Réseaux et sécurité

CNAM

Daniel Porumbel

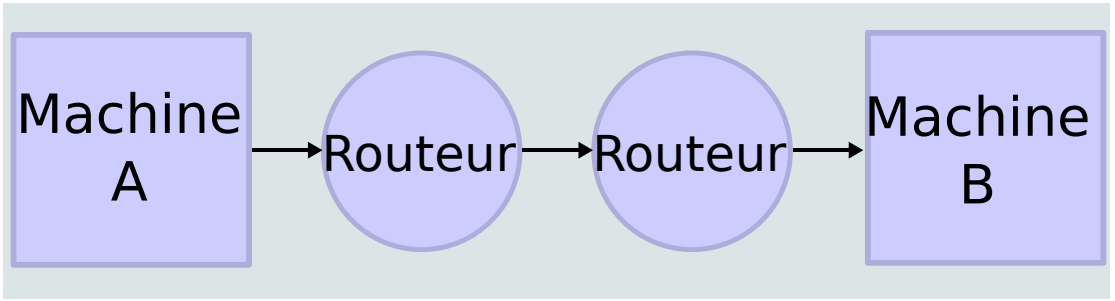
Contributions aux slides:
Fred Hemery (Univ. Artois)
Pascal Nicolas (Univ. Angers)

La pile TCP/IP

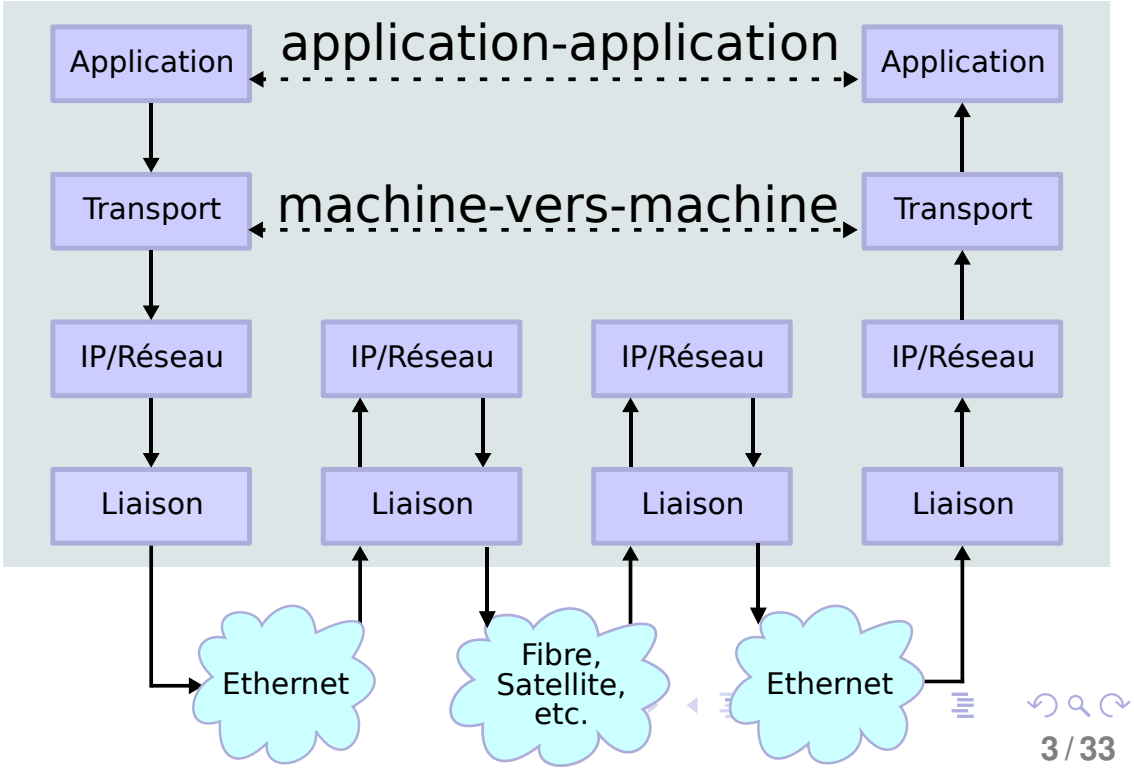
Quatre couches de protocoles qui s'appuient sur la couche physique :

