Chapitre 2

Vulnérabilités protocolaires et attaques réseaux

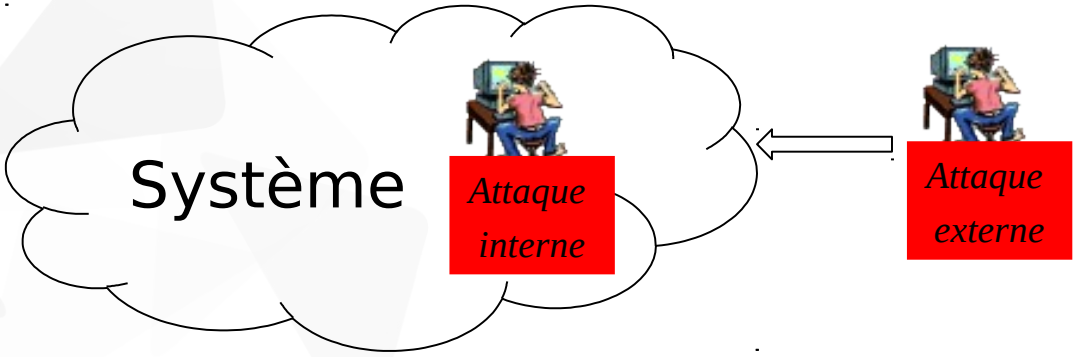
Définitions

- Vulnérabilité:
  - **Défaut ou faiblesse** d'un système dans sa conception, sa mise en œuvre ou son contrôle interne pouvant mener à une faille de sécurité ou à la violation de sa politique de sécurité.
- Menace:
  - La **possibilité** qu'une vulnérabilité soit exploitée accidentellement ou par un agent malicieux.
- Attaque
  - **Action** malveillante exploitant des vulnérabilités d'un système
  - Employée pour casser les services de la sécurité en détournant les mécanismes

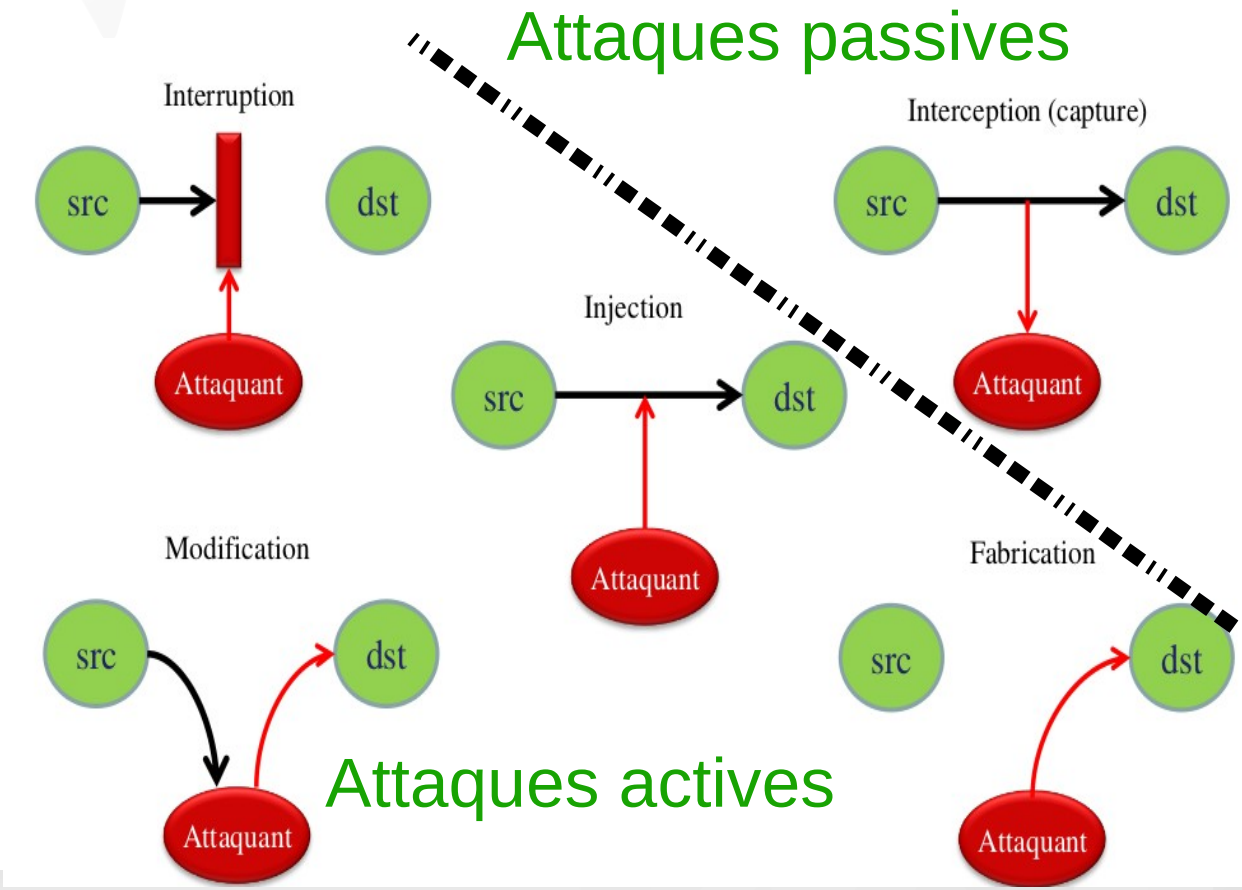
Objectifs / motivation des attaquants

- Objectifs
  - Désinformer
  - Empêcher l'accès à une ressource
  - Prendre le contrôle d'une ressource
  - Récupérer de l'information
  - Utiliser le système compromis pour attaquer un autre (rebondir)
  - Etc.
- Motivations
  - Vengeance/rancune
  - Politique/religion
  - Défis intellectuels
  - Envie de nuire aux autres
  - Impressionner les autres
  - Vol d’information
  - Désir d’argent
  - Falsification d’information
  - Etc.

