Couche réseau

IP et ARP

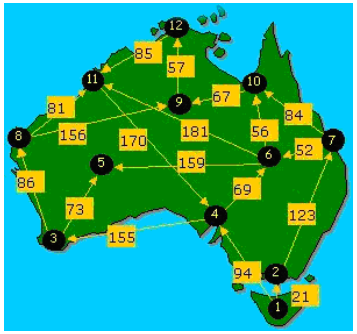
Objectifs

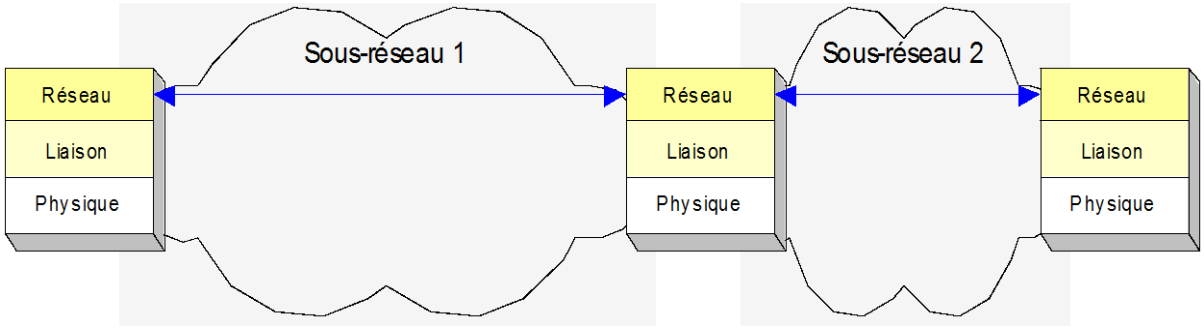
- Savoir expliquer les mécanismes du protocole IPv4
- Connaitre la structure des adresses IPv4
- Savoir calculer des plages d'adresses avec un masque de sous-réseaux
- Connaitre l'utilité de l'adressage privé et de NAT
- Savoir expliquer le fonctionnement de NAT
- Savoir expliquer le fonctionnement du protocole ARP
- Comprendre la base des attaques possibles sur la couche réseau (IP spoofing, ARP spoofing/poisoning) et leur impact sur les différents aspects de la sécurité de l'information

Couche réseau et modèle OSI

Permettre la communication à travers un réseau entier, qui est composé de sous-réseaux hétérogènes

- Adressage globale des systèmes terminaux
- Routage de paquets à travers le réseau
- Interconnexion de réseau hétérogènes
  - Par exemple fragmenter des paquets trop grands





IPv4

- Au niveau de la couche réseau, les adresses IP sont utilisées pour identifier les machines ou les routeurs
- Contrairement aux adresses MAC, les adresses IP:
  - N'identifient pas un équipement de manière unique
  - Ne sont pas fixes
- Les équipements peuvent utiliser différentes technologies pour les couches 1 et 2, mais tous doivent utiliser le protocole IP pour la couche 3
- Chaque interface réseau connectée à internet doit avoir une adresse IP pour être atteignable
- Un PC peut avoir plusieurs adresses IP, certaines adresses IP ont une signification particulière (locales, broadcast)

Caractéristiques d'IPv4

- Transmission sans connexion:
  - Une source peut envoyer des données à tout moment, sans connexion préalable
  - Un paquet contient toutes les informations nécessaires à son traitement
- Service non fiable «Best Effort»:
  - Les paquets sont placé par le routeur dans une file d'attente
  - Les paquets peuvent être perdus, arriver en retard ou dans le mauvais ordre
- Fragmentation et réassemblage:
  - Si un paquet est trop grand, le routeur le fragmente et transmet les fragments séparément
  - Le destinataire final réassemble le datagramme original

Structure des adresses IPv4

- Longueur: 4 octets
- Notation décimale: 127.0.0.1
- Contient deux parties:
  - NetworkID: identification de réseau, assigné par une autorité
  - HostID: identificateur de machine, assigné par l'entreprise, l'organisation ou l'utilisateur

- Il existe différentes classes d'adresses selon la longueur du NetworkID:
  - classe A 8 bits, classe B 16 bits, classe C 24 bits
- Le système de classes d'adresses fixes cause un gaspillage d'adresses

IPv4 – sous-réseaux

- Les sous-réseaux permettent de subdiviser une plage d'adresse en plages plus petites et de les allouer à différents réseaux physiques
- On définit un masque de sous-réseau qui détermine le nombre de sous-réseaux et attribue à chacun une plage d'adresses
- La première adresse d'une plage est l'adresse du sous-réseau
- La dernière adresse d'une plage est l'adresse de broadcast du sous-réseau
- Ces deux adresses ne peuvent pas être assignées à des machines

Exemple de masque de sous-réseau

- A partir d'un NetworkID de classe C (24 bits), on veut créer 4 sous-réseaux
- NetworkID: 200.123.230
- Masque de sous-réseau 255.255.255.192
- Dans chaque sous-réseau, 62 adresses IP peuvent être attribuées à des machines

Première adresse (adresse du sous-réseau)	Dernière adresse (broadcast)
200.123.230.0	200.123.230.63
200.123.230.64	200.123.230.127
200.123.230.128	200.123.230.191
200.123.230.192	200.123.230.255

IPv4 – adressage privé

- Autre problème: pas assez d'adresses possibles
- Utilisation d'adresses privées
- Permet de réutiliser les adresses IP
- Pas uniques donc pas utilisables sur internet
- Plages d'adresses privées:

Première adresse (adresse du réseau)	Dernière adresse (broadcast)
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