1. Couche Application (Firefox, MSN, FTP)
2. Couche Transport (TCP/UDP)
3. Couche IP/Réseaux
4. Couche Liaison

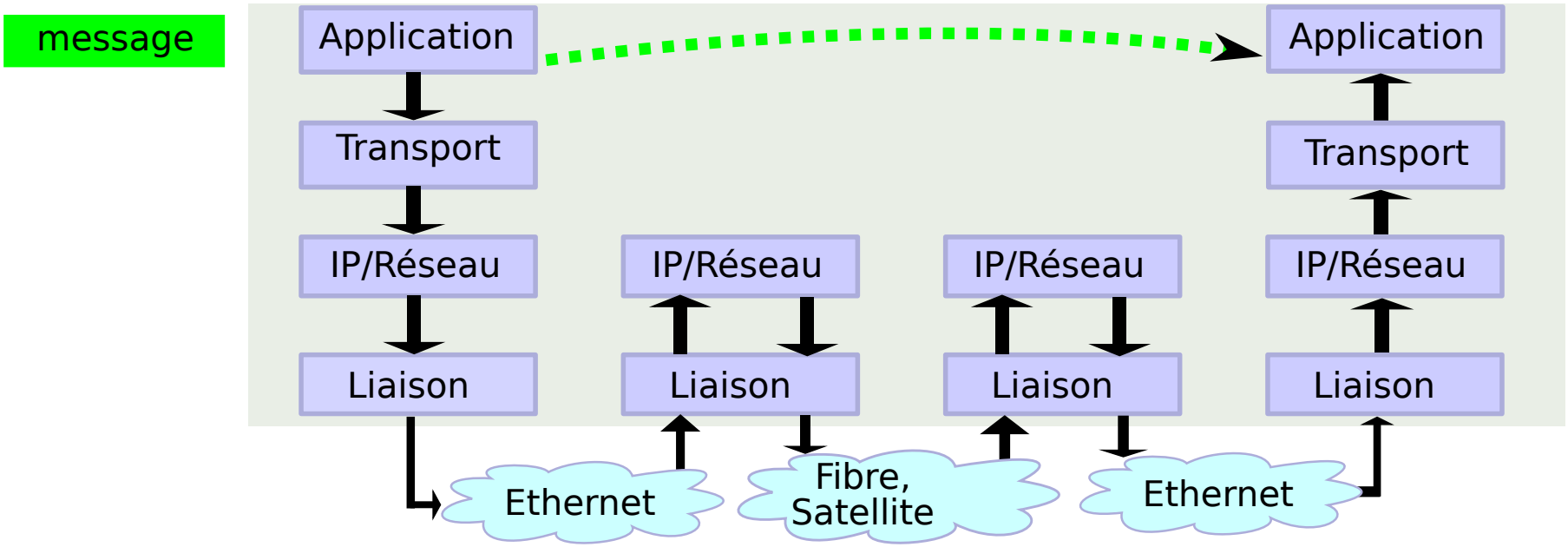
Topologie Réseau



Flux de données

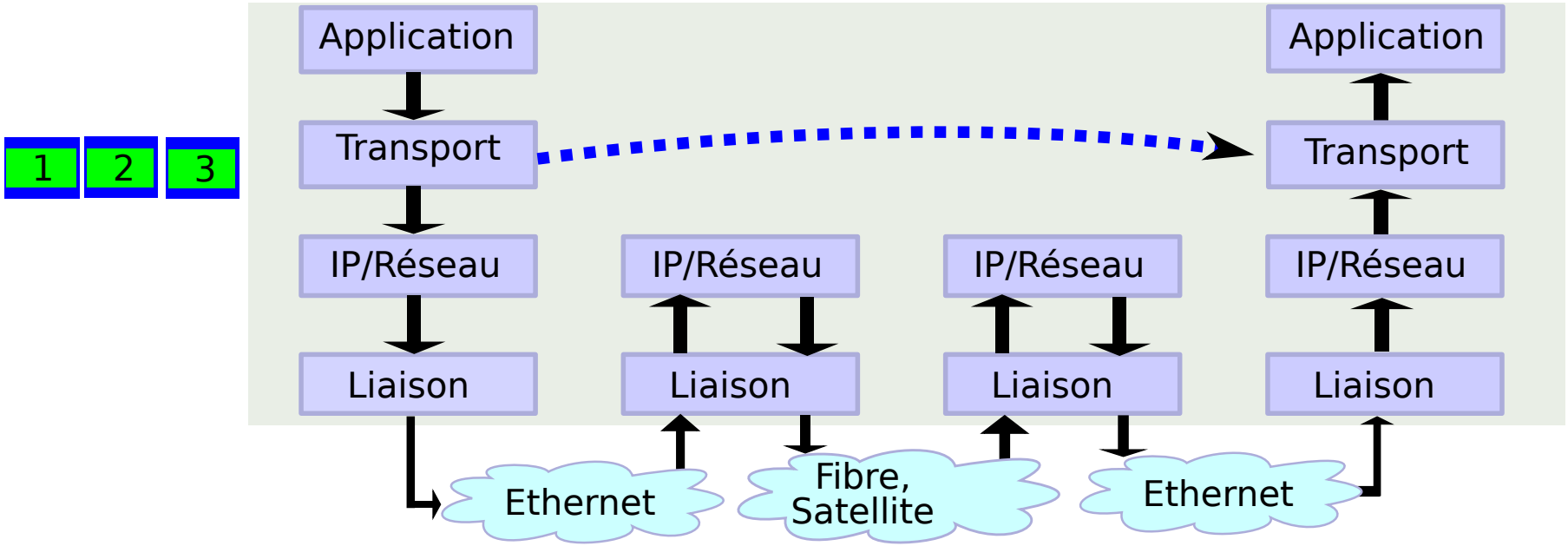


La Couche Application