Typologie d'attaques (Rappel)



Type d'attaque	Propriétés visées
interception	confidentialité
interruption	disponibilité
injection	Integrité
modification	Confidentialité Integrité
fabrication	authenticité



Attaques passives/actives

- Attaques passives
  - **Écoute et analyse du trafic réseau**
  - Exemple d’outils: wireshark,
  - But: trouver des informations susceptibles d'intéresser un attaquant
    - Adresses IP importantes
    - Architecture du réseau
    - Emplacement des nœuds
    - Informations d’authentification
    - Information secrète (en cas de guerre par exemple)
    - Etc.
- Attaques actives
  - **Modification** des données stockées ou en transit
  - **Injection** de données,
  - **Rejeu**: ré-envoyer d’anciens données
  - **Fabrication** (mascarade): injecter des données en spécifiant une adresse source légitime
  - **Suppression** de données
  - **Etc.**

Approche commune des attaques

- Etape 1: Reconnaissance
  - Recherche d'informations sur le système cible
- Etape 2: Enumération
  - Ressources réseaux, utilisateurs et groupes, applications...
- Etape 3: Balayage (scan)
  - Scan des ports, des vulnérabilités, du réseau (topologie)
- Etape 4: **Exploit**
  - Exploiter les vulnérabilités des protocoles, des applications, de l'OS, du réseau, etc.
- Etape 5: Maintenir l'accès.
- Etape 6: Effacer les traces d'intrusion.

Exploit des vulnérabilités

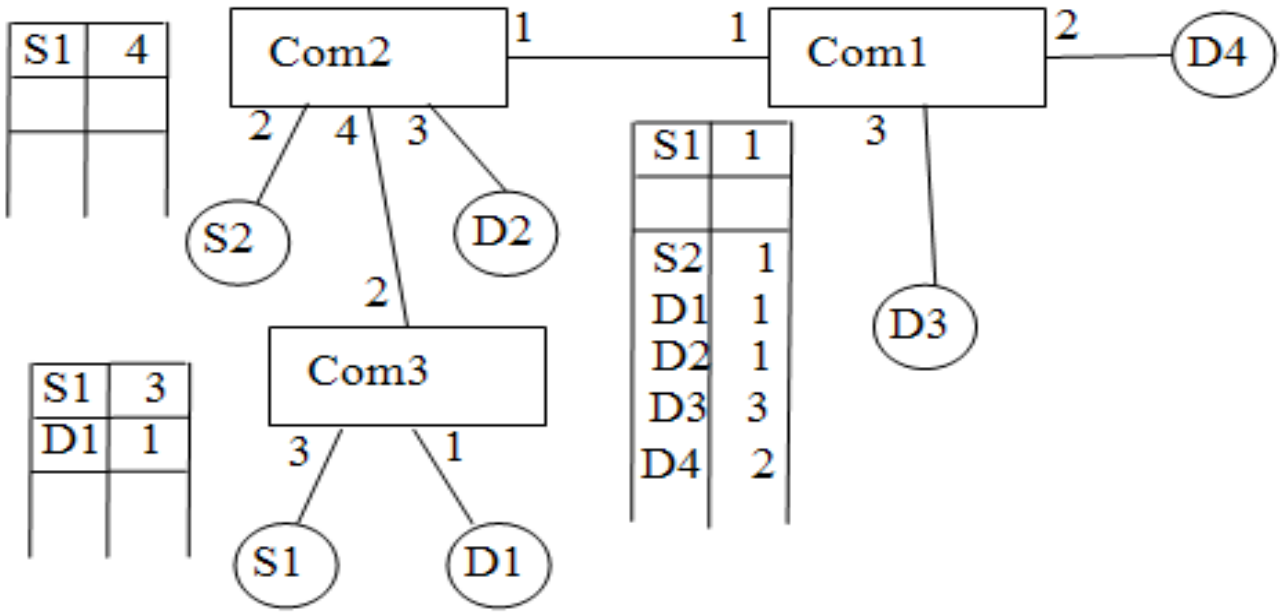
- Exploiter les vulnérabilités
  - Des protocoles
    - Protocoles légers, non sécurisés, peu de contrôle
  - Des implémentations
    - Exemple : mot de passe en clair sur le réseau
  - Des configurations :
    - Exemple : firewall mal configuré
  - Des mécanismes d'authentification
    - Exemple : mot de passe simple

Exemples d'attaques réseaux

- Niveau liaison :
  - Inondation de la table de commutation (CAM : Content addressable memory)
  - Usurpation de l’adresse MAC (MAC spoofing)
- Niveau réseau
  - IP spoofing
  - ARP spoofing
- Niveau transport
  - TCP syn flooding
- Niveau application
  - DHCP starvation
  - Faux serveurs DHCP

Ethernet - rappel

- Réseau composé de répéteurs (hubs) et de commutateurs (switches) liés en point à point
  - Les hubs diffusent les trames.
  - Les commutateurs utilisent leurs tables de commutation (Content Adressable Memory : CAM) pour diriger une trame vers un port spécifique s'il peut déterminer à quel sous réseau appartient le destinataire de la trame. Sinon, la trame est diffusé de façon générale.



Ethernet- Rappel

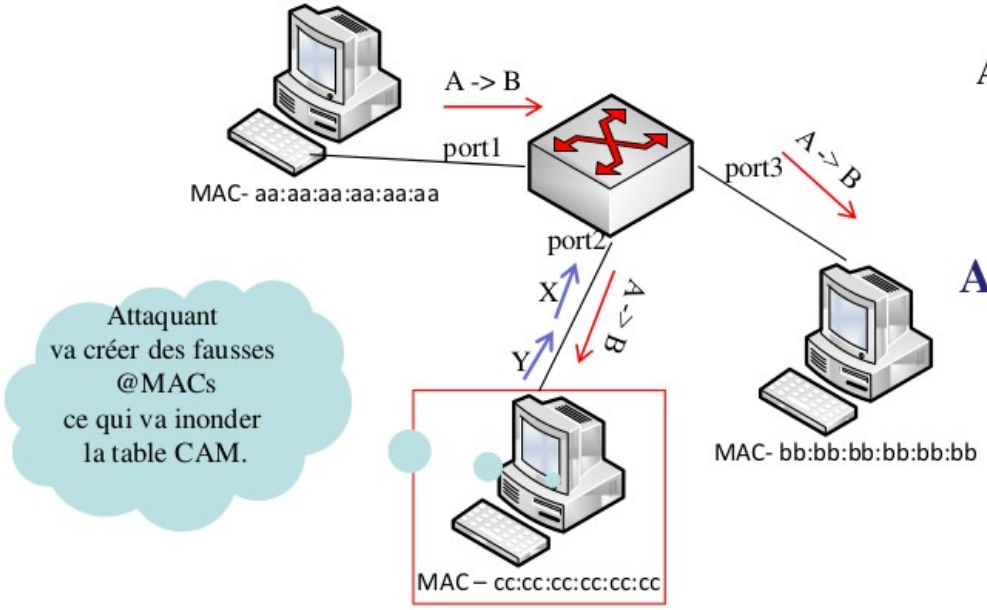
- Les commutateurs apprennent les adresses MAC à partir de l'adresse source des trames Ethernet sur les ports

