Le protocole IP (*Internet Protocol*) V

IP est un exemple typique de protocole en *best effort*.

Les fonctionnalités de qualité de service (QoS) et diverses extensions peuvent tempérer certaines de ces affirmations.

Format d'en-tête des datagrammes IPv4

Voir Wireshark `ipv4frags.pcap`

Format d'en-tête des datagrammes IPv4 I

- ***Version* :** toujours à 4 (0100) pour IPv4;
- ***Header length* :** taille des en-têtes, en nombre de mots de 32 bits (variable à cause des options);
- *Differentiated Services Code Point* : indicateur de qualité de service (*QoS*), utilisé notamment pour la VoIP ou la vidéo;
- *Explicit Congestion Notification* : optionnel, pour un contrôle de congestion au niveau IP;

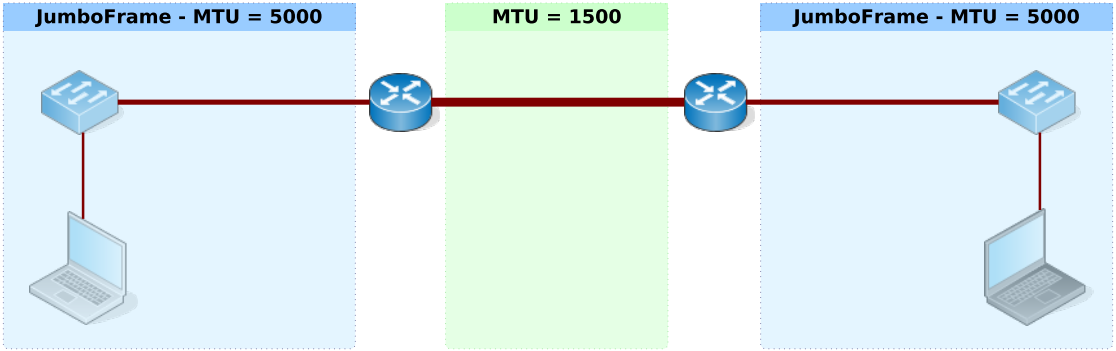
Format d'en-tête des datagrammes IPv4 II

- ***Total length* :** longueur totale du paquet, en octets ;
- *Identification* : identifiant utilisé pour reconnaître les fragments issus d'un même paquet d'origine ;
- *Flags* : le premier est toujours à 0, DF (*Don't Fragment*) et MF (*More Fragments*) sont utilisés pour la fragmentation ;

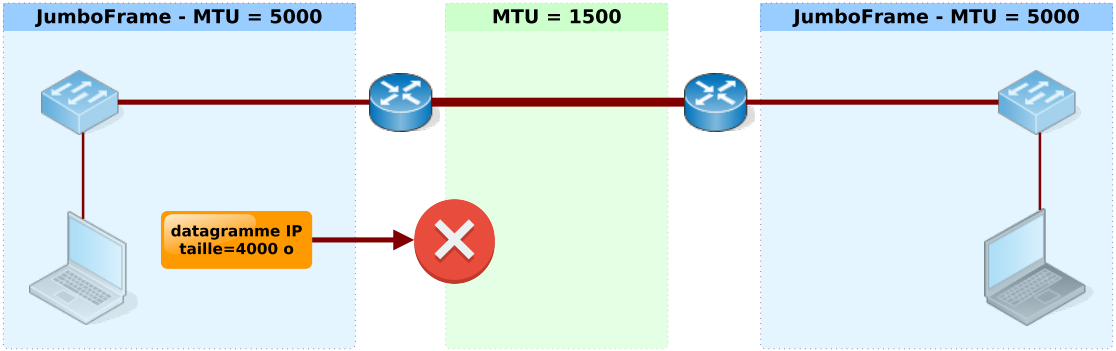
Format d'en-tête des datagrammes IPv4 III

- *Fragment offset* : en cas de fragmentation, décalage, en mots de 8 octets, du fragment courant par rapport au début du paquet d'origine ;
- ***Time To Live (TTL)* :** nombre de sauts restants (décrémenté à chaque routeur) ;
- ***Protocol* :** identification du protocole utilisé (1 pour ICMP, 6 pour TCP, 17 pour UDP… cf. RFC 790) ;
- ***Header checksum* :** code détecteur d'erreur sur les en-têtes IP ;
- ***Source / Destination IP Address* :** *self-explanatory*, non ?