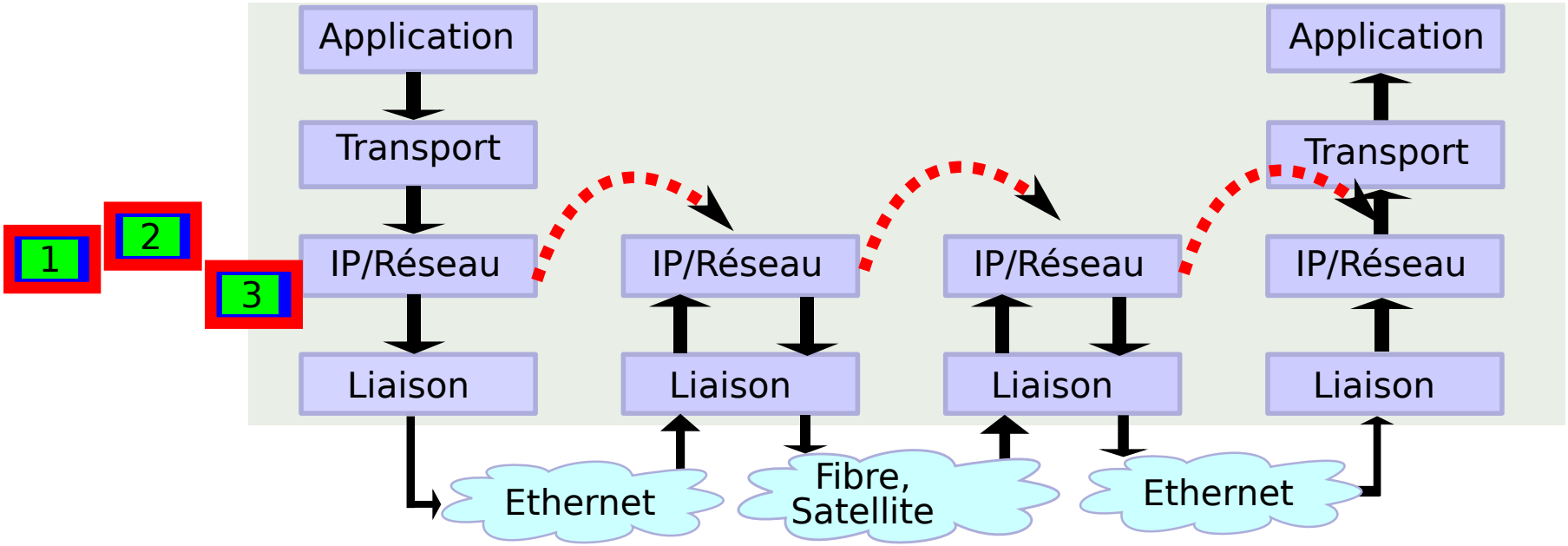
- Cette couche analyse les protocoles de haut niveau (http, ssh), y compris la cryptographie
  - Les messages sont envoyés d'une application à l'autre (ex., du client au serveur)
    - `10.0.0.1` vers `10.0.0.2` : "Donne moi le fichier `index.html`"