- Quand un dispositif connecté à un port particulier envoie une trame vers le commutateur, le commutateur note l'@MAC source et le port puis vérifie la table CAM:
  - Si c'est une nouvelle @MAC, il ajoute une entrée dans la table CAM,
  - S'il s'agit d'une @MAC existante sur un port différent, il met à jour le numéro de port associé,
  - si c'est la même @MAC sur le même port, il met à jour l'âge.

- Lorsque la table est pleine, des entrées existantes sont enlevées.

Attaques Ethernet: inondation de la table CAM

- **Vulnérabilité:** Lorsqu'une adresse MAC ne se retrouve pas dans la table CAM, le commutateur diffuse la trame sur tous les ports.
- **Attaque:** L'attaquant inonde le commutateur avec de fausses trames ==> **le commutateur se transforme en HUB**
- **Risque:** Divulgation d'informations sensibles (p.ex. mots de passe) qui ne devraient pas être envoyées sur un port.



Avant

Port1	aa:aa:aa:aa:aa:aa
Port 2	cc:cc:cc:cc:cc:cc
Port 3	bb:bb:bb:bb:bb:bb

Assume CAM Table Now Fu

Après

Port1	aa:aa:aa:aa:aa:aa
Port 2	xx:xx:xx:xx:xx:xx
Port 2	yy:yy:yy:yy:yy:yy

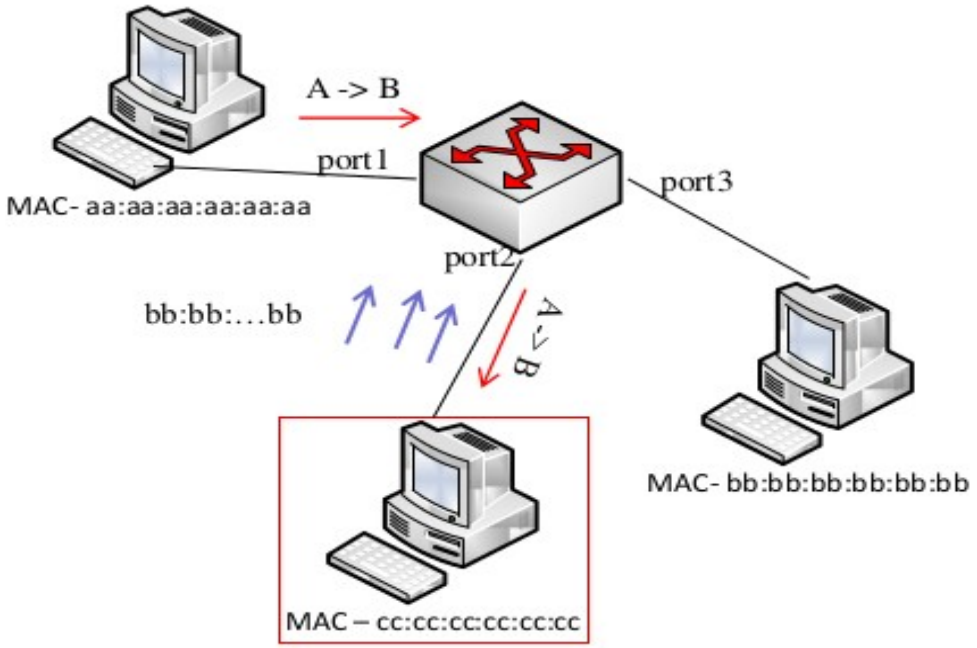
22

Attaques Ethernet: inondation de la table CAM

- Parades
  - Limiter le nombre d'@ MAC permises sur un port donné.
  - Limiter la durée qu'une @ MAC reste assignée à un port:
    - Une fois pleine de fausses entrées, la table se videra d'elle-même.
  - Assigner des @ MACs statiques à des ports.
    - Ces @ ne seraient jamais enlevées si la table devenait pleine.
    - Les @ des serveurs ou des équipements importants sont ainsi configurées dans le commutateur.
  - Authentification 802.1X
    - L'accès à un port n'est permis qu'après une authentification.