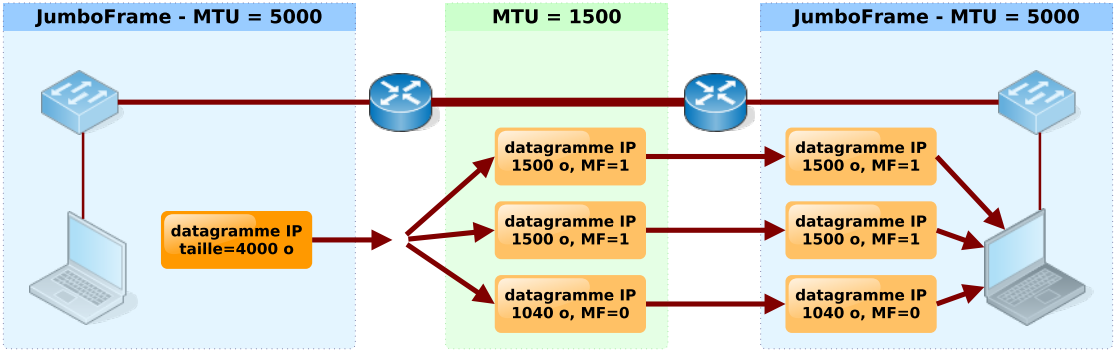
La fragmentation IPv4



La fragmentation IPv4



La fragmentation IPv4



La fragmentation IPv4 I

Mise en œuvre “basique” de la fragmentation

- La fragmentation est réalisée par le **routeur** qui doit envoyer le datagramme sur un réseau local, directement connecté, avec un MTU trop faible ;
- Le datagramme est **découpé** en autant de fragments que nécessaire pour respecter le MTU, en tenant compte des en-têtes IP ;
- Un **identifiant** est choisi pour les fragments d’un même datagramme ;

La fragmentation IPv4 II

Mise en œuvre “basique” de la fragmentation

- Le ***fragment offset*** de chaque fragment est calculé en mots de 8 octets ;
- Les $n - 1$ premiers fragments ont leur bit **MF à 1**, le dernier a son bit **MF à 0** ;
- Les fragments sont envoyés sur le réseau comme des datagrammes indépendants et sont **réassemblés par le destinataire**.

La fragmentation IPv4 II

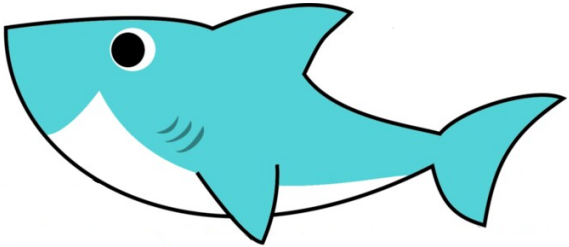
Mise en œuvre “basique” de la fragmentation

- Le ***fragment offset*** de chaque fragment est calculé en mots de 8 octets ;
- Les $n - 1$ premiers fragments ont leur bit **MF à 1**, le dernier a son bit **MF à 0** ;
- Les fragments sont envoyés sur le réseau comme des datagrammes indépendants et sont **réassemblés par le destinataire**.

C’est pas bien !

La fragmentation est quelque chose que l’on souhaite éviter. Plusieurs mécanismes, dans les couches Internet et transport, sont là pour cela.

Petit exercice Wireshark



‘

1. Ouvrez la capture `ipv4frags.pcap`
2. Combien de fragments ?
3. Quelle est la taille du MTU ?
4. Quelles sont les valeurs des flags des premier et dernier fragments ?

ICMP I

Internet Control Message Protocol (ICMP)

Protocole “assistant”d’IP, messages de contrôle permettant à IP de fonctionner au mieux. Protocole du “haut de la couche Internet”, encapsulé dans IP.

ICMP II

Les missions d'ICMP

- Tester activement la connectivité avec une interface (*ping*) ;
- Avertir lorsqu'une machine, un réseau ou un protocole est injoignable (messages *XXX unreachable*) ;
- Avertir lorsque la route choisie est trop longue (expiration du TTL) ;
- Avertir lorsque la route choisie exige de la fragmentation ;
- Permettre la publication et découverte de routes (entre routeurs, voir section suivante).

ICMP echo / request, alias ping / pong

Exemple : “ping”d’une machine distante

```
1   > ping -c 5 8.8.8.8
2   PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
3   64 bytes from 8.8.8.8: icmp_seq=1 ttl=121 time=35.6 ms
4   64 bytes from 8.8.8.8: icmp_seq=2 ttl=121 time=34.7 ms
5   64 bytes from 8.8.8.8: icmp_seq=3 ttl=121 time=33.9 ms
6   64 bytes from 8.8.8.8: icmp_seq=4 ttl=121 time=32.7 ms
7   64 bytes from 8.8.8.8: icmp_seq=5 ttl=121 time=33.8 ms
8
9   --- 8.8.8.8 ping statistics ---
10  5 packets transmitted, 5 received, 0% packet loss, time 4007ms
11  rtt min/avg/max/mdev = 32.750/34.171/35.601/0.968 ms
```

▲ Adressage IPv4

Format des adresses IPv4

Adresses IPv4 sur **32 bits (4 octets)** :
11000001 00110110 11000000 000110101
En **notation décimale pointée :**
193.54.192.21
Chaque chiffre représentant un octet, il peut théoriquement varier entre 0 et 255.