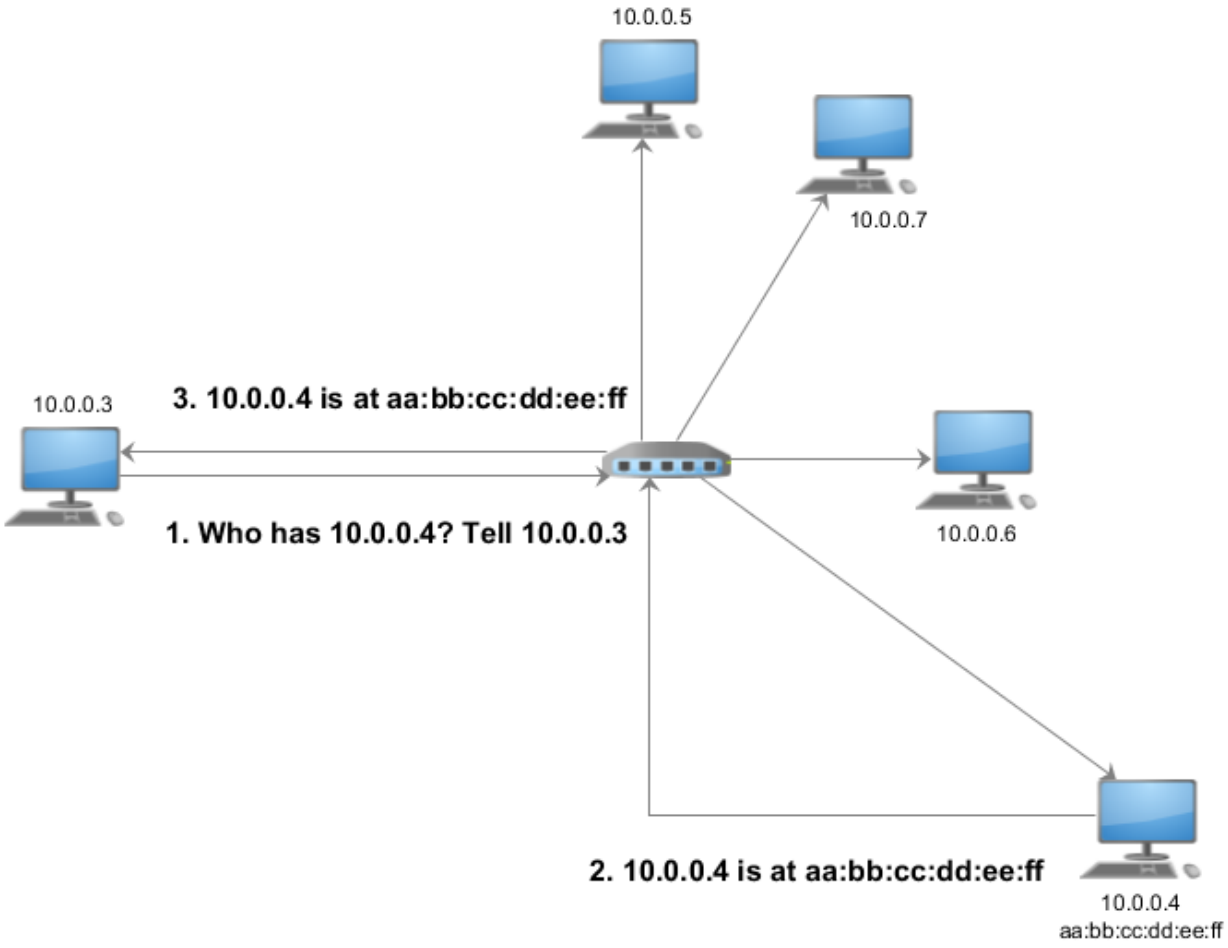
NAT

- NAT: Network Address Translation
- Permet de traduire les adresses privées entre le réseau interne et le réseau public
- Différents types de NAT:
  - Pool d'adresses publiques, définissant un nombre maximum de connexions simultanées
  - Une seule adresse publique, différenciation avec les ports
  - …

ARP

- ARP: Address Resolution Protocol
- Entre la couche liaison et réseau
- Permet de trouver l'adresse MAC qui correspond à une adresse IP
- Fonctionnement:
  - ARP garde en cache les correspondances entre adresse IP et adresse mac
  - Quand une adresse IP n'est pas dans la table, une requête ARP est envoyée
  - La machine concernée répond avec son adresse MAC
  - Les tables ARP sont mises à jour régulièrement

Exemple ARP


10.0.0.5
10.0.0.7
10.0.0.3
3. 10.0.0.4 is at aa:bb:cc:dd:ee:ff
10.0.0.6
1. Who has 10.0.0.4? Tell 10.0.0.3
2. 10.0.0.4 is at aa:bb:cc:dd:ee:ff
10.0.0.4
aa:bb:cc:dd:ee:ff

Attaques sur la couche réseau

- De manière générale, on ne vérifie pas que la source des paquets correspond à la personne qui les envoie
- Il est souvent possible de se faire passer pour quelqu'un d'autre
- Exemples:
  - IP Spoofing
  - ARP Spoofing/Poisoning

- Une attaque de type IP Spoofing consiste à modifier l'adresse IP source d'un paquet, par exemple pour masquer la provenance d'une attaque de déni de service

ARP Spoofing/Poisoning

- Le but d'une attaque d'ARP spoofing est généralement pour un attaquant d'associer son adresse MAC avec l'adresse IP de quelqu'un d'autre pour recevoir le trafic qui lui est destiné
- Permet de voir le trafic, de le modifier, ou de le stopper
  - Atteinte à la confidentialité, intégrité et disponibilité possible

- Principe: on envoie en boucle une réponse ARP forgée, pour qu'elle soit ajoutée à la table ARP de la cible et qu'elle ne fasse pas d'autre requête

Exemple ARP spoofing/poisoning