Attaques Ethernet: MAC spoofing

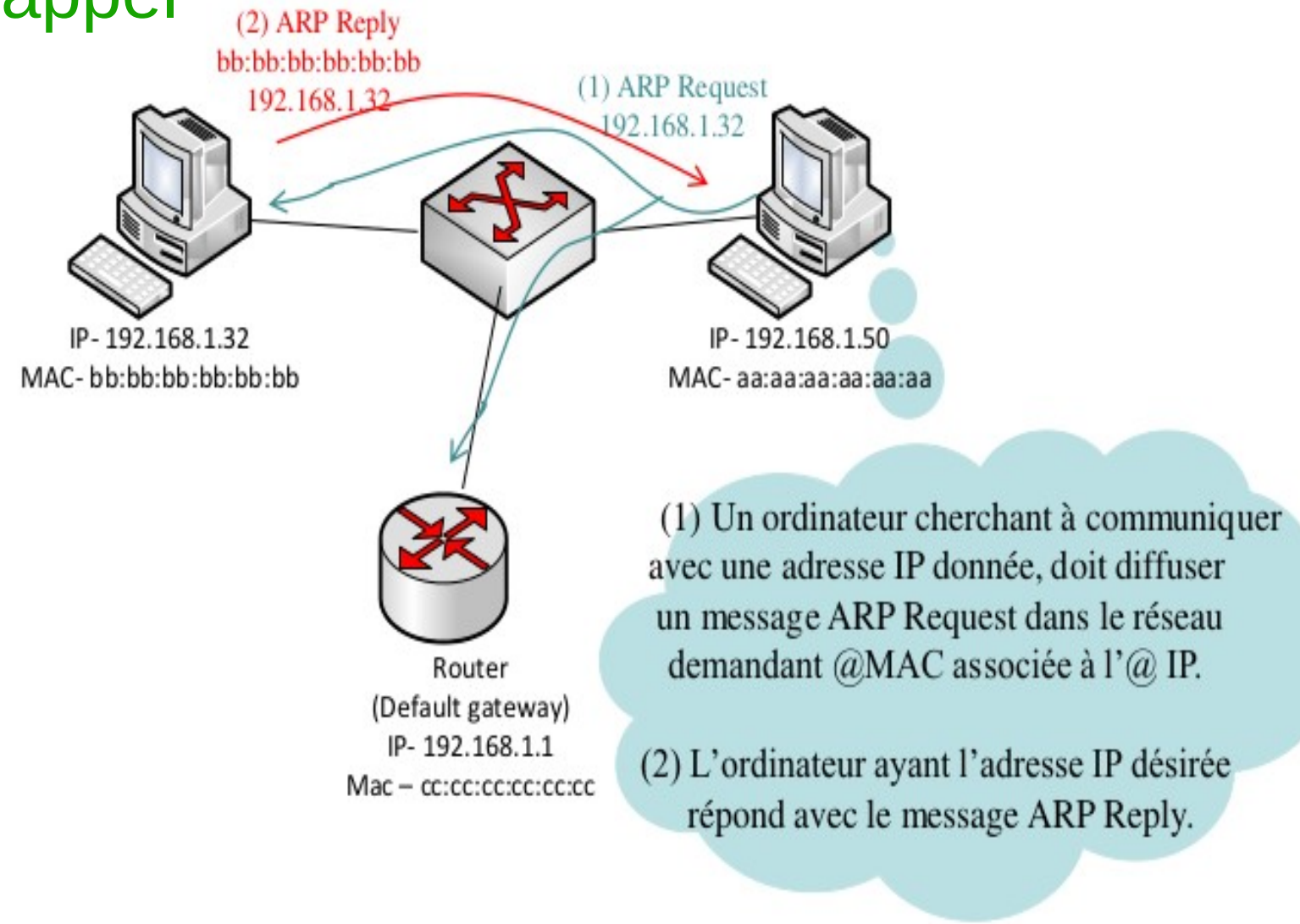
- **Vulnérabilité:** lorsqu'une adresse MAC (source) apparaît sur un autre port, le commutateur met à jour sa table.
- **Attaque:** inonder le commutateur avec de fausses trames ayant l'adresse MAC source ciblée
  - Le commutateur ajoute cette nouvelle paire (MAC, Port) dans sa table et enlève celle qui était déjà là.
  - ==> Concurrence critique avec l'ordinateur légitime.
- **Risque:** Déni de service et divulgation d'informations sensibles



Attaques Ethernet: MAC spoofing

- Parades:
  - Assigner des adresses MAC statiques à des ports.
    - Ces adresses ne seront jamais enlevées.
    - Les adresses des serveurs ou des équipements importants sont ainsi configurées dans le commutateur.
  - Utiliser l’information qui se trouve dans la table DHCP Snooping Binding
    - L’adresse MAC n’est pas apprise du composant connecté mais de l’offre DHCP.
  - Authentification 802.1X
    - L’accès à un port n’est permis qu’après une authentification.