La couche Transport



- Le *message* de la couche Application est découpé en *segments*
- La transmission se fait en utilisant des sockets
  - Une socket = une adresse IP + un port, ex. `10.0.0.1:80` ou `10.0.0.1:22`
- La communication *socket—socket* fait abstraction des machines intermédiaires

La couche Réseaux

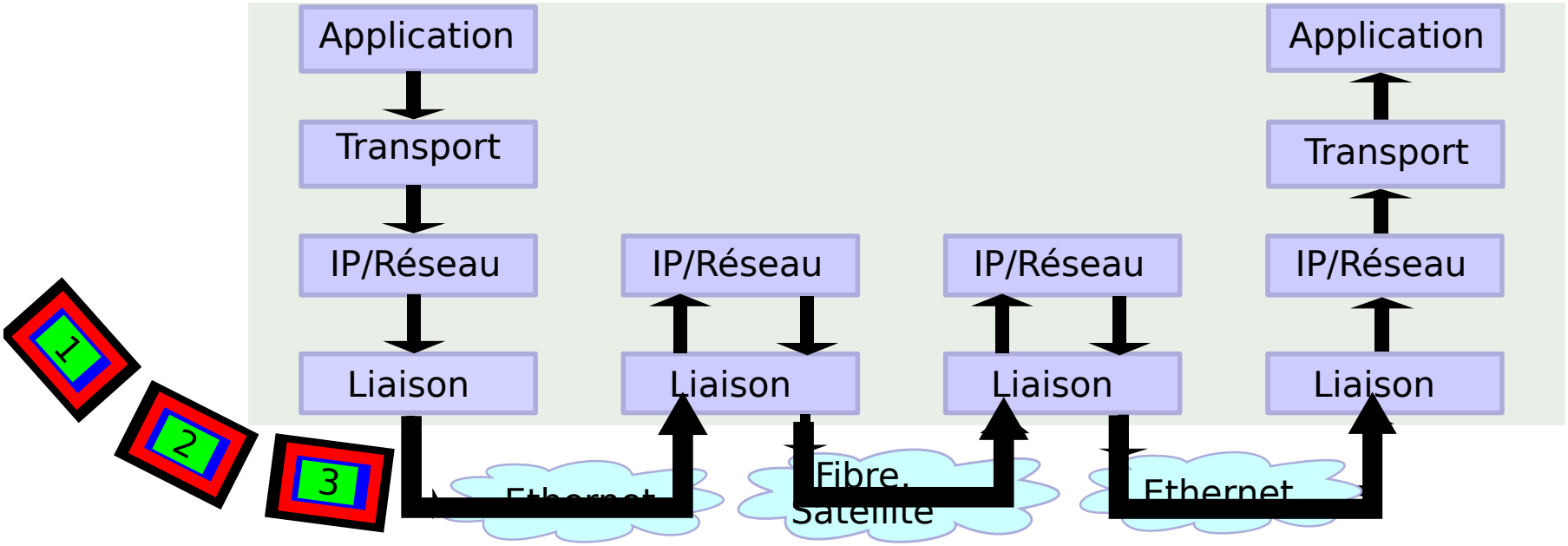


- Couche transport : segment envoyé de A vers B

$$\Longrightarrow$$

- Couche réseau : transfert $A \to A_1 \to A_2 \to A_3 \ldots\ldots\cdots \to B$
  - Chaque routeur peut “cacher” un pirate qui sniffe la communication

La couche Liaison



- La couche *liaison* indique comment les paquets sont transportés sur la couche physique (Ethernet/Wifi)
- L'en-tête des trames Ethernet comporte l'adresse MAC destination
- Le protocole ARP fait la connexion IP $\rightarrow$ MAC.
  - Etant donnée une adresse IP de notre sous-réseau, quelle est son adresse MAC ?
  - Un point très sensible de la sécurité des réseaux locaux

Vulnérabilités Couche Application : le DNS (*nom* $\rightarrow$ IP)

Pour se connecter à un site :

- Le navigateur interroge son serveur DNS (Domain Name Server)
  - Voir `/etc/resolv.conf` sous Linux
  - Voir `/etc/hosts` sous Linux
- Le serveur DNS a deux options :
  1. Il renvoie l'adresse IP s'il a cette information OU
  2. Demande cette information à un serveur DNS de niveau supérieur
- Vulnérabilité grave : ce processus n'est pas trop sécurisé $\Rightarrow$ si la réponse DNS est fausse, la navigation Web est compromise

Vulnérabilités Couche Transport : le TCP

Une connexion TCP comporte trois étapes :

1. Établissement de la connexion TCP.
2. Transfert de données