Interface réseau

Une adresse IP est associée à une **interface réseau**, concept logique qui peut correspondre à un adaptateur physique (carte réseau) ou émulé (interface virtuelle).

▲ Adressage IPv4 I

Adresse réseau et adresse hôte

Les n premiers bits d'une adresse IPv4 déterminent l'**adresse réseau**. Ils sont communs à toutes les interfaces d'un même réseau local (cette adresse *définit* la notion de réseau).
Les $32 - n$ derniers bits sont spécifique à l'**adresse hôte**. Ils sont (normalement) propres à chaque interface sur le réseau local. Dans l'adresse réseau, ces bits sont positionnés à zéro.

Adresse complète (adresse de l'hôte) :	**193.54.192.21**
Adresse réseau (8 derniers bits à 0) :	**193.54.192.0**

Adressage IPv4 II

Comment déterminer de combien de bits est formée l'adresse réseau ?

Classes d'adresses IPv4 I

Classes

Historiquement, l'espace d'adressage d'IPv4 a été divisé en **classes** de manière à définir des réseaux de tailles différentes (identifiants de réseau sur 8, 16 ou 24 bits).

Classe	Bits réseau	Bits hôte	Nb réseaux	Nb hôtes	Plage d'adresses
A	8	24	128 (2^7)	~16M (2^{24})	0.0.0.0-127.255.255.255
B	16	16	16384 (2^{14})	65536 (2^{16})	128.0.0.0-191.255.0.0
C	24	8	~2M (2^{21})	256 (2^8)	192.0.0.0-223.255.255.0
D	N/A	N/A	N/A	N/A	224.0.0.0-239.255.255.255
E	N/A	N/A	N/A	N/A	240.0.0.0-255.255.255.255

Classes d'adresses IPv4 II

Quelques autres plages d'adresses réservées

- 0.0.0.0 – 0.255.255.255 (plage réservée classe A);
- **127.0.0.0 – 127.255.255.255 (boucle locale)**;
- 169.254.0.0 – 169.254.255.255 (adresses locales autoconfigurées);
- 192.0.0.0 – 192.0.0.255, 223.255.255.0 – 223.255.255.255 (plages réservées classe C);
- **255.255.255.255 (diffusion locale)**;
- ...

▲ Adressage IPv4 *classless* I

Classless InterDomain Routing (CIDR) sans E

Principe : on définit un réseau IPv4 en accolant directement le nombre de bits de l'identifiant du réseau (notation CIDR) :

172.16.1.0/24
10.42.128.0/17
192.168.0.192/26

▲ Adressage IPv4 *classless* II

Classless InterDomain Routing (CIDR) sans E

Cette information est souvent représentée sous la forme d'un **masque de sous-réseau**, 32 bits en notation décimale pointée avec les bits de l'identifiant réseau à 1 et les autres à 0 :

255.255.255.0
255.255.128.0
255.255.255.192

Les masques des classes A, B et C sont respectivement 255.0.0.0, 255.255.0.0 et 255.255.255.0.

Tous les bits de l'hôte à 0 → adresse réseau
Tous les bits de l'hôte à 1 → adresse de diffusion

▲ Adressage IPv4 *classless* I

Manipulation des masques de sous-réseau

Exemple : adresse = 192.168.1.5, masque = 255.255.192.0 (18 bits)

Quelle est l'adresse du réseau local correspondant ?

▲ Adressage IPv4 *classless* I

Manipulation des masques de sous-réseau

Exemple : adresse = 192.168.1.5, masque = 255.255.192.0 (18 bits)

Quelle est l'adresse du réseau local correspondant ?

C'est le résultat d'un `ET` logique, bit à bit, entre les deux adresses :

```
11000000 10101000 00000001 00000101 - 192.168.1.5
11111111 11111111 11000000 00000000 - 255.255.192.0
```

```
11000000 10101000 00000000 00000000 - 192.168.0.0
```

▲ Adressage IPv4 *classless* II

Manipulation des masques de sous-réseau

L'adresse de diffusion (*broadcast*) est obtenue en positionnant à 1 tous les bits de la partie machine de l'adresse : `11000000 10101000 00111111 11111111` - `192.168.63.255`

- L'adresse 192.168.5.1 est-elle sur le même réseau ?
- L'adresse 192.168.130.1 est-elle sur le même réseau ?

Exercices de calcul

- Calculs de classes
- Calculs de réseaux locaux
- Calculs de notations CIDR

Bibliographie I

[1] Cookie Connecté. *Comprendre le DHCP en 3 minutes*. https://www.youtube.com/watch?v=yH9UvkeAz-I. 2020.

[2] Cookie Connecté. *Comprendre les modèles OSI et TCP/IP*. https://www.youtube.com/watch?v=26jazyc7VNk. 2020.

[3] Wikipedia. *IPsec*. https://fr.wikipedia.org/wiki/IPsec. 2021.

[4] Wireshark. *Sample captures*. https://gitlab.com/wireshark/wireshark/-/wikis/SampleCaptures. 2020.