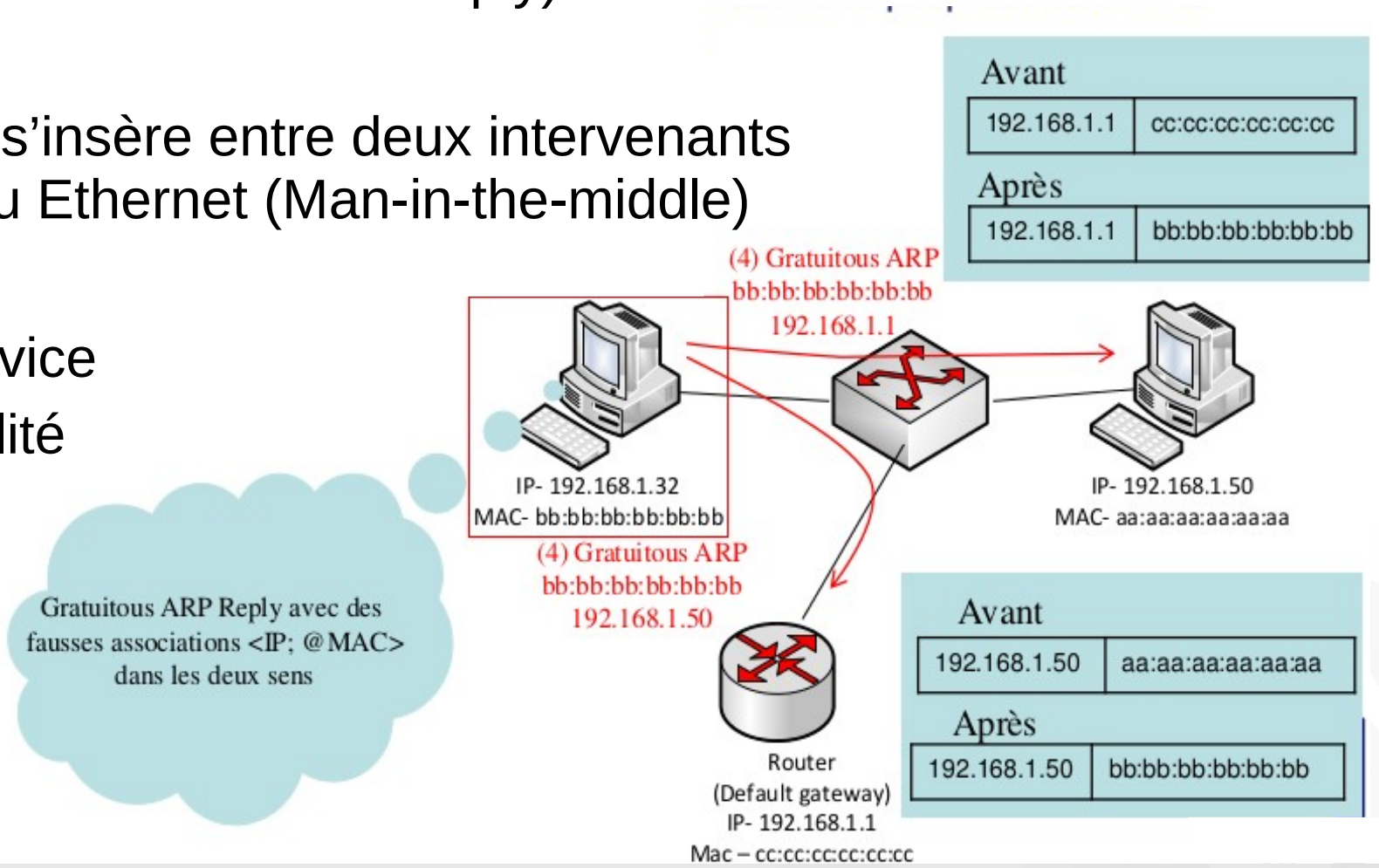
ARP - Rappel



- Les données peuvent être transmises à l'adresse MAC maintenant connue (bb:bb:bb:bb:bb:bb) du host ayant l'@IP 192.168.1.32 et retourner à l'hôte de MAC aa:aa:aa:aa:aa:aa

Attaque ARP spoofing:

- Vulnérabilité :
  - Toute personne peut prétendre être le propriétaire d'une adresse IP donnée (Gratuitous ARP Reply).
- Menace:
  - L'attaquant s'insère entre deux intervenants IP au niveau Ethernet (Man-in-the-middle)
- Risque :
  - Déni de service
  - Confidentialité



Attaque ARP spoofing:parades

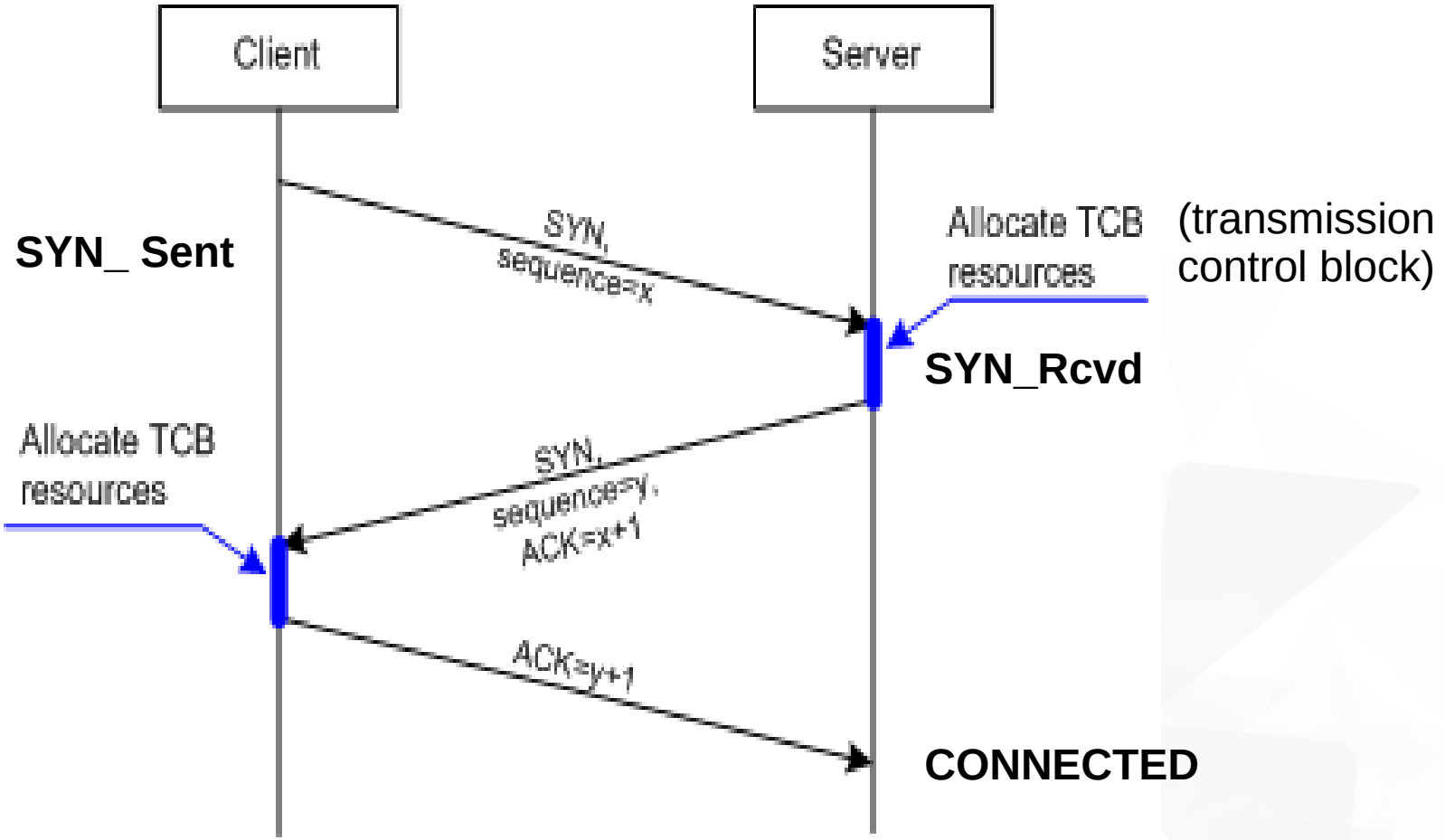
- Parade:
  - Utiliser l’information qui se trouve dans la table DHCP Snooping Binding
    - L’adresse MAC n’est pas apprise du composant connecté mais de l’offre DHCP.
  - Dynamic ARP Inspection (DAI) (Cisco)
    - Accepter les réponses ARP sur les “trusted ports” sinon vérifier leurs contenu avec la table “DHCP binding”
  - Authentification 802.1X
    - L’accès à un port n’est permis qu’après une authentification.