3. Fermeture de la connexion TCP.

Ce canal de communication est une socket défini par deux adresses IP:PORT, par exemple :

`123.123.123.123:20312` ⇔ `207.142.131.203:80`

Couche Réseau/IP

1. Chaque segment TCP est placé dans un paquet IP.
2. Chaque paquet IP indique une IP source (l'émetteur) et une IP destination finale du paquet.
3. Chaque paquet est transféré de routeur en routeur jusqu'à l'adresse IP destination
4. Chaque routeur a une table de routage qui indique l'IP de sortie à emprunter pour arriver à la destination finale.

Couche Réseau/IP

1. Chaque segment TCP est placé dans un paquet IP.
2. Chaque paquet IP indique une IP source (l'émetteur) et une IP destination finale du paquet.
3. Chaque paquet est transféré de routeur en routeur jusqu'à l'adresse IP destination
4. Chaque routeur a une table de routage qui indique l'IP de sortie à emprunter pour arriver à la destination finale.

Couche Réseau/IP

1. Chaque segment TCP est placé dans un paquet IP.
2. Chaque paquet IP indique une IP source (l'émetteur) et une IP destination finale du paquet.
3. Chaque paquet est transféré de routeur en routeur jusqu'à l'adresse IP destination
4. Chaque routeur a une table de routage qui indique l'IP de sortie à emprunter pour arriver à la destination finale.

Couche Réseau/IP

1. Chaque segment TCP est placé dans un paquet IP.
2. Chaque paquet IP indique une IP source (l'émetteur) et une IP destination finale du paquet.
3. Chaque paquet est transféré de routeur en routeur jusqu'à l'adresse IP destination
4. Chaque routeur a une table de routage qui indique l'IP de sortie à emprunter pour arriver à la destination finale.