Attaque IP spoofing

- Vulnérabilité:
  - L’adresse IP source est contrôlé par la source
- Attaque
  - Un attaquant peut envoyer des attaques tout en personnifiant n’importe quelle source pour ne pas être retracé.
- Risque:
  - Utiliser les privilèges de l’adresse usurpée.
- Contre mesure:
  - Authentification (Ipsec, SSL…)
  - Eliminer les mesures d'authentification basées sur l'hôte

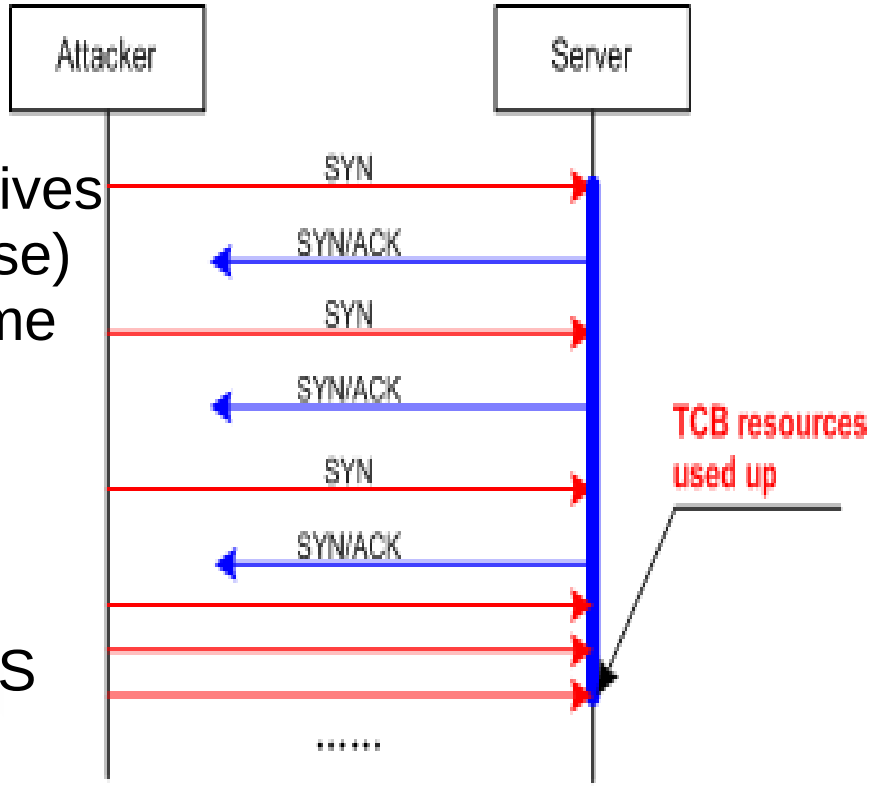
TCP: ouverture de connexion

- Connexion TCP

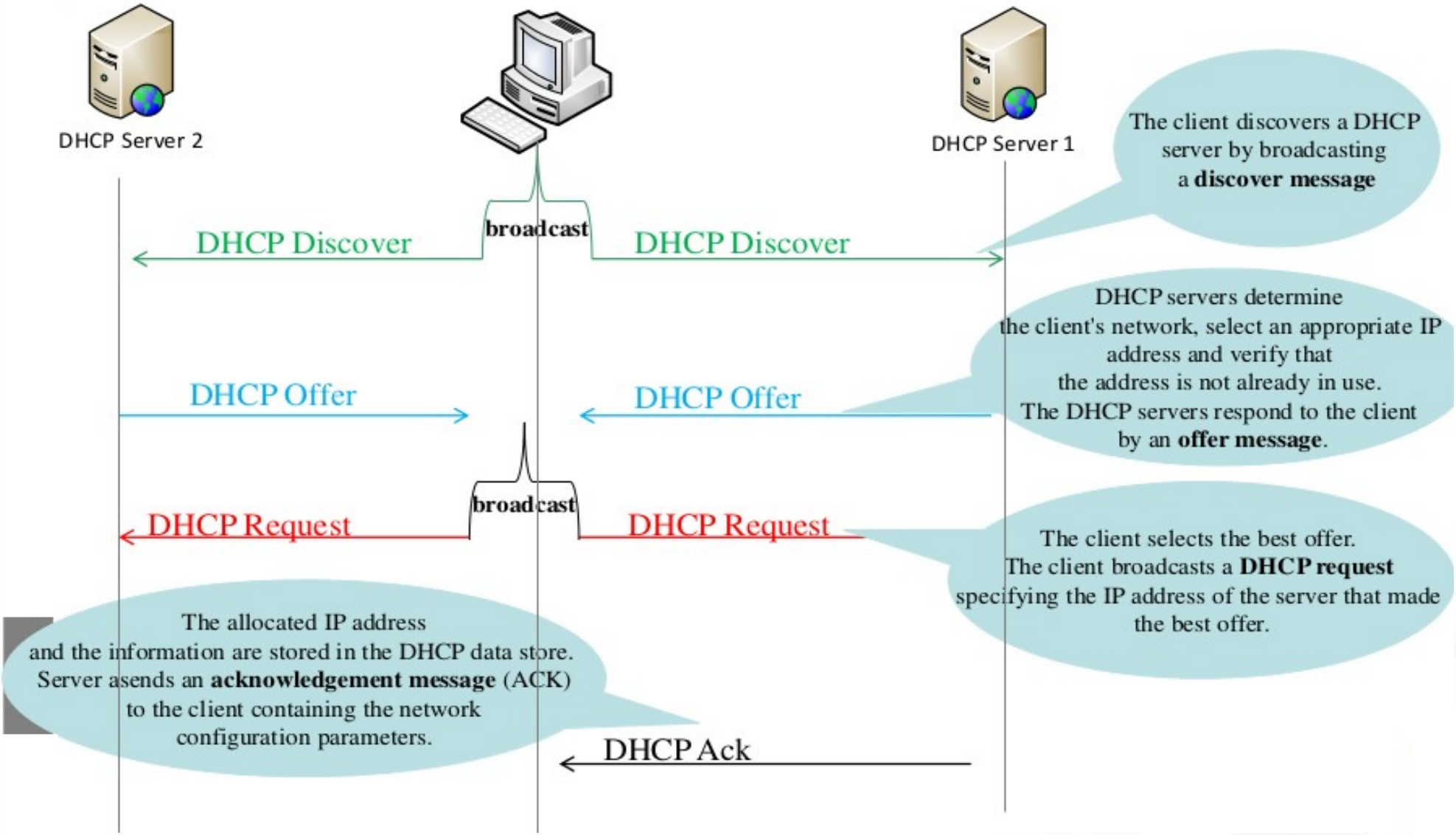


TCP SYN flooding

- Données:
  - Attente dans l'état SYN_RCVD (75s)
  - Nombre limité de connexions dans cet état
- Attaque:
  - Etablir plusieurs connexions successives semi-ouvertes (avec adresse IP fausse) afin de saturer la pile TCP de la victime
- Risque:
  - DoS, Perte de connectivité
- Parade
  - SYN cache, SYN cookies dans les OS modernes
  - Filtrage en analysant les communications TCP

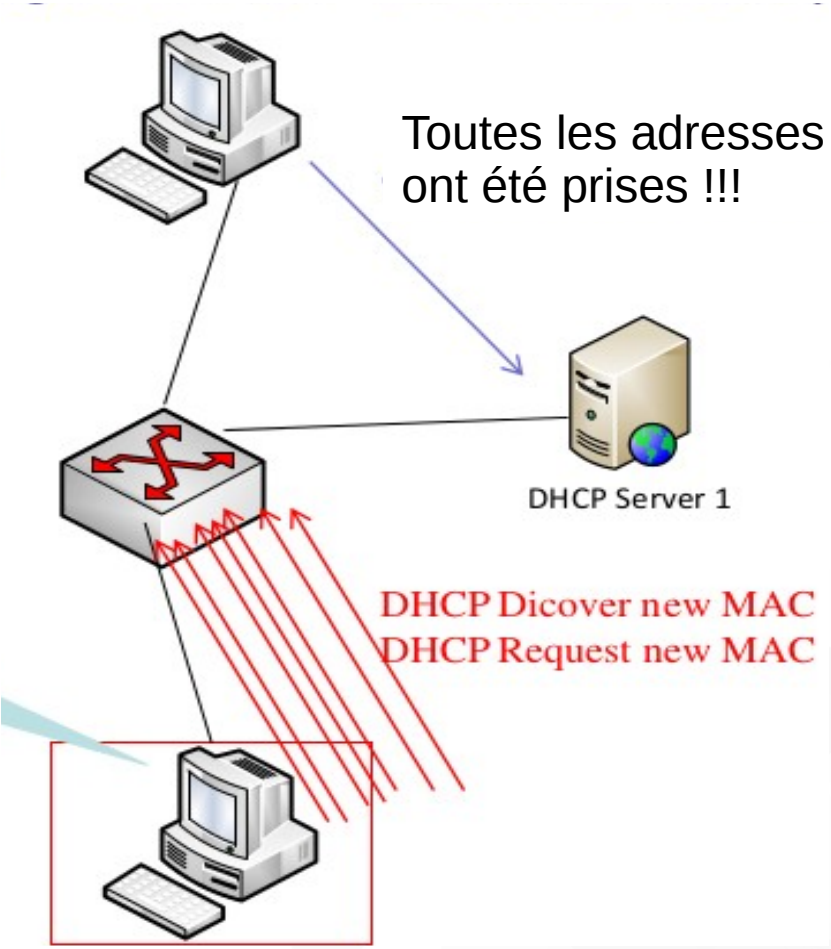


DHCP: fonctionnement



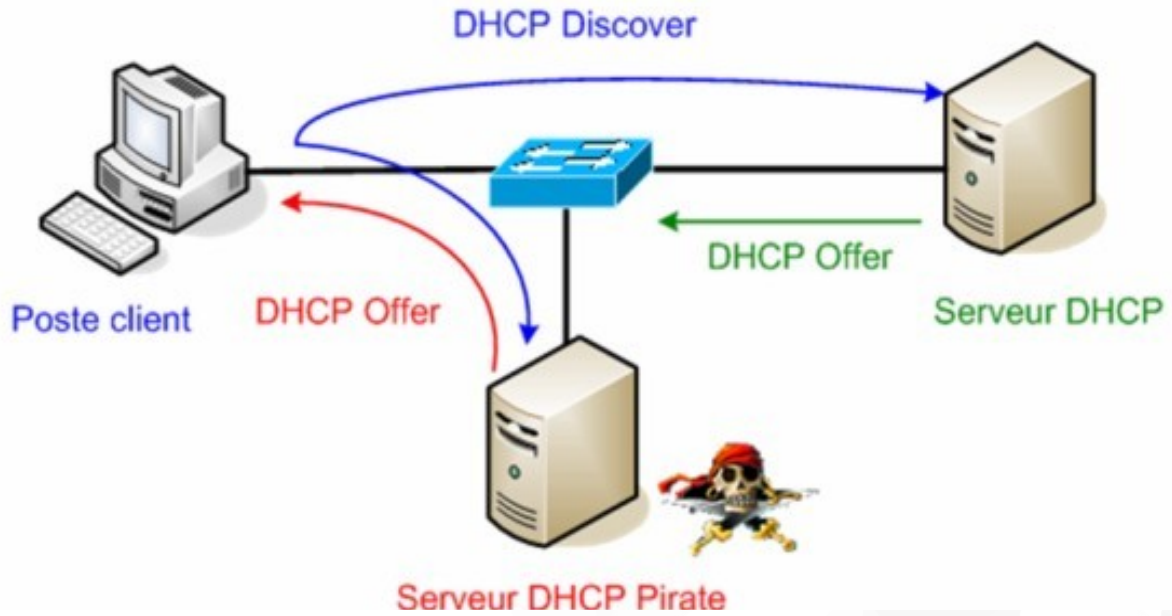
DHCP starvation

- Vulnérabilité:
  - Les requêtes DHCP sont authentifiées par l'@ MAC
- Attaque:
  - inonder le serveur avec des messages DHCP Discover et Request avec de nouvelles (spoofed) @MAC afin de réserver toutes les adresses IP disponibles.
- Risque:
  - Dénie de service.
- Contre mesures:
  - Limiter le nombre d'adresses MAC par port
  - Authentification 802.1x