Vulnérabilités Couche Réseau

Un paquet IP peut transiter des dizaines de routeurs pour arriver à destination

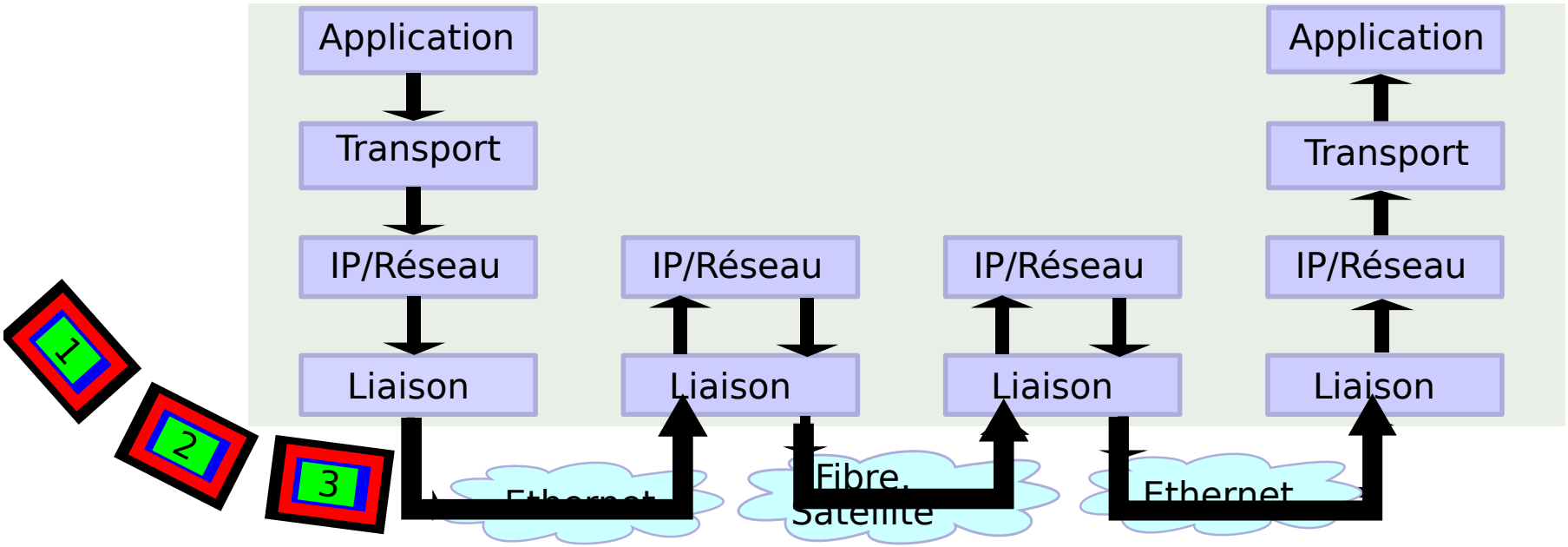
- Chaque routeur peut “cacher” un pirate qui sniffe la communication
- Données pas codées par les couches supérieurs $\Rightarrow$ tout routeur peut forger de faux paquets IP (l’attaque du l’homme du milieu)

Vulnérabilités Couche Réseau

Un paquet IP peut transiter des dizaines de routeurs pour arriver à destination

- Chaque routeur peut “cacher” un pirate qui sniffe la communication
- Données pas codées par les couches supérieurs $\Rightarrow$ tout routeur peut forger de faux paquets IP (l’attaque du l’homme du milieu)

Rappels : La couche Liaison



- Les paquets IPs sont emboités dans des trames Ethernet/Wifi
  - les trames comportent comme destination une adresse MAC (Media Access Control) : 6 octets, ex hexa : `00:12:3F:DD:A2:17`
- Si A a besoin d'accéder à IP_B, A doit d'abord obtenir l'adresse MAC_B de B, ou la MAC de la passerelle
- Pour obtenir MAC_B, A fait appel au protocole ARP non-sécurisé :
  - X demande en diffusion l'adresse MAC_B
  - X fait confiance à la réponse

Vulnérabilités couche Liaison 1

- Dans un réseau Wifi/Ethernet, plusieurs machines C, D, E . . . sont en connexion directe avec l'émetteur A
- Une trame envoyée vers MAC_B devrait être reçue uniquement par B mais pas de contrainte physiques pour assurer cela
- Pour faire capter les trames destinées à d'autres machines, une carte peut passer en :
  - Mode Moniteur en Wifi (`iwconfig`)
  - Mode "Promiscuité" en Ethernet (`ifconfig`)

- Les signaux électriques sur un câble Ethernet peuvent être sniffés
  - Solution de protection : pressuriser les câbles

Vulnérabilités couche Liaison 1

- Dans un réseau Wifi/Ethernet, plusieurs machines C, D, E ... sont en connexion directe avec l'émetteur A
- Une trame envoyée vers MAC_B devrait être reçue uniquement par B mais pas de contrainte physiques pour assurer cela
- Pour faire capter les trames destinées à d'autres machines, une carte peut passer en :
  - Mode Moniteur en Wifi (`iwconfig`)
  - Mode "Promiscuité" en Ethernet (`ifconfig`)

- Les signaux électriques sur un câble Ethernet peuvent être sniffés
  - Solution de protection : pressuriser les câbles

1. Le fonctionnement de la pile TCP/IP
2. Exemples d'attaques et de vulnérabilités

Pirater les mails des eurodéputés : un “jeu d’enfant” selon un pirate cité par médiapart (2013)

“Avec un ordinateur portable bas de gamme équipé du wifi et quelques connaissances que tout le monde est capable de trouver sur internet, n’importe qui est capable de faire la même chose”

La méthode est simple

1. le pirate s’est installé dans un lieu public à proximité du parlement.
2. il s’est arrangé pour que les téléphones mobiles des gens se trouvant à portée passent par le wifi de son ordinateur pour se connecter à internet
3. Cela lui permet de récupérer les identifiants et mots de passe de ses cibles
   - le téléphone affiche un message abscons, mais beaucoup d’utilisateurs cliquent OK sans le lire

2 Exemples d'attaques et de vulnérabilités

Exemple 1 : Phishing

Attaque facile à base d'ingénierie sociale (*social engineering*)

- Envoyer à la victime une page web/mail identique à celui d'un organisme de confiance (la banque de la victime) et lui demander des mots de passe
- Cibles populaires : banques, amazon, paypal, ebay
- Leçons :
  - L'adresse e-mail d'un expéditeur ne garantit pas son identité
    - tout le monde peut envoyer un email avec expéditeur `bill.gates@microsoft.com`
  - attention à vérifier l'adresse web dans la barre d'adresse du navigateur web

Exemple 1 : Phishing

Attaque facile à base d'ingénierie sociale (*social engineering*)

- Envoyer à la victime une page web/mail identique à celui d'un organisme de confiance (la banque de la victime) et lui demander des mots de passe
- Cibles populaires : banques, amazon, paypal, ebay
- Leçons :
  - L'adresse e-mail d'un expéditeur ne garantit pas son identité
    - tout le monde peut envoyer un email avec expéditeur `bill.gates@microsoft.com`
  - attention à vérifier l'adresse web dans la barre d'adresse du navigateur web

Exemple 2 : applications web et réseaux sociaux

Sur les réseaux sociaux/smart-phones, les utilisateurs permettent souvent aux programmes *third-party* (écrits par d'autres utilisateurs) d'accéder à leurs mots de passe
Facebook offre des prix pour ceux qui trouvent des failles de sécurités dans les applications

- record détenu par un homme qui a touché 7000$ pour six failles
- Facebook offre 500$ au minimum mais certaines failles valent plus

Exemple 3 : Le Déni de Service 1

Cette attaque est souvent distribuée. Un exemple :

- Si la machine A exécute "`ping` B", B répond avec un *ping reply*
- Si les machines $A_1, A_2, \ldots A_n$ sont infectées est programmées à exécuter "ping B" m fois

  $\Rightarrow$ B doit envoyer $n \cdot m$ réponses

  $\Rightarrow$ Si $n > 1.000.000$ et $m = 100$, B doit envoyer des centaines de millions de *ping reply* $\Longrightarrow$ B ne peut plus gérer d'autres demandes légitimes et subit un déni de service.