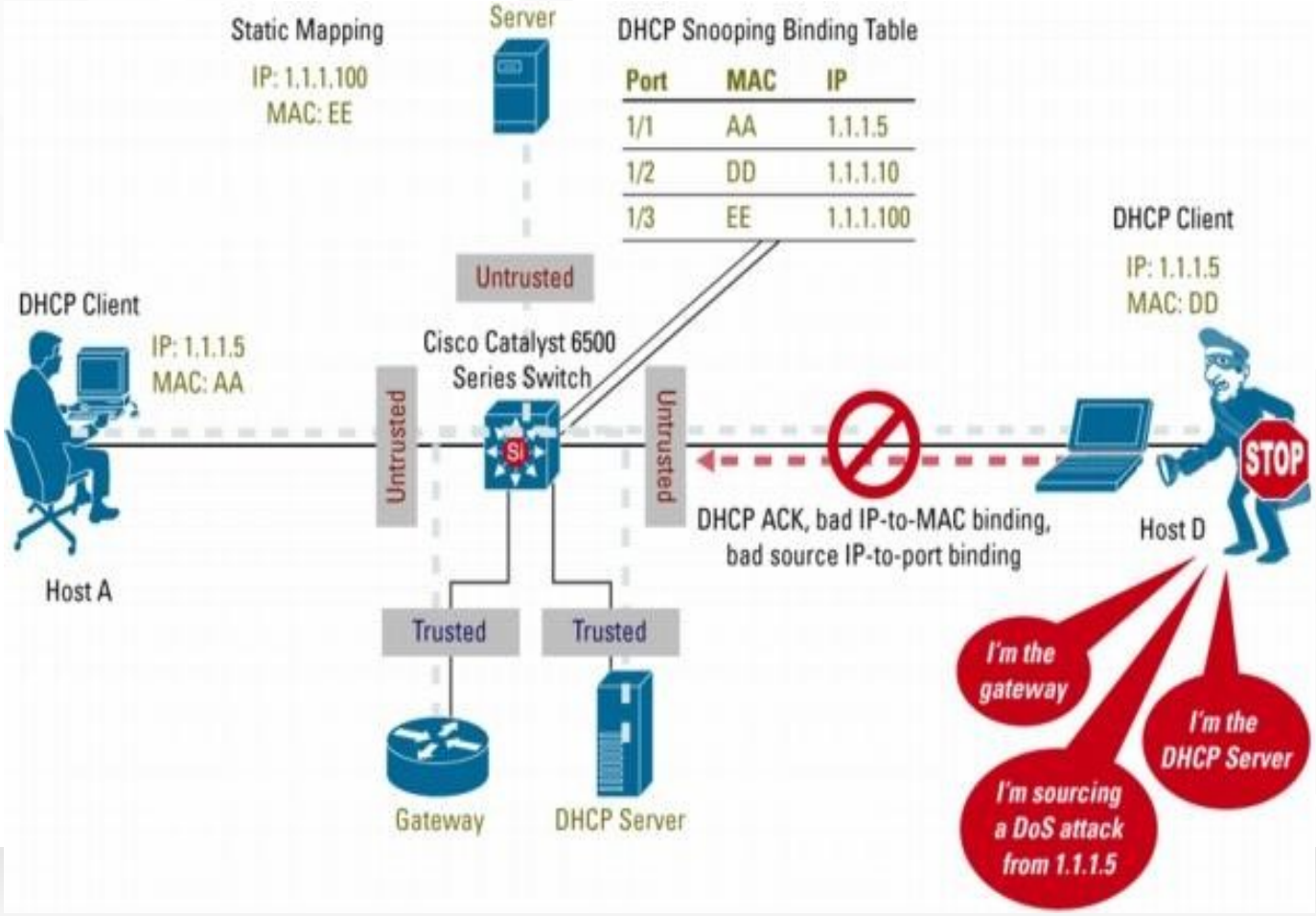
Faux serveur DHCP

- Vulnérabilité:
  - Les offres DHCP ne sont pas authentifiées.
- Attaque:
  - Prendre le rôle d'un serveur DCHP et répondre avec un DHCPOFFER en donnant de faux paramètres IP au client
    - Fausses @IP et @réseau,
    - faux routeur par défaut (=@IP de l'attaquant si celui ci veut voir tout le trafic de la victime).
- Risques:
  - DOS
  - Divulgation d'information
- Parades
  - DHCP snooping



DHCP snooping

- Utilise le concept de ports de confiance pour filtrer les paquets DHCP reçus au niveau du commutateur.
- La table DHCP snooping contient les @MAC, @IP, et information sur les interfaces « untrusted » du commutateur seulement.



Autres attaques réseaux

- Niveau ethernet
  - Manipulation des VLAN
  - Manipulation des messages STP (Spanning Tree Protocol)
  - etc.
- Niveau réseau
  - Attaques sur la fragmentation (ping of death, tiny fragment, teardrop)
  - Attaques sur l'adressage (smurf, LAND)
  - ICMP destination unreachable,
  - ICMP redirection
  - etc
- Niveau transport
  - TCP session hijacking,
  - TCP reset flooding,
  - UDP Bombing
  - etc

A venir…

- … Attaques web
- … Vulnérabilités logicielles