Exemple 3 : Le Déni de Service 1

Cette attaque est souvent distribuée. Un exemple :

- Si la machine A exécute "`ping` B", B répond avec un *ping reply*
- Si les machines $A_1, A_2, \ldots A_n$ sont infectées est programmées à exécuter "ping B" m fois

  $\Rightarrow$ B doit envoyer $n \cdot m$ réponses

  $\Rightarrow$ Si $n >$ 1.000.000 et $m = 100$, B doit envoyer des centaines de millions de *ping reply* $\Longrightarrow$ B ne peut plus gérer d'autres demandes légitimes et subit un déni de service.

Exemple 3 : Le Déni de Service 2

Certaines attaques Déni de Service sont renommées

Attaque historique 1 7-8 février 2000, *Yahoo, Amazon, Ebay et Cnn.com* ont été quasi-inaccessibles $\Rightarrow$ pertes de millions

Attaque historique 2 8 décembre 2010, *MasterCard et Visa* quasi-inacces à cause du groupe “Anonymous” (solidarité avec Wiki-Leaks)

Il y a des pirates spécialisés dans la “levée” de *zombies* (les machines $A_1, A_2, \ldots A_n$ infectées pour installer des agents d'attaque)

- Cette “armée de zombies” peut être ensuite louée à d'autres pirates

Exemple 3 : Le Déni de Service 2

Certaines attaques Déni de Service sont renommées

Attaque historique 1 7-8 février 2000, *Yahoo, Amazon, Ebay et Cnn.com* ont été quasi-inaccessibles $\Rightarrow$ pertes de millions

Attaque historique 2 8 décembre 2010, *MasterCard et Visa* quasi-inacces à cause du groupe "Anonymous" (solidarité avec Wiki-Leaks)

Il y a des pirates spécialisés dans la "levée" de *zombies* (les machines $A_1, A_2, \ldots A_n$ infectées pour installer des agents d'attaque)

- Cette "armée de zombies" peut être ensuite louée à d'autres pirates

Exemple 4 : Failles de programmation

Les pirates cherchent souvent des failles dans *les implémentations des protocoles*. Exemple *C/C++* :

```
1 int main (int argc, char **argv)
2 {
3     char buf [1000] ;
4     strcpy (buf,argv [1]) ;
5 }
```

Pour mémoire :*Linux, Windows et Mac OS* sont écrits en *C/C++*

Exécution :

```
@$ ./demo aaa...1010 fois...aaaaaaaaaaaaaa
Segmentation fault
```

→ Erreur de *buffer overflow* : dépassement de tampon/mémoire

→ Ce type de problème apparaît très souvent lors de la réception de paquets, trames et autres données de réseaux

Exemple 4 : Failles de programmation

Les pirates cherchent souvent des failles dans *les implémentations des protocoles*. Exemple *C/C++* :

```
1 int main (int argc, char **argv)
2 {
3     char buf [1000] ;
4     strcpy (buf,argv [1]) ;
5 }
```

Pour mémoire :*Linux, Windows et Mac OS* sont écrits en *C/C++*

Exécution :

```
@$ ./demo aaa...1010 fois...aaaaaaaaaaaaaa
Segmentation fault
```

→ Erreur de *buffer overflow* : dépassement de tampon/mémoire
→ Ce type de problème apparaît très souvent lors de la réception de paquets, trames et autres données de réseaux

Exemple 5 : Ping de la mort

- Attaque historique réalisée par un paquet ping malformé
- Un ping a normalement une taille de 56 octets $\rightarrow$ risques dépassement de mémoire pour des paquets plus grands
  - Ce dépassement de mémoire provoquait un crash sur plusieurs SEs (Windows/Linux)
- Un simple *ping* pouvait provoquer un crash d'une machine cible (Unix, Linux, MacOS, Windows)